Gestire l'accesso ai file utilizzando SMB

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire l’accesso ai file utilizzando SMB

Utilizzare utenti e gruppi locali per l’autenticazione e l’autorizzazione

Modalità di utilizzo di utenti e gruppi locali da parte di ONTAP

Concetti relativi a utenti e gruppi locali

Prima di stabilire se configurare e utilizzare utenti e gruppi locali nel proprio ambiente, è necessario conoscere gli utenti e i gruppi locali e alcune informazioni di base.

- **Utente locale**

  Un account utente con un identificatore di protezione univoco (SID) che ha visibilità solo sulla macchina virtuale di storage (SVM) su cui è creato. Gli account utente locali dispongono di una serie di attributi, tra cui nome utente e SID. Un account utente locale esegue l’autenticazione locale sul server CIFS utilizzando l’autenticazione NTLM.

  Gli account utente possono essere utilizzati in diversi modi:

  - Utilizzato per concedere privilegi di *User Rights Management* a un utente.
  - Utilizzato per controllare l’accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Gruppo locale**

  Un gruppo con un SID univoco ha visibilità solo sulla SVM su cui è creato. I gruppi contengono un insieme di membri. I membri possono essere utenti locali, utenti di dominio, gruppi di dominio e account di computer di dominio. I gruppi possono essere creati, modificati o cancellati.

  I gruppi hanno diversi utilizzi:

  - Utilizzato per concedere privilegi a *User Rights Management* ai propri membri.
  - Utilizzato per controllare l’accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Dominio locale**

  Dominio con ambito locale, delimitato dalla SVM. Il nome del dominio locale è il nome del server CIFS. Gli utenti e i gruppi locali sono contenuti all’interno del dominio locale.

- **Identificatore di sicurezza (SID)**

  Un SID è un valore numerico di lunghezza variabile che identifica le entità di protezione di tipo Windows. Ad esempio, un SID tipico assume la seguente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticazione NTLM**

  Metodo di protezione Microsoft Windows utilizzato per autenticare gli utenti su un server CIFS.

- **Cluster Replicated Database (RDB)**

  Database replicato con un'istanza su ciascun nodo di un cluster. Gli oggetti utente e gruppo locali vengono memorizzati nell'RDB.

Motivi per la creazione di utenti locali e gruppi locali

Esistono diversi motivi per creare utenti locali e gruppi locali sulla macchina virtuale di storage (SVM). Ad esempio, è possibile accedere a un server SMB utilizzando un account utente locale se i controller di dominio (DC) non sono disponibili, se si desidera utilizzare gruppi locali per assegnare privilegi o se il server SMB si trova in un gruppo di lavoro.

È possibile creare uno o più account utente locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e gli utenti di dominio non sono disponibili.

  Nelle configurazioni dei gruppi di lavoro sono richiesti utenti locali.

- Se i controller di dominio non sono disponibili, si desidera eseguire l'autenticazione e l'accesso al server SMB.

  Gli utenti locali possono autenticarsi con il server SMB utilizzando l'autenticazione NTLM quando il controller di dominio non è attivo o quando i problemi di rete impediscono al server SMB di contattare il controller di dominio.

- Si desidera assegnare i privilegi di *User Rights Management* a un utente locale.

  User Rights Management è la capacità di un amministratore del server SMB di controllare i diritti degli utenti e dei gruppi sulla SVM. È possibile assegnare i privilegi a un utente assegnando i privilegi all'account dell'utente o facendo in modo che l'utente sia membro di un gruppo locale che dispone di tali privilegi.

È possibile creare uno o più gruppi locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e i gruppi di dominio non sono disponibili.

  I gruppi locali non sono richiesti nelle configurazioni dei gruppi di lavoro, ma possono essere utili per la gestione dei privilegi di accesso per gli utenti dei gruppi di lavoro locali.

- Si desidera controllare l'accesso alle risorse di file e cartelle utilizzando gruppi locali per il controllo della condivisione e dell'accesso ai file.
- Si desidera creare gruppi locali con privilegi personalizzati di *User Rights Management*.

  Alcuni gruppi di utenti integrati dispongono di privilegi predefiniti. Per assegnare un set personalizzato di privilegi, è possibile creare un gruppo locale e assegnare i privilegi necessari a tale gruppo. È quindi possibile aggiungere utenti locali, utenti di dominio e gruppi di dominio al gruppo locale.

Informazioni correlate

Come funziona l'autenticazione utente locale

Elenco dei privilegi supportati

Come funziona l'autenticazione utente locale

Prima che un utente locale possa accedere ai dati su un server CIFS, l'utente deve creare una sessione autenticata.

Poiché SMB è basato sulla sessione, l'identità dell'utente può essere determinata una sola volta, quando la sessione viene configurata per la prima volta. Il server CIFS utilizza l'autenticazione basata su NTLM per l'autenticazione degli utenti locali. Sono supportati sia NTLMv1 che NTLMv2.

ONTAP utilizza l'autenticazione locale in tre casi di utilizzo. Ogni caso di utilizzo dipende dal fatto che la parte di dominio del nome utente (con il formato DOMINIO/utente) corrisponda al nome di dominio locale del server CIFS (il nome del server CIFS):

- La parte di dominio corrisponde

  Gli utenti che forniscono credenziali utente locali quando richiedono l'accesso ai dati vengono autenticati localmente sul server CIFS.

- La porzione di dominio non corrisponde

  ONTAP tenta di utilizzare l'autenticazione NTLM con un controller di dominio nel dominio a cui appartiene il server CIFS. Se l'autenticazione ha esito positivo, l'accesso è completo. In caso contrario, ciò che accade in seguito dipende dal motivo per cui l'autenticazione non ha avuto esito positivo.

  Ad esempio, se l'utente esiste in Active Directory ma la password non è valida o è scaduta, ONTAP non tenta di utilizzare l'account utente locale corrispondente sul server CIFS. Al contrario, l'autenticazione non riesce. In altri casi, ONTAP utilizza l'account locale corrispondente sul server CIFS, se esistente, per l'autenticazione, anche se i nomi di dominio NetBIOS non corrispondono. Ad esempio, se esiste un account di dominio corrispondente ma è disattivato, ONTAP utilizza l'account locale corrispondente sul server CIFS per l'autenticazione.

- La porzione di dominio non è specificata

  ONTAP tenta innanzitutto l'autenticazione come utente locale. Se l'autenticazione come utente locale non riesce, ONTAP autentica l'utente con un controller di dominio nel dominio a cui appartiene il server CIFS.

Una volta completata correttamente l'autenticazione dell'utente locale o di dominio, ONTAP crea un token di accesso utente completo, che tiene conto dell'appartenenza al gruppo locale e dei privilegi.

Per ulteriori informazioni sull'autenticazione NTLM per gli utenti locali, consultare la documentazione di Microsoft Windows.

Informazioni correlate

Attivazione o disattivazione dell'autenticazione utente locale

Come vengono costruiti i token di accesso degli utenti

Quando un utente mappa una condivisione, viene stabilita una sessione SMB autenticata e viene creato un token di accesso utente che contiene informazioni sull'utente, l'appartenenza al gruppo dell'utente e i privilegi cumulativi e l'utente UNIX mappato.

A meno che la funzionalità non sia disattivata, al token di accesso dell'utente vengono aggiunte anche le informazioni relative all'utente locale e al gruppo. La modalità di creazione dei token di accesso dipende dal fatto che l'accesso sia destinato a un utente locale o a un utente di dominio Active Directory:

- Accesso utente locale

  Sebbene gli utenti locali possano essere membri di diversi gruppi locali, i gruppi locali non possono essere membri di altri gruppi locali. Il token di accesso dell'utente locale è composto da un'Unione di tutti i privilegi assegnati ai gruppi a cui è membro un particolare utente locale.

- Login utente di dominio

  Quando un utente di dominio effettua l'accesso, ONTAP ottiene un token di accesso utente che contiene il SID e i SID dell'utente per tutti i gruppi di dominio a cui l'utente è membro. ONTAP utilizza l'Unione del token di accesso dell'utente di dominio con il token di accesso fornito dalle appartenenze locali dei gruppi di dominio dell'utente (se presenti), nonché qualsiasi privilegio diretto assegnato all'utente di dominio o a una qualsiasi delle sue appartenenze ai gruppi di dominio.

Per l'accesso dell'utente locale e di dominio, viene impostato anche l'RID del gruppo primario per il token di accesso dell'utente. L'RID predefinito è `Domain Users` (RID 513). Non è possibile modificare l'impostazione predefinita.

Il processo di mappatura dei nomi da Windows a UNIX e da UNIX a Windows segue le stesse regole per gli account locali e di dominio.

> Non esiste alcuna mappatura automatica implicita da un utente UNIX a un account locale. Se necessario, è necessario specificare una regola di mappatura esplicita utilizzando i comandi di mappatura dei nomi esistenti.

Linee guida per l'utilizzo di SnapMirror su SVM che contengono gruppi locali

È necessario conoscere le linee guida per la configurazione di SnapMirror su volumi di proprietà di SVM che contengono gruppi locali.

Non è possibile utilizzare gruppi locali nelle ACE applicate a file, directory o condivisioni replicate da SnapMirror su un'altra SVM. Se si utilizza la funzione SnapMirror per creare un mirror DR su un volume su un altro SVM e il volume dispone di un ACE per un gruppo locale, l'ACE non è valido sul mirror. Se i dati vengono replicati su una SVM diversa, i dati vengono effettivamente trasferiti in un dominio locale diverso. Le autorizzazioni concesse agli utenti e ai gruppi locali sono valide solo nell'ambito della SVM in cui sono stati creati originariamente.

Cosa accade agli utenti e ai gruppi locali quando si eliminano i server CIFS

Il set predefinito di utenti e gruppi locali viene creato quando viene creato un server CIFS e sono associati alla macchina virtuale di storage (SVM) che ospita il server CIFS. Gli amministratori di SVM possono creare utenti e gruppi locali in qualsiasi momento. È necessario essere consapevoli di ciò che accade agli utenti e ai gruppi locali quando si elimina il server CIFS.

Gli utenti e i gruppi locali sono associati alle SVM; pertanto, non vengono cancellati quando i server CIFS vengono cancellati a causa di considerazioni di sicurezza. Anche se gli utenti e i gruppi locali non vengono cancellati quando il server CIFS viene cancellato, essi sono nascosti. Non è possibile visualizzare o gestire utenti e gruppi locali fino a quando non viene ricreato un server CIFS su SVM.

