# Gestire i server SMB

ONTAP 9

NetApp
April 24, 2024

# Sommario

# Gestire i server SMB

## Modificare i server SMB

È possibile spostare un server SMB da un gruppo di lavoro a un dominio Active Directory, da un gruppo di lavoro a un altro gruppo di lavoro o da un dominio Active Directory a un gruppo di lavoro utilizzando `vserver cifs modify` comando.

**A proposito di questa attività**

È inoltre possibile modificare altri attributi del server SMB, ad esempio il nome del server SMB e lo stato amministrativo. Per ulteriori informazioni, consulta la pagina man.

**Scelte**

- Spostare il server SMB da un gruppo di lavoro a un dominio Active Directory:

  a. Impostare lo stato amministrativo del server SMB su `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Spostare il server SMB dal gruppo di lavoro a un dominio Active Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Per creare un account macchina Active Directory per il server SMB, è necessario fornire il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer a `ou=`*`example`* `ou` container all'interno di `*example*`dominio .com.

  A partire da ONTAP 9.7, l'amministratore ad può fornire un URI a un file keytab in alternativa a un nome e una password a un account Windows con privilegi. Quando si riceve l'URI, includerlo in `-keytab-uri` con il `vserver cifs` comandi.

- Spostare il server SMB da un gruppo di lavoro a un altro gruppo di lavoro:

  a. Impostare lo stato amministrativo del server SMB su `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modificare il gruppo di lavoro per il server SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Spostare il server SMB da un dominio Active Directory a un gruppo di lavoro:

a. Impostare lo stato amministrativo del server SMB su `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Spostare il server SMB dal dominio Active Directory a un gruppo di lavoro: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> Per accedere alla modalità workgroup, tutte le funzioni basate sul dominio devono essere disattivate e la relativa configurazione rimossa automaticamente dal sistema, incluse le condivisioni a disponibilità continua, le copie shadow e AES. Tuttavia, gli ACL delle condivisioni configurati nel dominio, come "EXAMPLE.COM\userName", non funzionano correttamente, ma non possono essere rimossi da ONTAP. Rimuovere questi ACL di condivisione il prima possibile utilizzando strumenti esterni dopo il completamento del comando. Se AES è attivato, potrebbe essere richiesto di fornire il nome e la password di un account Windows con privilegi sufficienti per disattivarlo nel dominio "example.com".

- Modificare gli altri attributi utilizzando il parametro appropriato di `vserver cifs modify` comando.

# Utilizzare le opzioni per personalizzare i server SMB

## Opzioni server SMB disponibili

È utile sapere quali opzioni sono disponibili quando si considera come personalizzare il server SMB. Anche se alcune opzioni sono per uso generale sul server SMB, molte vengono utilizzate per abilitare e configurare funzionalità SMB specifiche. Le opzioni dei server SMB sono controllate con `vserver cifs options modify` opzione.

L'elenco seguente specifica le opzioni del server SMB disponibili a livello di privilegi di amministratore:

- **Configurazione del valore di timeout della sessione SMB**

  La configurazione di questa opzione consente di specificare il numero di secondi di inattività prima della disconnessione di una sessione SMB. Una sessione inattiva è una sessione in cui un utente non ha file o directory aperti sul client. Il valore predefinito è 900 secondi.

- **Configurazione dell'utente UNIX predefinito**

  La configurazione di questa opzione consente di specificare l'utente UNIX predefinito utilizzato dal server SMB. ONTAP crea automaticamente un utente predefinito denominato "pcuser" (con un UID di 65534), crea un gruppo denominato "pcuser" (con un GID di 65534) e aggiunge l'utente predefinito al gruppo "pcuser". Quando si crea un server SMB, ONTAP configura automaticamente "pcuser" come utente UNIX predefinito.

- **Configurazione dell'utente UNIX guest**

La configurazione di questa opzione consente di specificare il nome di un utente UNIX a cui vengono mappati gli utenti che accedono da domini non attendibili, consentendo a un utente di un dominio non attendibile di connettersi al server SMB. Per impostazione predefinita, questa opzione non è configurata (non esiste alcun valore predefinito); pertanto, l'impostazione predefinita è di non consentire agli utenti di domini non attendibili di connettersi al server SMB.