Lo stato amministrativo del server CIFS non influisce sulla visibilità degli utenti o dei gruppi locali.

Come utilizzare Microsoft Management Console con utenti e gruppi locali

È possibile visualizzare informazioni su utenti e gruppi locali dalla console di gestione Microsoft. Con questa versione di ONTAP, non è possibile eseguire altre attività di gestione per utenti e gruppi locali dalla console di gestione Microsoft.

Linee guida per il ripristino

Se si prevede di ripristinare il cluster a una release di ONTAP che non supporta utenti e gruppi locali e utenti e gruppi locali vengono utilizzati per gestire l'accesso ai file o i diritti utente, è necessario tenere presente alcune considerazioni.

- A causa di motivi di sicurezza, le informazioni relative a utenti, gruppi e privilegi locali configurati non vengono eliminate quando ONTAP viene reimpostato su una versione che non supporta la funzionalità di utenti e gruppi locali.
- In caso di ripristino di una versione principale precedente di ONTAP, ONTAP non utilizza utenti e gruppi locali durante l'autenticazione e la creazione delle credenziali.
- Gli utenti e i gruppi locali non vengono rimossi dagli ACL di file e cartelle.
- Le richieste di accesso ai file che dipendono dall'accesso concesso a causa delle autorizzazioni concesse agli utenti o ai gruppi locali vengono negate.

  Per consentire l'accesso, è necessario riconfigurare le autorizzazioni dei file in modo da consentire l'accesso in base agli oggetti di dominio anziché agli oggetti utente e gruppo locali.

Quali sono i privilegi locali

Elenco dei privilegi supportati

ONTAP dispone di un set predefinito di privilegi supportati. Per impostazione predefinita, alcuni gruppi locali predefiniti dispongono di alcuni di questi privilegi. È inoltre possibile aggiungere o rimuovere privilegi dai gruppi predefiniti o creare nuovi utenti o gruppi locali e aggiungere privilegi ai gruppi creati o a utenti e gruppi di dominio esistenti.

La seguente tabella elenca i privilegi supportati sulla macchina virtuale di storage (SVM) e fornisce un elenco di gruppi BUILTIN con privilegi assegnati:

Nome privilegio	Impostazione di sicurezza predefinita	Descrizione
`SeTcbPrivilege`	Nessuno	Agire come parte del sistema operativo
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Eseguire il backup di file e directory, sovrascrivendo eventuali ACL

Nome privilegio	Impostazione di sicurezza predefinita	Descrizione
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Ripristinare file e directory, sovrascrivendo gli ACL, impostare qualsiasi SID utente o gruppo valido come proprietario del file
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Assumere la proprietà di file o altri oggetti
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gestire il controllo Ciò include la visualizzazione, lo scarico e la cancellazione del registro di protezione.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Bypass controllo traversa Agli utenti con questo privilegio non è richiesto di disporre di autorizzazioni trasversali (x) per attraversare cartelle, collegamenti simbolici o giunzioni.

Informazioni correlate

- Assegnare privilegi locali
- Configurazione del controllo incrociato bypass

Assegnare privilegi

È possibile assegnare i privilegi direttamente agli utenti locali o agli utenti di dominio. In alternativa, è possibile assegnare utenti a gruppi locali i cui privilegi assegnati corrispondono alle funzionalità desiderate per tali utenti.

- È possibile assegnare un set di privilegi a un gruppo creato.

  Quindi, aggiungere un utente al gruppo che dispone dei privilegi che si desidera assegnare a tale utente.

- È inoltre possibile assegnare utenti locali e utenti di dominio a gruppi predefiniti i cui privilegi predefiniti corrispondono ai privilegi che si desidera concedere a tali utenti.

Informazioni correlate

- Aggiunta di privilegi a utenti o gruppi locali o di dominio
- Rimozione dei privilegi da utenti o gruppi locali o di dominio
- Reimpostazione dei privilegi per utenti e gruppi locali o di dominio
- Configurazione del controllo incrociato bypass

Linee guida per l'utilizzo dei gruppi BUILTIN e dell'account amministratore locale

Esistono alcune linee guida da tenere presenti quando si utilizzano i gruppi BUILTIN e l'account amministratore locale. Ad esempio, è possibile rinominare l'account amministratore locale, ma non è possibile eliminarlo.

- L'account Administrator può essere rinominato ma non eliminato.
- Impossibile rimuovere l'account Administrator dal gruppo BUILTIN/Administrators.
- I gruppi INCORPORATI possono essere rinominati ma non eliminati.

  Dopo aver rinominato il gruppo BUILTIN, è possibile creare un altro oggetto locale con il nome noto; tuttavia, all'oggetto viene assegnato un nuovo RID.

- Nessun account Guest locale.

Informazioni correlate

Gruppi BUILTIN predefiniti e privilegi predefiniti

Requisiti per le password dell'utente locale

Per impostazione predefinita, le password degli utenti locali devono soddisfare i requisiti di complessità. I requisiti di complessità delle password sono simili ai requisiti definiti nella *policy di sicurezza locale* di Microsoft Windows.

La password deve soddisfare i seguenti criteri:

- Deve essere composto da almeno sei caratteri
- Non deve contenere il nome dell'account utente
- Deve contenere almeno tre caratteri delle seguenti quattro categorie:
  - Caratteri maiuscoli inglesi (Dalla A alla Z)
  - Caratteri minuscoli inglesi (da a a z)
  - Base 10 cifre (da 0 a 9)
  - Caratteri speciali:

    ~! @ ` % ^ & * _ - + = / | ( ) [ ] : ; " < > , . ? /

Informazioni correlate

Attivazione o disattivazione della complessità della password richiesta per gli utenti SMB locali

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Modifica delle password degli account utente locali

Gruppi BUILTIN predefiniti e privilegi predefiniti

È possibile assegnare l'appartenenza di un utente locale o di un utente di dominio a un set predefinito di gruppi BUILTIN forniti da ONTAP. Ai gruppi predefiniti sono assegnati privilegi predefiniti.

La seguente tabella descrive i gruppi predefiniti:

Gruppo BUILTIN predefinito	Privilegi predefiniti
`BUILTIN\Administrators`RID 544 Quando viene creato per la prima volta, il locale `Administrator` L'account, con un RID di 500, viene automaticamente reso membro di questo gruppo. Quando la macchina virtuale di storage (SVM) viene unita a un dominio, il `domain\Domain Admins` il gruppo viene aggiunto al gruppo. Se SVM lascia il dominio, il `domain\Domain Admins` il gruppo viene rimosso dal gruppo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo hanno le seguenti caratteristiche: • Può creare e gestire utenti e gruppi locali. • Impossibile aggiungere se stessi o altri oggetti a `BUILTIN\Administrators` gruppo.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo possono sovrascrivere i permessi di lettura e scrittura su file o cartelle se vengono aperti con finalità di backup.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Quando creato per la prima volta, questo gruppo non ha membri (oltre a quelli impliciti `Authenticated Users` gruppo speciale). Quando la SVM viene unita a un dominio, la `domain\Domain Users` il gruppo viene aggiunto a questo gruppo. Se SVM lascia il dominio, il `domain\Domain Users` il gruppo viene rimosso da questo gruppo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Questo gruppo include tutti gli utenti, inclusi gli utenti guest (ma non gli utenti anonimi). Si tratta di un gruppo implicito con un'appartenenza implicita.	`SeChangeNotifyPrivilege`

Informazioni correlate

Linee guida per l'utilizzo dei gruppi BUILTIN e dell'account amministratore locale

Elenco dei privilegi supportati

Configurazione del controllo incrociato bypass

Attiva o disattiva la funzionalità di utenti e gruppi locali

Attivare o disattivare la panoramica delle funzionalità di utenti e gruppi locali

Prima di poter utilizzare utenti e gruppi locali per il controllo dell'accesso ai dati di sicurezza NTFS, è necessario attivare la funzionalità locale di utenti e gruppi. Inoltre, se si desidera utilizzare gli utenti locali per l'autenticazione SMB, è necessario attivare la funzionalità di autenticazione dell'utente locale.

Per impostazione predefinita, le funzionalità degli utenti e dei gruppi locali e l'autenticazione dell'utente locale sono attivate. Se non sono abilitati, è necessario abilitarli prima di poter configurare e utilizzare utenti e gruppi locali. È possibile disattivare la funzionalità di utenti e gruppi locali in qualsiasi momento.

Oltre a disattivare esplicitamente le funzionalità di utenti e gruppi locali, ONTAP disattiva le funzionalità di utenti e gruppi locali se un nodo del cluster viene reimmesso in una release di ONTAP che non supporta tale funzionalità. La funzionalità utente e gruppo locale non viene attivata finché tutti i nodi del cluster non eseguono una versione di ONTAP che la supporta.

Informazioni correlate

Modificare gli account utente locali

Modificare i gruppi locali

Aggiungere privilegi a utenti o gruppi locali o di dominio

Attivare o disattivare utenti e gruppi locali

È possibile attivare o disattivare utenti e gruppi locali per l'accesso SMB sulle macchine virtuali di storage (SVM). La funzionalità utenti e gruppi locali è attivata per impostazione predefinita.

A proposito di questa attività

È possibile utilizzare utenti e gruppi locali durante la configurazione delle autorizzazioni di condivisione SMB e file NTFS e, facoltativamente, utilizzare utenti locali per l'autenticazione quando si crea una connessione SMB. Per utilizzare gli utenti locali per l'autenticazione, è necessario attivare anche l'opzione di autenticazione degli utenti e dei gruppi locali.

Fasi

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

Se si desidera che utenti e gruppi locali siano…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Disattivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

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

Esempio

L'esempio seguente abilita le funzionalità di utenti e gruppi locali 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-local-users-and
-groups-enabled true

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

Informazioni correlate

Attiva o disattiva l'autenticazione utente locale

Attivare o disattivare gli account utente locali

Attiva o disattiva l'autenticazione utente locale

È possibile attivare o disattivare l'autenticazione utente locale per l'accesso SMB sulle macchine virtuali di storage (SVM). L'impostazione predefinita prevede l'autenticazione dell'utente locale, utile quando SVM non è in grado di contattare un controller di dominio o se si sceglie di non utilizzare i controlli di accesso a livello di dominio.

Prima di iniziare

La funzionalità di utenti e gruppi locali deve essere attivata sul server CIFS.

A proposito di questa attività

È possibile attivare o disattivare l'autenticazione utente locale in qualsiasi momento. Se si desidera utilizzare utenti locali per l'autenticazione durante la creazione di una connessione SMB, è necessario attivare anche l'opzione utenti e gruppi locali del server CIFS.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`

2. Eseguire una delle seguenti operazioni:

Se si desidera che l'autenticazione locale sia…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Disattivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

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

Esempio

L'esempio seguente abilita l'autenticazione dell'utente locale 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-local-auth
-enabled true

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

Informazioni correlate

Come funziona l'autenticazione utente locale

Attivazione o disattivazione di utenti e gruppi locali

Gestire gli account utente locali

Modificare gli account utente locali

È possibile modificare un account utente locale se si desidera modificare il nome completo o la descrizione di un utente esistente e se si desidera attivare o disattivare l'account utente. È inoltre possibile rinominare un account utente locale se il nome dell'utente è compromesso o se è necessario modificare il nome per scopi amministrativi.

Se si desidera…	Immettere il comando…
Modificare il nome completo dell'utente locale	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Se il nome completo contiene uno spazio, deve essere racchiuso tra virgolette doppie.
Modificare la descrizione dell'utente locale	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Attivare o disattivare l'account utente locale	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* -user-name *`user_name`* -is -account-disabled {true
false}`	Rinominare l'account utente locale

Esempio

Nell'esempio seguente l'utente locale "CIFS_SERVER` sue" viene rinomina in "`CIFS_SERVER sue_new" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Attivare o disattivare gli account utente locali

Attivare un account utente locale se si desidera che l'utente possa accedere ai dati contenuti nella macchina virtuale di storage (SVM) tramite una connessione SMB. È inoltre possibile disattivare un account utente locale se non si desidera che l'utente acceda ai dati SVM tramite SMB.

A proposito di questa attività

Per abilitare un utente locale, modificare l'account utente.

Fase

1. Eseguire l'azione appropriata:

Se si desidera…	Immettere il comando…
Attivare l'account utente	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`

Se si desidera…	Immettere il comando…
Disattivare l'account utente	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Modificare le password dell'account utente locale

È possibile modificare la password dell'account di un utente locale. Ciò può essere utile se la password dell'utente viene compromessa o se l'utente ha dimenticato la password.

Fase

1. Modificare la password eseguendo l'azione appropriata: `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Esempio

Nell'esempio seguente viene impostata la password per l'utente locale "`CIFS_SERVER` sue" associato alla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informazioni correlate

Attivazione o disattivazione della complessità della password richiesta per gli utenti SMB locali

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Visualizza le informazioni sugli utenti locali

È possibile visualizzare un elenco di tutti gli utenti locali in un modulo riepilogativo. Se si desidera determinare quali impostazioni dell'account sono configurate per un utente specifico, è possibile visualizzare informazioni dettagliate sull'account per tale utente, nonché informazioni sull'account per più utenti. Queste informazioni consentono di determinare se è necessario modificare le impostazioni di un utente e risolvere i problemi di autenticazione o di accesso ai file.

A proposito di questa attività

Le informazioni relative alla password di un utente non vengono mai visualizzate.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Visualizzare le informazioni su tutti gli utenti sulla macchina virtuale per lo storage (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Visualizza informazioni dettagliate sull'account di un utente	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

Quando si esegue il comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutti gli utenti locali su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Visualizza le informazioni sulle appartenenze ai gruppi per gli utenti locali

È possibile visualizzare informazioni sui gruppi locali a cui appartiene un utente locale. È possibile utilizzare queste informazioni per determinare l'accesso dell'utente a file e cartelle. Queste informazioni possono essere utili per determinare i diritti di accesso che l'utente deve avere a file e cartelle o per risolvere i problemi di accesso ai file.

A proposito di questa attività

È possibile personalizzare il comando per visualizzare solo le informazioni desiderate.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Visualizza le informazioni di appartenenza dell'utente locale per un utente locale specificato	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Visualizza le informazioni di appartenenza dell'utente locale per il gruppo locale di cui l'utente locale è membro	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*

Se si desidera…	Immettere il comando…
Visualizzazione delle informazioni di appartenenza degli utenti locali associati a una specifica SVM (Storage Virtual Machine)	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Visualizza informazioni dettagliate per tutti gli utenti locali su una SVM specificata	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Esempio

Nell'esempio seguente vengono visualizzate le informazioni di appartenenza per tutti gli utenti locali su SVM vs1; l'utente "CIFS_SERVER` Administrator" è membro del gruppo "BUILTIN`Administrators" e "`CIFS_SERVER` sue" è membro del gruppo " CIFS_SERVER g1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Eliminare gli account utente locali

È possibile eliminare gli account utente locali dalla macchina virtuale di storage (SVM) se non sono più necessari per l'autenticazione SMB locale al server CIFS o per determinare i diritti di accesso ai dati contenuti nella SVM.

A proposito di questa attività

Quando si eliminano gli utenti locali, tenere presente quanto segue:

- Il file system non viene modificato.

  I descrittori di protezione di Windows su file e directory che fanno riferimento a questo utente non vengono modificati.

- Tutti i riferimenti agli utenti locali vengono rimossi dai database di appartenenza e privilegi.
- Gli utenti standard e noti come Administrator non possono essere eliminati.

Fasi

1. Determinare il nome dell'account utente locale che si desidera eliminare: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Eliminare l'utente locale: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Verificare che l'account utente sia stato eliminato: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Esempio

Nell'esempio seguente viene eliminato l'utente locale "`CIFS_SERVER` sue" associato a SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Gestire i gruppi locali

Modificare i gruppi locali

È possibile modificare i gruppi locali esistenti modificando la descrizione di un gruppo locale esistente o rinominando il gruppo.

Se si desidera…	Utilizzare il comando…
Modificare la descrizione del gruppo locale	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Rinominare il gruppo locale	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Esempi

Nell'esempio seguente il gruppo locale "CIFS_SERVER` Engineering" viene rinomina in "`CIFS_SERVER Engineering_New":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Nell'esempio seguente viene modificata la descrizione del gruppo locale "`CIFS_SERVER` engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Visualizza informazioni sui gruppi locali

È possibile visualizzare un elenco di tutti i gruppi locali configurati sul cluster o su una specifica macchina virtuale di storage (SVM). Queste informazioni possono essere utili per la risoluzione dei problemi di accesso ai file dei dati contenuti nella SVM o dei problemi relativi ai diritti utente (privilegi) sulla SVM.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera ottenere informazioni su…	Immettere il comando…
Tutti i gruppi locali del cluster	`vserver cifs users-and-groups local-group show`
Tutti i gruppi locali sulla SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   Quando si esegue questo comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutti i gruppi locali su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gestire l’appartenenza al gruppo locale

È possibile gestire l’appartenenza a un gruppo locale aggiungendo e rimuovendo utenti locali o di dominio oppure aggiungendo e rimuovendo gruppi di dominio. Questa funzione è utile se si desidera controllare l’accesso ai dati in base ai controlli di accesso posizionati nel gruppo o se si desidera che gli utenti dispongano di privilegi associati a tale gruppo.

A proposito di questa attività

Linee guida per l’aggiunta di membri a un gruppo locale:

- Non è possibile aggiungere utenti al gruppo speciale *Everyone*.
- Il gruppo locale deve esistere prima di poter aggiungere un utente.
- L’utente deve esistere prima di poter aggiungere l’utente a un gruppo locale.
- Non è possibile aggiungere un gruppo locale a un altro gruppo locale.
- Per aggiungere un utente o un gruppo di dominio a un gruppo locale, Data ONTAP deve essere in grado di risolvere il nome in un SID.

Linee guida per la rimozione dei membri da un gruppo locale:

- Non puoi rimuovere membri dal gruppo speciale *Everyone*.
- Il gruppo da cui si desidera rimuovere un membro deve esistere.
- ONTAP deve essere in grado di risolvere i nomi dei membri che si desidera rimuovere dal gruppo in un SID corrispondente.

Fase

1. Aggiungere o rimuovere un membro di un gruppo.

Se si desidera…	Quindi utilizzare il comando…
Aggiungere un membro a un gruppo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.
Rimuovere un membro da un gruppo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.

Nell’esempio seguente vengono aggiunti un utente locale “SMB_SERVER` sue” e un gruppo di domini “ad_DOM `Sdom_eng” al gruppo locale "MB_SERVER engineering" su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Nell'esempio seguente vengono rimossi gli utenti locali "SMB_SERVER` sue" e "SMB_SERVER `Sjames" dal gruppo locale "MB_SERVER engineering" su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informazioni correlate

Visualizzazione delle informazioni sui membri dei gruppi locali

Visualizza le informazioni sui membri dei gruppi locali

È possibile visualizzare un elenco di tutti i membri dei gruppi locali configurati sul cluster o su una specifica macchina virtuale di storage (SVM). Queste informazioni possono essere utili per la risoluzione dei problemi di accesso ai file o di diritti dell'utente (privilegio).

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Immettere il comando…
Membri di tutti i gruppi locali del cluster	`vserver cifs users-and-groups local-group show-members`
Membri di tutti i gruppi locali sulla SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Esempio

Nell'esempio seguente vengono visualizzate informazioni sui membri di tutti i gruppi locali su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ---------------------------- ------------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

Eliminare un gruppo locale

È possibile eliminare un gruppo locale dalla macchina virtuale di storage (SVM) se non è più necessario per determinare i diritti di accesso ai dati associati a tale SVM o se non è più necessario per assegnare i diritti utente (privilegi) di SVM ai membri del gruppo.

A proposito di questa attività

Quando si eliminano gruppi locali, tenere presente quanto segue:

- Il file system non viene modificato.

  I descrittori di protezione di Windows su file e directory che fanno riferimento a questo gruppo non vengono modificati.

- Se il gruppo non esiste, viene restituito un errore.
- Impossibile eliminare il gruppo speciale *Everyone*.
- I gruppi incorporati come *BUILTIN/Administrators BUILTIN/Users* non possono essere eliminati.

Fasi

1. Determinare il nome del gruppo locale che si desidera eliminare visualizzando l'elenco dei gruppi locali sulla SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminare il gruppo locale: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verificare che il gruppo sia stato eliminato: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Esempio

Nell'esempio seguente viene eliminato il gruppo locale "`CIFS_SERVER` sales" associato a SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Aggiornare i nomi degli utenti e dei gruppi di dominio nei database locali

È possibile aggiungere utenti e gruppi di dominio ai gruppi locali di un server CIFS. Questi oggetti di dominio vengono registrati nei database locali del cluster. Se un oggetto di dominio viene rinominato, i database locali devono essere aggiornati manualmente.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) su cui si desidera aggiornare i nomi di dominio.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire l'azione appropriata:

Se si desidera aggiornare utenti e gruppi di dominio e…	Utilizzare questo comando…
Visualizza gli utenti e i gruppi di dominio che hanno eseguito l'aggiornamento e che non sono riusciti ad aggiornare	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

Se si desidera aggiornare utenti e gruppi di dominio e…	Utilizzare questo comando…
Visualizzare gli utenti e i gruppi di dominio che sono stati aggiornati correttamente	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Visualizzare solo gli utenti e i gruppi di dominio che non riescono ad aggiornare	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Elimina tutte le informazioni di stato relative agli aggiornamenti	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

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

Esempio

Nell'esempio riportato di seguito vengono aggiornati i nomi degli utenti e dei gruppi di dominio associati alla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. Per l'ultimo aggiornamento, è necessario aggiornare una catena di nomi dipendente:

```
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 users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

Gestire i privilegi locali

Aggiungere privilegi a utenti o gruppi locali o di dominio

È possibile gestire i diritti utente per utenti o gruppi locali o di dominio aggiungendo privilegi. I privilegi aggiunti sovrascrivono i privilegi predefiniti assegnati a uno di questi oggetti. In questo modo è possibile migliorare la sicurezza, consentendo di personalizzare i privilegi di un utente o di un gruppo.

Prima di iniziare

L'utente o il gruppo locale o di dominio a cui verranno aggiunti i privilegi deve già esistere.

A proposito di questa attività

L'aggiunta di un privilegio a un oggetto sovrascrive i privilegi predefiniti per quell'utente o gruppo. L'aggiunta di un privilegio non rimuove i privilegi aggiunti in precedenza.

Quando si aggiungono privilegi a utenti o gruppi locali o di dominio, è necessario tenere presente quanto segue:

- È possibile aggiungere uno o più privilegi.
- Quando si aggiungono privilegi a un utente o a un gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio.

  Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Aggiungere uno o più privilegi a un utente o a un gruppo locale o di dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verificare che i privilegi desiderati siano applicati all'oggetto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Esempio

Nell'esempio seguente vengono aggiunti i privilegi "SeTcbPrivilege" e "SeTakeOwnershipPrivilege" all'utente "`CIFS_SERVER` sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Rimuovere i privilegi da utenti o gruppi locali o di dominio

È possibile gestire i diritti utente per utenti o gruppi locali o di dominio rimuovendo i privilegi. In questo modo è possibile migliorare la sicurezza, consentendo di

personalizzare i privilegi massimi di utenti e gruppi.

Prima di iniziare

L'utente o il gruppo locale o di dominio da cui verranno rimossi i privilegi deve già esistere.

A proposito di questa attività

Quando si rimuovono privilegi da utenti o gruppi locali o di dominio, è necessario tenere presente quanto segue:

- È possibile rimuovere uno o più privilegi.
- Quando si rimuovono i privilegi da un utente o gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio.

  Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Rimuovere uno o più privilegi da un utente o gruppo locale o di dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verificare che i privilegi desiderati siano stati rimossi dall'oggetto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Esempio

Nell'esempio seguente vengono rimossi i privilegi "SeTcbPrivilege" e "SeTakeOwnershipPrivilege" dall'utente "`CIFS_SERVER` sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Ripristinare i privilegi per utenti e gruppi locali o di dominio

È possibile reimpostare i privilegi per utenti e gruppi locali o di dominio. Ciò può risultare utile quando si apportano modifiche ai privilegi di un utente o di un gruppo locale o di dominio e tali modifiche non sono più richieste o necessarie.

A proposito di questa attività

La reimpostazione dei privilegi per un utente o un gruppo locale o di dominio rimuove eventuali voci di privilegio per tale oggetto.

Fasi

1. Ripristinare i privilegi di un utente o di un gruppo locale o di dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Verificare che i privilegi siano ripristinati sull'oggetto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Esempi

Nell'esempio seguente vengono ripristinati i privilegi dell'utente "`CIFS_SERVER` sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. Per impostazione predefinita, gli utenti normali non dispongono di privilegi associati ai propri account:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Nell'esempio riportato di seguito vengono ripristinati i privilegi per il gruppo "`BUILTIN` Administrators", rimuovendo in modo efficace la voce di privilegio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Visualizza le informazioni sugli override dei privilegi

È possibile visualizzare informazioni sui privilegi personalizzati assegnati agli account o ai gruppi di utenti locali o di dominio. Queste informazioni consentono di determinare se vengono applicati i diritti utente desiderati.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Immettere questo comando…
Privilegi personalizzati per tutti gli utenti e i gruppi locali e di dominio sulla macchina virtuale di storage (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilegi personalizzati per un dominio o un utente e gruppo locale specifico sulla SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Quando si esegue questo comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

Esempio

Il seguente comando visualizza tutti i privilegi esplicitamente associati agli utenti e ai gruppi locali o di dominio per SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

Configurare il controllo incrociato del bypass

Configurare la panoramica del controllo incrociato del bypass

Il controllo incrociato del bypass è un diritto utente (noto anche come *privilegio*) che determina se un utente può attraversare tutte le directory nel percorso verso un file anche se l'utente non dispone delle autorizzazioni per la directory attraversata. È necessario comprendere cosa accade quando si consente o non si consente il controllo incrociato del bypass e come configurare il controllo incrociato del bypass per gli utenti sulle macchine virtuali di storage (SVM).

Cosa accade quando si consente o si non si consente il controllo incrociato del bypass

- Se consentito, quando un utente tenta di accedere a un file, ONTAP non controlla l'autorizzazione di attraversamento per le directory intermedie quando determina se concedere o negare l'accesso al file.
- Se non consentito, ONTAP controlla l'autorizzazione di traslazione (esecuzione) per tutte le directory nel percorso del file.

  Se una qualsiasi delle directory intermedie non dispone di "X" (autorizzazione trasversale), ONTAP nega l'accesso al file.

Configurare il controllo incrociato del bypass

È possibile configurare il controllo incrociato di bypass utilizzando l'interfaccia utente di ONTAP o configurando i criteri di gruppo di Active Directory con questo diritto utente.

Il `SeChangeNotifyPrivilege` il privilegio controlla se gli utenti sono autorizzati a ignorare il controllo incrociato.

- L'aggiunta a utenti o gruppi SMB locali sulla SVM o a utenti o gruppi di dominio consente di evitare il controllo incrociato.
- La sua rimozione da utenti o gruppi SMB locali sulla SVM o da utenti o gruppi di dominio non consente di ignorare il controllo incrociato.

Per impostazione predefinita, i seguenti gruppi BUILTIN su SVM hanno il diritto di ignorare il controllo incrociato:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Se non si desidera consentire ai membri di uno di questi gruppi di ignorare il controllo incrociato, è necessario rimuovere questo privilegio dal gruppo.

Durante la configurazione del bypass, è necessario tenere presente quanto segue per gli utenti e i gruppi SMB locali sulla SVM utilizzando la CLI:

- Se si desidera consentire ai membri di un gruppo locale o di dominio personalizzato di ignorare il controllo incrociato, è necessario aggiungere `SeChangeNotifyPrivilege` privilegio per quel gruppo.
- Se si desidera consentire a un singolo utente locale o di dominio di ignorare il controllo incrociato e tale utente non è membro di un gruppo con tale privilegio, è possibile aggiungere `SeChangeNotifyPrivilege` privilegio per l'account utente.
- È possibile disattivare il controllo incrociato bypass per utenti o gruppi locali o di dominio rimuovendo `SeChangeNotifyPrivilege` privilegio in qualsiasi momento.

> Per disattivare la funzione di bypass travers per utenti o gruppi locali o di dominio specifici, è necessario rimuovere anche `SeChangeNotifyPrivilege` privilegio di `Everyone` gruppo.

Informazioni correlate

Consenti a utenti o gruppi di ignorare il controllo incrociato della directory

Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory

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

Creare elenchi di controllo degli accessi di condivisione SMB

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

Elenco dei privilegi supportati

Aggiungere privilegi a utenti o gruppi locali o di dominio

Consenti a utenti o gruppi di ignorare il controllo incrociato della directory

Se si desidera che un utente sia in grado di attraversare tutte le directory del percorso verso un file anche se non dispone delle autorizzazioni per una directory attraversata, è possibile aggiungere `SeChangeNotifyPrivilege` Privilegio per utenti o gruppi SMB locali su macchine virtuali storage (SVM). Per impostazione predefinita, gli utenti possono ignorare il controllo incrociato della directory.

Prima di iniziare

- Un server SMB deve essere presente sulla SVM.
- È necessario attivare l'opzione server SMB per utenti e gruppi locali.
- L'utente o il gruppo locale o di dominio in cui si utilizza `SeChangeNotifyPrivilege` il privilegio verrà aggiunto deve essere già esistente.

A proposito di questa attività

Quando si aggiungono privilegi a un utente o a un gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Abilitare il controllo incrociato bypass aggiungendo `SeChangeNotifyPrivilege` privilegio per un utente o un gruppo locale o di dominio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Il valore di `-user-or-group-name` il parametro è un utente o un gruppo locale o un utente o un gruppo di dominio.

2. Verificare che l'utente o il gruppo specificato abbia attivato il controllo incrociato bypass: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Esempio

Il seguente comando consente agli utenti che appartengono al gruppo "EXAMPLE" di ignorare il controllo incrociato della directory aggiungendo il `SeChangeNotifyPrivilege` privilegio per il gruppo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Informazioni correlate

Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory

Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory

Se non si desidera che un utente attraversi tutte le directory nel percorso di un file perché l'utente non dispone delle autorizzazioni per la directory attraversata, è possibile rimuovere `SeChangeNotifyPrivilege` Privilegio di utenti o gruppi SMB locali su macchine virtuali storage (SVM).

Prima di iniziare

L'utente o il gruppo locale o di dominio da cui verranno rimossi i privilegi deve già esistere.

A proposito di questa attività

Quando si rimuovono i privilegi da un utente o gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Non consentire il controllo incrociato del bypass: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Il comando rimuove `SeChangeNotifyPrivilege` privilegio dell'utente o del gruppo locale o di dominio specificato con il valore per `-user-or-group-name` *`name`* parametro.

2. Verificare che l'utente o il gruppo specificato abbia disattivato il controllo incrociato bypass: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Esempio

Il seguente comando non consente agli utenti che appartengono al gruppo "EXAMPLE" di ignorare il controllo incrociato della directory:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           -
```

Informazioni correlate

Consentire a utenti o gruppi di ignorare il controllo incrociato della directory

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

Visualizza informazioni generali sulla sicurezza dei file e sui criteri di controllo

È possibile visualizzare informazioni sulla sicurezza dei file su file e directory contenuti nei volumi su macchine virtuali di storage (SVM). È possibile visualizzare informazioni sui criteri di controllo sui volumi FlexVol. Se configurato, è possibile visualizzare informazioni sulle impostazioni di protezione accesso a livello di storage e controllo dinamico degli accessi sui volumi FlexVol.

Visualizzazione delle informazioni sulla sicurezza dei file

È possibile visualizzare le informazioni sulla sicurezza dei file applicate ai dati contenuti nei volumi e nei qtree (per i volumi FlexVol) con i seguenti stili di sicurezza:

- NTFS
- UNIX
- Misto

Visualizzazione delle informazioni sui criteri di controllo

È possibile visualizzare informazioni sulle policy di audit per il controllo degli eventi di accesso sui volumi FlexVol sui seguenti protocolli NAS:

- SMB (tutte le versioni)
- NFSv4.x

Visualizzazione di informazioni sulla sicurezza di Storage-Level Access Guard (SLAG)

La protezione degli accessi a livello di storage può essere applicata a volumi FlexVol e oggetti qtree con i seguenti stili di sicurezza:

- NTFS
- Misto
- UNIX (se un server CIFS è configurato sulla SVM che contiene il volume)

Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi (DAC)

La protezione del controllo dinamico degli accessi può essere applicata a un oggetto all'interno di un volume FlexVol con i seguenti stili di protezione:

- NTFS
- Misto (se l'oggetto dispone di una protezione efficace NTFS)

Informazioni correlate

Protezione dell'accesso ai file mediante Storage-Level Access Guard

Visualizzazione di informazioni su Storage-Level Access Guard

Visualizza le informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi di sicurezza NTFS, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli attributi DOS. 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.

- Poiché i volumi e i qtree di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file, i campi di output relativi a UNIX contengono informazioni sulle autorizzazioni per i file UNIX di sola visualizzazione.
- L'output ACL viene visualizzato per file e cartelle con protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata sulla radice del volume o sul qtree, l'output di un volume o percorso del qtree in cui è configurato Storage-Level Access Guard potrebbe visualizzare sia gli ACL dei file normali che gli ACL di Storage-Level Access Guard.
- L'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se il controllo dinamico degli accessi è configurato per il percorso di file o directory specificato.

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`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/vol4` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         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
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza con maschere estese sul percorso `/data/engineering` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
```

```
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
```

```
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Nell’esempio riportato di seguito vengono visualizzate le informazioni di sicurezza, incluse le informazioni di protezione Storage-Level Access Guard, per il volume 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
```

Informazioni correlate

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

Visualizza informazioni sulla sicurezza dei file su volumi misti di sicurezza

È possibile visualizzare informazioni sulla sicurezza di file e directory su volumi misti di sicurezza, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. 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.

- I volumi e i qtree misti di sicurezza possono contenere alcuni file e cartelle che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.
- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le directory che utilizzano la protezione UNIX e che hanno solo autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia le autorizzazioni dei file UNIX che gli ACL Storage-Level Access Guard.
- Se il percorso immesso nel comando riguarda i dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se è configurato Dynamic Access Control per il percorso di file o directory specificato.

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`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/projects` In SVM vs1 in forma di maschera espansa. Questo percorso misto in stile di sicurezza offre una sicurezza efficace per UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/data` In SVM vs1. Questo percorso misto di sicurezza ha una protezione efficace NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                 Vserver: vs1
                               File Path: /data
                       File Inode Number: 544
                          Security Style: mixed
                         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
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza relative al volume nel percorso `/datavol5` In SVM vs1. Il livello superiore di questo volume misto di sicurezza 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
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Informazioni correlate

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

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

Visualizza informazioni sulla sicurezza dei file su volumi UNIX di tipo Security

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi UNIX di tipo Security, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni

applicate e le informazioni sui proprietari e sui gruppi UNIX. 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 directory. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo le autorizzazioni dei file UNIX, ovvero i bit di modalità o gli ACL NFSv4 per determinare i diritti di accesso ai file.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NFSv4.

  Questo campo è vuoto per i file e le directory che utilizzano la protezione UNIX e che hanno solo autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi di output del proprietario e del gruppo nell'output ACL non sono validi nel caso dei descrittori di protezione NFSv4.

  Sono significativi solo per i descrittori di protezione NTFS.

- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

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`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` In SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` In SVM vs1 sotto forma di maschera espansa:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: 0x10
                      ...0 .... .... .... = Offline
                      .... ..0. .... .... = Sparse
                      .... .... 0... .... = Normal
                      .... .... ..0. .... = Archive
                      .... .... ...1 .... = Directory
                      .... .... .... .0.. = System
                      .... .... .... ..0. = Hidden
                      .... .... .... ...0 = Read Only
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Informazioni correlate

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

Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

  I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

Fase

1. Visualizzare le impostazioni dei criteri di controllo 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`
Come elenco dettagliato	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` In SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         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:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/datavol1` In SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```
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:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         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
```

Visualizza informazioni sui criteri di audit NFSv4 sui volumi FlexVol utilizzando la CLI

È possibile visualizzare informazioni sui criteri di controllo di NFSv4 sui volumi FlexVol

utilizzando l'interfaccia CLI di ONTAP, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo dell'accesso al sistema (SACL). È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle directory di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo SACL NFSv4 per le policy di controllo.
- I file e le directory di un volume misto di sicurezza con stile UNIX possono applicare criteri di controllo NFSv4.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NFSv4.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL normali di file NFSv4, directory e SACL NTFS di Storage-Level Access Guard.
- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

Fasi

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`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/lab` In SVM vs1. Questo percorso di sicurezza UNIX ha un SACL NFSv4.

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

È possibile utilizzare il carattere jolly (*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o volume root.

Il carattere jolly (**) può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory. Se si desidera visualizzare le informazioni di un particolare file o directory denominata "**", è necessario fornire il percorso completo tra virgolette doppie ("``").

Esempio

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso `/1/` Di SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                   Vserver: vs1
                 File Path: /1/1
            Security Style: mixed
           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:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                   Vserver: vs1
                 File Path: /1/1/abc
            Security Style: mixed
           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:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Il seguente comando visualizza le informazioni di un file denominato "*" sotto il percorso `/vol1/a` Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la CLI

Gestisci la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la panoramica CLI

È possibile gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su macchine virtuali storage (SVM) utilizzando la CLI.

È possibile gestire la sicurezza dei file NTFS e le policy di controllo dai client SMB o utilizzando la CLI. Tuttavia, l’utilizzo della CLI per configurare le policy di controllo e sicurezza dei file elimina la necessità di utilizzare un client remoto per gestire la sicurezza dei file. L’utilizzo della CLI può ridurre significativamente il tempo necessario per applicare la protezione a molti file e cartelle utilizzando un singolo comando.

È possibile configurare Access Guard a livello di storage, un altro livello di sicurezza applicato da ONTAP ai volumi SVM. Storage-Level Access Guard si applica agli accessi da tutti i protocolli NAS all’oggetto storage a cui è applicato Storage-Level Access Guard.

Access Guard a livello di storage può essere configurato e gestito solo dalla CLI di ONTAP. Non è possibile gestire le impostazioni di Storage-Level Access Guard dai client SMB. Inoltre, se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, non viene visualizzata la protezione Storage-Level Access Guard. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX). Pertanto, Storage-Level Access Guard offre un ulteriore livello di sicurezza per l’accesso ai dati, impostato e gestito in modo

indipendente dall'amministratore dello storage.

> Anche se sono supportate solo le autorizzazioni di accesso NTFS per Storage-Level Access Guard, ONTAP può eseguire controlli di sicurezza per l'accesso via NFS ai dati sui volumi in cui viene applicato Storage-Level Access Guard se l'utente UNIX esegue il mapping a un utente Windows sulla SVM proprietaria del volume.

Volumi NTFS di tipo Security

Tutti i file e le cartelle contenuti nei volumi e nei qtree di sicurezza NTFS dispongono di un'efficace protezione NTFS. È possibile utilizzare `vserver security file-directory` Famiglia di comandi per implementare i seguenti tipi di protezione sui volumi NTFS di tipo Security:

- Permessi dei file e policy di controllo per file e cartelle contenuti nel volume
- Protezione degli accessi a livello di storage sui volumi

Volumi misti di sicurezza

I volumi e i qtree misti in stile di sicurezza possono contenere alcuni file e cartelle con una protezione efficace UNIX e che utilizzano autorizzazioni per i file UNIX, i criteri di controllo Mbit di modalità o ACL NFSv4.x e NFSv4.x, nonché alcuni file e cartelle con una protezione effettiva NTFS e che utilizzano le autorizzazioni per i file NTFS e i criteri di controllo. È possibile utilizzare `vserver security file-directory` famiglia di comandi per applicare i seguenti tipi di protezione a dati misti di tipo sicurezza:

- Permessi dei file e policy di controllo per file e cartelle con NTFS efficace in stile di sicurezza nel volume misto o nel qtree
- Access Guard a livello di storage per i volumi con sicurezza efficace NTFS e UNIX

Volumi UNIX di tipo Security

I volumi e le qtree UNIX di sicurezza contengono file e cartelle con protezione efficace UNIX (ovvero i bit di modalità o gli ACL NFSv4.x). Se si desidera utilizzare il, tenere presente quanto segue `vserver security file-directory` Famiglia di comandi per implementare la sicurezza su volumi UNIX di tipo Security:

- Il `vserver security file-directory` La famiglia di comandi non può essere utilizzata per gestire la sicurezza dei file UNIX e le policy di controllo su qtree e volumi di sicurezza UNIX.
- È possibile utilizzare `vserver security file-directory` Famiglia di comandi per configurare Storage-Level Access Guard su volumi UNIX di tipo Security, a condizione che SVM con il volume di destinazione contenga un server CIFS.

Informazioni correlate

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

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

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la CLI

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

Casi di utilizzo dell'interfaccia CLI per impostare la sicurezza di file e cartelle

Poiché è possibile applicare e gestire la sicurezza di file e cartelle in locale senza il coinvolgimento di un client remoto, è possibile ridurre significativamente il tempo necessario per impostare la protezione in blocco su un gran numero di file o cartelle.

È possibile utilizzare la CLI per impostare la sicurezza di file e cartelle nei seguenti casi di utilizzo:

- Storage di file in ambienti aziendali di grandi dimensioni, ad esempio lo storage di file nelle home directory
- Migrazione dei dati
- Modifica del dominio Windows
- Standardizzazione delle policy di controllo e sicurezza dei file nei file system NTFS

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

È necessario conoscere alcuni limiti quando si utilizza la CLI per impostare la sicurezza di file e cartelle.

- Il `vserver security file-directory` La famiglia di comandi non supporta l'impostazione degli ACL NFSv4.

  È possibile applicare i descrittori di protezione NTFS solo a file e cartelle NTFS.

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

I descrittori di protezione contengono gli elenchi di controllo degli accessi che determinano le azioni che un utente può eseguire su file e cartelle e le operazioni controllate quando un utente accede a file e cartelle.

- **Autorizzazioni**

  Le autorizzazioni sono consentite o negate dal proprietario di un oggetto e determinano le azioni che un oggetto (utenti, gruppi o oggetti computer) può eseguire su file o cartelle specifici.

- **Descrittori di sicurezza**

  I descrittori di protezione sono strutture di dati che contengono informazioni di sicurezza che definiscono le autorizzazioni associate a un file o a una cartella.

- **ACL (Access Control List)**

  Gli elenchi di controllo degli accessi sono gli elenchi contenuti in un descrittore di protezione che contengono informazioni sulle azioni che gli utenti, i gruppi o gli oggetti computer possono eseguire nel file o nella cartella a cui è applicato il descrittore di protezione. Il descrittore di protezione può contenere i seguenti due tipi di ACL:

  - DACL (Discretionary Access Control List)
  - SACL (System Access Control List)

- **Elenchi di controllo degli accessi discrezionali (DACL)**

I DACL contengono l'elenco dei SIDS per gli utenti, i gruppi e gli oggetti computer ai quali è consentito o negato l'accesso per eseguire azioni su file o cartelle. I DACL contengono zero o più voci di controllo degli accessi (ACE).

- **System access control list (SACL)**

  I SACL contengono l'elenco di SIDS per gli utenti, i gruppi e gli oggetti computer per i quali vengono registrati eventi di controllo riusciti o non riusciti. I SACL contengono zero o più voci di controllo degli accessi (ACE).

- **Voci di controllo di accesso (ACE)**

  Gli assi sono singole voci in DACL o SACL:

  - Una voce di controllo dell'accesso DACL specifica i diritti di accesso consentiti o negati per determinati utenti, gruppi o oggetti computer.
  - Una voce di controllo dell'accesso SACL specifica gli eventi di successo o di errore da registrare quando si controllano le azioni specifiche eseguite da utenti, gruppi o oggetti computer specifici.

- **Ereditarietà delle autorizzazioni**

  L'ereditarietà delle autorizzazioni descrive il modo in cui le autorizzazioni definite nei descrittori di protezione vengono propagate a un oggetto da un oggetto padre. Solo le autorizzazioni ereditabili vengono ereditate dagli oggetti figlio. Quando si impostano le autorizzazioni sull'oggetto padre, è possibile decidere se cartelle, sottocartelle e file possono ereditare tali autorizzazioni con "applicabile a. `this-folder`, `sub-folders`e `files`".

Informazioni correlate

"Controllo SMB e NFS e tracciamento della sicurezza"

Configurazione e applicazione dei criteri di controllo a file e cartelle NTFS mediante l'interfaccia CLI

Linee guida per l'applicazione di policy di directory di file che utilizzano utenti o gruppi locali sulla destinazione di disaster recovery SVM

Prima di applicare i criteri di directory dei file alla destinazione di disaster recovery SVM (Storage Virtual Machine) in una configurazione di eliminazione dell'ID, è necessario tenere presenti alcune linee guida se la configurazione dei criteri di directory dei file utilizza utenti o gruppi locali nel descrittore di protezione o nelle voci DACL o SACL.

È possibile configurare una configurazione di disaster recovery per una SVM in cui la SVM di origine sul cluster di origine replica i dati e la configurazione dalla SVM di origine a una SVM di destinazione su un cluster di destinazione.

È possibile configurare uno dei due tipi di disaster recovery SVM:

- Identità preservata

  Con questa configurazione, l'identità di SVM e del server CIFS viene preservata.

- Identità scartata

  Con questa configurazione, l'identità di SVM e del server CIFS non viene preservata. In questo scenario, il

nome di SVM e del server CIFS sulla SVM di destinazione è diverso da SVM e dal nome del server CIFS sulla SVM di origine.

Linee guida per le configurazioni di identità scartate

In una configurazione con eliminazione dell'identità, per un'origine SVM che contiene configurazioni di utente, gruppo e privilegi locali, il nome del dominio locale (nome del server CIFS locale) deve essere modificato in modo che corrisponda al nome del server CIFS sulla destinazione SVM. Ad esempio, se il nome SVM di origine è "vs1" e il nome del server CIFS è "CIFS1" e il nome SVM di destinazione è "vs1_dst" e il nome del server CIFS è "CIFS1_DST", il nome del dominio locale di un utente locale denominato "CIFS1` user1" viene automaticamente modificato in "`CIFST_DVM_1".

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Anche se i nomi degli utenti e dei gruppi locali vengono modificati automaticamente nei database degli utenti e dei gruppi locali, i nomi degli utenti o dei gruppi locali non vengono modificati automaticamente nelle configurazioni dei criteri delle directory dei file (criteri configurati sulla CLI tramite `vserver security file-directory` famiglia di comandi).

Ad esempio, per "vs1", se è stata configurata una voce DACL in cui si trova `-account` Il parametro è impostato su "`CIFS1` user1", l'impostazione non viene modificata automaticamente sulla SVM di destinazione per riflettere il nome del server CIFS di destinazione.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

È necessario utilizzare `vserver security file-directory modify` Comandi per modificare manualmente il nome del server CIFS nel nome del server CIFS di destinazione.

Componenti di configurazione dei criteri di directory dei file che contengono parametri dell'account

Esistono tre componenti di configurazione dei criteri di directory dei file che possono utilizzare le impostazioni dei parametri che possono contenere utenti o gruppi locali:

- Descrittore di sicurezza

  È possibile specificare il proprietario del descrittore di protezione e il gruppo primario del proprietario del descrittore di protezione. Se il descrittore di protezione utilizza un utente o un gruppo locale per le voci del proprietario e del gruppo primario, è necessario modificare il descrittore di protezione per utilizzare la SVM di destinazione nel nome dell'account. È possibile utilizzare `vserver security file-directory ntfs modify` per apportare le modifiche necessarie ai nomi degli account.

- Voci DACL

  Ogni voce DACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i DACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci DACL esistenti, è necessario rimuovere eventuali voci DACL con utenti o gruppi locali dai descrittori di protezione, creare nuove voci DACL con i nomi account di destinazione corretti e associare queste nuove voci DACL ai descrittori di protezione appropriati.

- Voci SACL

  Ogni voce SACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i SACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci SACL esistenti, è necessario rimuovere eventuali voci SACL con

utenti o gruppi locali dai descrittori di protezione, creare nuove voci SACL con i nomi account di destinazione corretti e associare queste nuove voci SACL ai descrittori di protezione appropriati.

Prima di applicare il criterio, è necessario apportare le modifiche necessarie agli utenti o ai gruppi locali utilizzati nella configurazione del criterio della directory dei file; in caso contrario, il processo di applicazione non riesce.

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

Creare un descrittore di protezione NTFS

La creazione di un descrittore di sicurezza NTFS (policy di sicurezza dei file) è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo degli accessi NTFS (ACL) a file e cartelle che risiedono nelle macchine virtuali di storage (SVM). È possibile associare il descrittore di protezione al percorso di file o cartelle in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Aggiungere le voci di controllo dell'accesso DACL NTFS al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) al descrittore di protezione NTFS è il secondo passo nella configurazione e nell'applicazione di ACL NTFS a un file o a una cartella. Ciascuna voce identifica l'oggetto a cui è consentito o negato l'accesso e definisce le operazioni che l'oggetto può o non può eseguire nei file o nelle cartelle definiti nell'ACE.

A proposito di questa attività

È possibile aggiungere uno o più ACE al DACL del descrittore di protezione.

Se il descrittore di protezione contiene un DACL con ACE esistenti, il comando aggiunge il nuovo ACE al DACL. Se il descrittore di protezione non contiene un DACL, il comando crea il DACL e aggiunge il nuovo ACE.

È possibile personalizzare le voci DACL specificando i diritti che si desidera consentire o negare per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)

> Se non si specificano i diritti per la voce DACL, l'impostazione predefinita è impostare i diritti su `Full Control`.

È possibile personalizzare le voci DACL specificando come applicare l'ereditarietà.

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere una voce DACL a un descrittore di protezione: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verificare che la voce DACL sia corretta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                    Vserver: vs1
     Security Descriptor Name: sd1
                Allow or Deny: deny
          Account Name or SID: DOMAIN\joe
                Access Rights: full-control
       Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

Creare policy di sicurezza

La creazione di una policy di sicurezza dei file per le SVM è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare i criteri di protezione a ogni SVM (contenente volumi di sicurezza NTFS o volumi di sicurezza misti).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può

essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, 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.

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

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

Quando si aggiungono attività ai criteri di protezione, è necessario specificare i seguenti quattro parametri richiesti:

- Nome SVM
- Nome policy
- Percorso
- Descrittore di sicurezza da associare al percorso

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori

informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Applicare le policy di sicurezza

L'applicazione di una policy di sicurezza dei file alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificare la sicurezza del file applicata

È possibile verificare le impostazioni di sicurezza del file per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione abbiano le impostazioni desiderate.

A proposito di questa attività

Specificare il nome della SVM contenente i dati e il percorso del file e delle cartelle in cui si desidera verificare le impostazioni di sicurezza. È possibile utilizzare il opzionale `-expand-mask` per visualizzare informazioni dettagliate sulle impostazioni di sicurezza.

Fase

1. Visualizzare le impostazioni di sicurezza di file e cartelle: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   ```

-expand-mask true

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
```

```
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
```

```
                                .... ...0 .... .... .... .... .... .... =
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI

È necessario eseguire diversi passaggi per applicare i criteri di controllo a file e cartelle NTFS quando si utilizza l'interfaccia utente di ONTAP. Innanzitutto, si crea un descrittore di protezione NTFS e si aggiungono SACL al descrittore di protezione. Quindi, creare una policy di sicurezza e aggiungere attività di policy. Quindi, applicare il criterio di protezione a una macchina virtuale di storage (SVM).

A proposito di questa attività

Dopo aver applicato il criterio di protezione, è possibile monitorare il processo di criteri di protezione e verificare le impostazioni per il criterio di controllo applicato.

Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Informazioni correlate

Protezione dell'accesso ai file mediante Storage-Level Access Guard

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

"Controllo SMB e NFS e tracciamento della sicurezza"

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

Creare un descrittore di protezione NTFS

La creazione di un criterio di audit del descrittore di protezione NTFS è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo di accesso (ACL) NTFS a file e cartelle che risiedono all'interno delle SVM. Il descrittore di protezione verrà associato al percorso del file o della cartella in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario

- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Se si desidera utilizzare i parametri avanzati, impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Creare un descrittore di sicurezza: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verificare che la configurazione del descrittore di protezione sia corretta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

   ```
                                       Vserver: vs1
                           Security Descriptor Name: sd1
                     Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se si è nel livello di privilegio avanzato, tornare al livello di privilegio admin: `set -privilege admin`

Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) SACL (elenco di controllo di accesso al sistema) al descrittore di protezione NTFS è la seconda fase della creazione di criteri di controllo NTFS per file o cartelle in SVM. Ogni voce identifica l'utente o il gruppo che si desidera controllare. La voce SACL definisce se si desidera controllare i tentativi di accesso riusciti o non riusciti.

A proposito di questa attività

È possibile aggiungere uno o più ACE al SACL del descrittore di protezione.

Se il descrittore di protezione contiene un SACL con ACE esistenti, il comando aggiunge il nuovo ACE al SACL. Se il descrittore di protezione non contiene un SACL, il comando crea il SACL e aggiunge il nuovo ACE.

È possibile configurare le voci SACL specificando i diritti da controllare per gli eventi di successo o di errore per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)

Se non si specificano i diritti per la voce SACL, l'impostazione predefinita è `Full Control`.

È possibile personalizzare le voci SACL specificando come applicare l'ereditarietà con `apply to` parametro. Se non si specifica questo parametro, l'impostazione predefinita prevede l'applicazione di questa voce SACL a questa cartella, sottocartelle e file.

Fasi

1. Aggiungere una voce SACL a un descrittore di protezione: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verificare che la voce SACL sia corretta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                  Vserver: vs1
                   Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                     Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Creare policy di sicurezza

La creazione di un criterio di audit per le macchine virtuali di storage (SVM) è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare la policy di sicurezza a ciascuna macchina virtuale di storage (SVM) (contenente volumi di sicurezza NTFS o volumi misti di sicurezza).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, 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.

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

Non assegnerà mai autorizzazioni di accesso aggiuntive.

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Applicare le policy di sicurezza

L'applicazione di un criterio di audit alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificare la policy di audit applicata

È possibile verificare il criterio di controllo per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione

dispongano delle impostazioni di sicurezza di controllo desiderate.

A proposito di questa attività

Si utilizza `vserver security file-directory show` comando per visualizzare le informazioni sui criteri di controllo. Specificare il nome della SVM che contiene i dati e il percorso dei dati di cui si desidera visualizzare le informazioni sui criteri di controllo del file o della cartella.

Fase

1. Visualizzare le impostazioni dei criteri di controllo: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Esempio

Il seguente comando visualizza le informazioni di policy di audit applicate al percorso "/corp" in SVM vs1. Il percorso ha applicato sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA:

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

                Vserver: vs1
              File Path: /corp
         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:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerazioni per la gestione dei processi di policy di sicurezza

Se esiste un processo di policy di sicurezza, in determinate circostanze non è possibile modificare tale policy o le attività assegnate a tale policy. È necessario comprendere in quali condizioni è possibile o meno modificare le policy di sicurezza in modo che i

tentativi di modifica vengano eseguiti correttamente. Le modifiche al criterio includono l'aggiunta, la rimozione o la modifica delle attività assegnate al criterio e l'eliminazione o la modifica del criterio.

Non è possibile modificare un criterio di protezione o un'attività assegnata a tale criterio se esiste un processo per tale criterio e tale processo si trova nei seguenti stati:

- Il lavoro è in esecuzione o in corso.
- Il processo viene messo in pausa.
- Il lavoro viene ripreso e si trova in esecuzione.
- Se il processo è in attesa di eseguire il failover su un altro nodo.

Nei seguenti casi, se esiste un processo per un criterio di protezione, è possibile modificare correttamente tale criterio di protezione o un'attività assegnata a tale criterio:

- Il processo di policy viene arrestato.
- Il processo di policy è stato completato correttamente.

Comandi per la gestione dei descrittori di sicurezza NTFS

Esistono comandi ONTAP specifici per la gestione dei descrittori di protezione. È possibile creare, modificare, eliminare e visualizzare informazioni sui descrittori di protezione.

Se si desidera…	Utilizzare questo comando…
Creare descrittori di protezione NTFS	`vserver security file-directory ntfs create`
Modificare i descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs modify`
Visualizza informazioni sui descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs show`
Eliminare i descrittori di protezione NTFS	`vserver security file-directory ntfs delete`

Vedere le pagine man per `vserver security file-directory ntfs` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS DACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi DACL (Access Control). È possibile aggiungere ACE ai DACL NTFS in qualsiasi momento. È inoltre possibile gestire i DACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei DACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai DACL NTFS	`vserver security file-directory ntfs dacl add`
Modificare gli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl modify`
Visualizza le informazioni sugli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl show`
Rimuovere gli ACE esistenti dai DACL NTFS	`vserver security file-directory ntfs dacl remove`

Vedere le pagine man per `vserver security file-directory ntfs dacl` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS SACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi SACL (ACE). È possibile aggiungere ACE ai SACL NTFS in qualsiasi momento. È inoltre possibile gestire i SACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei SACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai SACL NTFS	`vserver security file-directory ntfs sacl add`
Modificare gli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl modify`
Visualizza le informazioni sugli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl show`
Rimuovere gli ACE esistenti dai SACL NTFS	`vserver security file-directory ntfs sacl remove`

Vedere le pagine man per `vserver security file-directory ntfs sacl` per ulteriori informazioni.

Comandi per la gestione delle policy di sicurezza

Esistono comandi ONTAP specifici per la gestione delle policy di sicurezza. È possibile visualizzare informazioni sui criteri ed eliminare i criteri. Non è possibile modificare un criterio di protezione.

Se si desidera…	Utilizzare questo comando…
Creare policy di sicurezza	`vserver security file-directory policy create`
Visualizzare informazioni sulle policy di sicurezza	`vserver security file-directory policy show`
Eliminare le policy di sicurezza	`vserver security file-directory policy delete`

Vedere le pagine man per `vserver security file-directory policy` per ulteriori informazioni.

Comandi per la gestione delle attività dei criteri di protezione

Sono disponibili comandi ONTAP per aggiungere, modificare, rimuovere e visualizzare informazioni sulle attività dei criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Aggiungere attività di policy di sicurezza	`vserver security file-directory policy task add`
Modificare le attività dei criteri di protezione	`vserver security file-directory policy task modify`
Visualizza informazioni sulle attività dei criteri di protezione	`vserver security file-directory policy task show`
Rimuovere le attività dei criteri di protezione	`vserver security file-directory policy task remove`

Vedere le pagine man per `vserver security file-directory policy task` per ulteriori informazioni.

Comandi per la gestione dei processi di policy di sicurezza

Sono disponibili comandi ONTAP per mettere in pausa, riprendere, arrestare e visualizzare informazioni sui processi relativi ai criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Sospendere i processi di policy di sicurezza	`vserver security file-directory job pause -vserver vserver_name -id integer`
Riprendere i processi di policy di sicurezza	`vserver security file-directory job resume -vserver vserver_name -id integer`

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni sui processi di policy di sicurezza	`vserver security file-directory job show -vserver vserver_name` È possibile determinare l'ID lavoro di un lavoro utilizzando questo comando.
Arrestare i processi di policy di sicurezza	`vserver security file-directory job stop -vserver vserver_name -id integer`

Vedere le pagine man per `vserver security file-directory job` per ulteriori informazioni.

Configurare la cache dei metadati per le condivisioni SMB

Come funziona il caching dei metadati SMB

Il caching dei metadati consente il caching degli attributi dei file sui client SMB 1.0 per fornire un accesso più rapido agli attributi di file e cartelle. È possibile attivare o disattivare il caching degli attributi in base alla condivisione. È inoltre possibile configurare il time-to-live per le voci memorizzate nella cache se è attivata la cache dei metadati. La configurazione del caching dei metadati non è necessaria se i client si connettono alle condivisioni tramite SMB 2.x o SMB 3.0.

Quando questa opzione è attivata, la cache dei metadati SMB memorizza i dati di attributi di percorso e file per un periodo di tempo limitato. Ciò può migliorare le performance delle PMI per i client SMB 1.0 con carichi di lavoro comuni.

Per alcune attività, SMB crea una quantità significativa di traffico che può includere più query identiche per i metadati di percorso e file. È possibile ridurre il numero di query ridondanti e migliorare le performance per i client SMB 1.0 utilizzando il caching dei metadati SMB per recuperare le informazioni dalla cache.

> Sebbene improbabile, è possibile che la cache dei metadati serva informazioni obsolete ai client SMB 1.0. Se il tuo ambiente non può permettersi questo rischio, non dovresti attivare questa funzionalità.

Attivare la cache dei metadati SMB

È possibile migliorare le performance SMB per i client SMB 1.0 attivando la cache dei metadati SMB. Per impostazione predefinita, il caching dei metadati SMB è disattivato.

Fase

1. Eseguire l'azione desiderata:

Se si desidera…	Immettere il comando…
Attiva il caching dei metadati SMB quando crei una condivisione	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
Abilitare il caching dei metadati SMB su una condivisione esistente	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Informazioni correlate

Configurazione della durata delle voci della cache dei metadati SMB

Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente

Configurare la durata delle voci della cache dei metadati SMB

È possibile configurare la durata delle voci della cache dei metadati SMB per ottimizzare le prestazioni della cache dei metadati SMB nel proprio ambiente. L'impostazione predefinita è 10 secondi.

Prima di iniziare

È necessario aver attivato la funzione cache dei metadati SMB. Se il caching dei metadati SMB non è attivato, l'impostazione TTL della cache SMB non viene utilizzata.

Fase

1. Eseguire l'azione desiderata:

Se si desidera configurare la durata delle voci della cache dei metadati SMB quando…	Immettere il comando…
Creare una condivisione	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Modificare una condivisione esistente	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

È possibile specificare ulteriori proprietà e opzioni di configurazione della condivisione quando si creano o modificano le condivisioni. Per ulteriori informazioni, consulta le pagine man.

Gestire i blocchi dei file

Informazioni sul blocco dei file tra protocolli

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

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

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

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

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

    Il file verrà rimosso dopo l'ultima chiusura.
  - Le operazioni di scollegamento NFS non sono supportate.

    Non è supportato perché sono necessarie semantiche NTFS e SMB e l'ultima operazione Delete-on-Close non è supportata per NFS.
  - Per i filesystem UNIX, è supportata l'operazione di scollegamento.

    È supportato perché sono richieste semantiche NFS e UNIX.
- Rinominare
  - Per i file system NTFS, se il file di destinazione viene aperto da SMB o CIFS, il file di destinazione può essere rinominato.
  - La ridenominazione NFS non è supportata.

    Non è supportato perché sono necessarie semantiche NTFS e SMB.

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

Come ONTAP tratta i bit di sola lettura

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

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

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

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

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

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

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

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

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

Per evitare problemi causati dalla ridenominazione dei componenti del percorso, è possibile applicare impostazioni di sicurezza che impediscono agli utenti o alle applicazioni di rinominare le directory critiche.

Visualizza informazioni sui blocchi

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

A proposito di questa attività

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

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

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

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

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

Fase

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

Esempi

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

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

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

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
```

```
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Blocchi di interruzione

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

A proposito di questa attività

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

Fasi

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

   La pagina man del comando contiene informazioni dettagliate.

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

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

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

Monitorare l'attività delle PMI

Visualizzare le informazioni sulla sessione SMB

È possibile visualizzare informazioni sulle sessioni SMB stabilite, tra cui la connessione SMB, l'ID della sessione e l'indirizzo IP della workstation che utilizza la sessione. È possibile visualizzare informazioni sulla versione del protocollo SMB della sessione e sul livello di protezione continuamente disponibile, per identificare se la sessione supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare le informazioni relative a tutte le sessioni della SVM in forma di riepilogo. Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali:

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output relativo ai campi scelti.

È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sulle sessioni SMB stabilite.
- È possibile utilizzare `-fields` o il `-instance` parametro da solo o in combinazione con altri parametri opzionali.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le informazioni sulla sessione SMB…	**Immettere il seguente comando…**
Per tutte le sessioni su SVM in forma di riepilogo	`vserver cifs session show -vserver vserver_name`
Su un ID di connessione specificato	`vserver cifs session show -vserver vserver_name -connection-id integer`
Da un indirizzo IP della workstation specificato	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Su un indirizzo IP LIF specificato	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Su un nodo specificato	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Da un utente Windows specificato
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Con un meccanismo di autenticazione specificato
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Con una versione del protocollo specificata	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
SMB3	SMB3_1}`  [NOTE] ==== La protezione a disponibilità continua e SMB Multichannel sono disponibili solo su SMB 3.0 e sessioni successive. Per visualizzarne lo stato in tutte le sessioni qualificanti, specificare questo parametro con il valore impostato su `SMB3` o versioni successive. ====
Con un livello specifico di protezione a disponibilità continua	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Se lo stato di disponibilità continua è `Partial`, questo significa che la sessione contiene almeno un file aperto a disponibilità continua, ma la sessione ha alcuni file che non sono aperti con una protezione continuamente disponibile. È possibile utilizzare `vserver cifs sessions file show` comando per determinare quali file della sessione stabilita non sono aperti con una protezione continuamente disponibile. ====
Con uno stato di sessione SMB Signing specificato	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Esempi

Il seguente comando visualizza le informazioni sulla sessione per le sessioni su SVM vs1 stabilite da una workstation con indirizzo IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

Il seguente comando visualizza informazioni dettagliate sulla sessione per le sessioni con protezione continuamente disponibile su SVM vs1. La connessione è stata effettuata utilizzando l’account di dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Il seguente comando visualizza le informazioni di sessione su una sessione che utilizza SMB 3.0 e SMB Multichannel su SVM vs1. Nell'esempio, l'utente si è connesso a questa condivisione da un client SMB 3.0 utilizzando l'indirizzo IP LIF; pertanto, il meccanismo di autenticazione è stato impostato su NTLMv2 per impostazione predefinita. La connessione deve essere effettuata utilizzando l'autenticazione Kerberos per connettersi con la protezione continuamente disponibile.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informazioni correlate

Visualizzazione delle informazioni sui file SMB aperti

Visualizzare le informazioni sui file SMB aperti

È possibile visualizzare informazioni sui file SMB aperti, tra cui la connessione SMB e l'ID sessione, il volume di hosting, il nome della condivisione e il percorso di condivisione. È possibile visualizzare informazioni sul livello di protezione continuamente disponibile di un file, utile per determinare se un file aperto si trova in uno stato che supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare informazioni sui file aperti in una sessione SMB stabilita. Le informazioni visualizzate sono utili quando è necessario determinare le informazioni della sessione SMB per determinati file all'interno di una sessione SMB.

Ad esempio, se si dispone di una sessione SMB in cui alcuni dei file aperti sono aperti con una protezione continuamente disponibile e alcuni non sono aperti con una protezione continuamente disponibile (il valore per `-continuously-available` campo in `vserver cifs session show` l'output del comando è `Partial`), è possibile determinare quali file non sono continuamente disponibili utilizzando questo comando.

È possibile visualizzare le informazioni relative a tutti i file aperti nelle sessioni SMB stabilite sulle macchine virtuali di storage (SVM) in forma riepilogativa utilizzando `vserver cifs session file show` senza

parametri opzionali.

Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Ciò può essere utile quando si desidera visualizzare informazioni solo per un piccolo sottoinsieme di file aperti.

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output nei campi scelti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sui file SMB aperti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
Sul modulo SVM in forma di riepilogo	`vserver cifs session file show -vserver vserver_name`
Su un nodo specificato	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Su un ID file specificato
`vserver cifs session file show -vserver vserver_name -file-id integer`	Su un ID connessione SMB specificato
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Su un ID sessione SMB specificato
`vserver cifs session file show -vserver vserver_name -session-id integer`	Sull'aggregato di hosting specificato
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Sul volume specificato
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Sulla condivisione SMB specificata

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	Sul percorso SMB specificato
`vserver cifs session file show -vserver vserver_name -path path`	Con il livello specificato di protezione a disponibilità continua
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Se lo stato di disponibilità continua è `No`, questo significa che questi file aperti non sono in grado di eseguire il ripristino senza interruzioni dal takeover e dal giveback. Inoltre, non possono essere ripristinati dal trasferimento generale di aggregati tra partner in una relazione ad alta disponibilità. ====
Con lo stato di riconnessione specificato	`vserver cifs session file show -vserver vserver_name -reconnected {No

Sono disponibili ulteriori parametri opzionali che è possibile utilizzare per perfezionare i risultati di output. Per ulteriori informazioni, consulta la pagina man.

Esempi

Nell'esempio seguente vengono visualizzate informazioni sui file aperti su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sui file SMB aperti con ID file 82 su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informazioni correlate

Visualizzazione delle informazioni sulla sessione SMB

Determinare quali oggetti e contatori statistici sono disponibili

Prima di ottenere informazioni su CIFS, SMB, audit e statistiche hash BranchCache e monitorare le performance, è necessario sapere quali oggetti e contatori sono disponibili per ottenere i dati.

Fasi

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

Se si desidera determinare…	Inserisci…
Quali oggetti sono disponibili	`statistics catalog object show`
Oggetti specifici disponibili	`statistics catalog object show object object_name`
Quali contatori sono disponibili	`statistics catalog counter show object object_name`

   Per ulteriori informazioni sugli oggetti e i contatori disponibili, consultare le pagine man.

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

Esempi

Il seguente comando visualizza le descrizioni degli oggetti statistici selezionati relativi all'accesso CIFS e SMB nel cluster, come si vede al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Il seguente comando visualizza informazioni su alcuni contatori di `cifs` oggetto visto a livello di privilegi avanzati:

In questo esempio non vengono visualizzati tutti i contatori disponibili per `cifs` oggetto; l'output è troncato.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                      2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informazioni correlate

Visualizzazione delle statistiche

Visualizzare le statistiche

È possibile visualizzare varie statistiche, tra cui statistiche su CIFS e SMB, audit e hash di BranchCache, per monitorare le performance e diagnosticare i problemi.

Prima di iniziare

È necessario aver raccolto campioni di dati utilizzando `statistics start` e. `statistics stop` prima di poter visualizzare informazioni sugli oggetti.

Fasi

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

Se si desidera visualizzare le statistiche per…	Inserisci…
Tutte le versioni di SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x e SMB 3.0	`statistics show -object smb2`
Sottosistema CIFS del nodo	`statistics show -object nblade_cifs`
Audit multiprotocollo	`statistics show -object audit_ng`
Servizio hash BranchCache	`statistics show -object hashd`
DNS dinamico	`statistics show -object ddns_update`

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

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

Informazioni correlate

Determinazione degli oggetti e dei contatori delle statistiche disponibili

Monitoraggio delle statistiche delle sessioni firmate SMB

Visualizzazione delle statistiche di BranchCache

Utilizzo delle statistiche per monitorare l'attività di riferimento automatico del nodo

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

"Configurazione del monitoraggio delle performance"