- **Abilitazione o disabilitazione dell'esecuzione della concessione in lettura per i bit di modalità**

  L'attivazione o la disattivazione di questa opzione consente di specificare se consentire ai client SMB di eseguire file eseguibili con bit in modalità UNIX ai quali hanno accesso in lettura, anche quando il bit eseguibile UNIX non è impostato. Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione della possibilità di eliminare i file di sola lettura dai client NFS**

  L'attivazione o la disattivazione di questa opzione determina se consentire ai client NFS di eliminare file o cartelle con il set di attributi di sola lettura. La semantica di eliminazione NTFS non consente l'eliminazione di un file o di una cartella quando viene impostato l'attributo di sola lettura. La semantica di eliminazione di UNIX ignora il bit di sola lettura, utilizzando invece le autorizzazioni della directory principale per determinare se un file o una cartella può essere eliminata. L'impostazione predefinita è `disabled`, Che determina la semantica di eliminazione di NTFS.

- **Configurazione degli indirizzi del server Windows Internet Name Service**

  La configurazione di questa opzione consente di specificare un elenco di indirizzi del server WINS (Windows Internet Name Service) come elenco delimitato da virgole. Specificare gli indirizzi IPv4. Gli indirizzi IPv6 non sono supportati. Non esiste alcun valore predefinito.

L'elenco seguente specifica le opzioni del server SMB disponibili al livello di privilegio avanzato:

- **Concessione delle autorizzazioni di gruppo UNIX agli utenti CIFS**

  La configurazione di questa opzione determina se all'utente CIFS in entrata che non è il proprietario del file può essere concessa l'autorizzazione di gruppo. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `true`, quindi viene concessa l'autorizzazione di gruppo per il file. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `false`, Quindi, le normali regole UNIX sono applicabili per concedere l'autorizzazione al file. Questo parametro è applicabile ai file di sicurezza UNIX con autorizzazione impostata su `mode bits` E non è applicabile ai file con la modalità di sicurezza NTFS o NFSv4. L'impostazione predefinita è `false`.

- **Abilitazione o disabilitazione di SMB 1.0**

  SMB 1.0 è disattivato per impostazione predefinita su una SVM per la quale viene creato un server SMB in ONTAP 9.3.

  > A partire da ONTAP 9.3, SMB 1.0 è disattivato per impostazione predefinita per i nuovi server SMB creati in ONTAP 9.3. È necessario migrare a una versione SMB più recente il prima possibile per prepararsi ai miglioramenti di sicurezza e conformità. Per ulteriori informazioni, contatta il tuo rappresentante NetApp.

- **Abilitazione o disabilitazione di SMB 2.x**

  SMB 2.0 è la versione SMB minima che supporta il failover LIF. Se si disattiva SMB 2.x, anche ONTAP disattiva automaticamente SMB 3.X.

SMB 2.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.0**

  SMB 3.0 è la versione SMB minima che supporta le condivisioni a disponibilità continua. Windows Server 2012 e Windows 8 sono le versioni minime di Windows che supportano SMB 3.0.

  SMB 3.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.1**

  Windows 10 è l'unica versione di Windows che supporta SMB 3.1.

  SMB 3.1 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione dell'offload delle copie ODX**

  L'offload delle copie ODX viene utilizzato automaticamente dai client Windows che lo supportano. Questa opzione è attivata per impostazione predefinita.

- **Abilitazione o disabilitazione del meccanismo di copia diretta per l'offload delle copie ODX**

  Il meccanismo di copia diretta aumenta le prestazioni dell'operazione di offload delle copie quando i client Windows tentano di aprire il file di origine di una copia in una modalità che impedisce la modifica del file mentre la copia è in corso. Per impostazione predefinita, il meccanismo di copia diretta è attivato.

- **Abilitazione o disabilitazione dei riferimenti automatici ai nodi**

  Con i riferimenti automatici ai nodi, il server SMB fa automaticamente riferimento ai client a una LIF di dati locale al nodo che ospita i dati a cui si accede attraverso la condivisione richiesta.

- **Attivazione o disattivazione delle policy di esportazione per SMB**

  Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione dell'utilizzo dei punti di giunzione come punti di analisi**

  Se questa opzione è attivata, il server SMB espone i punti di giunzione ai client SMB come punti di analisi. Questa opzione è valida solo per connessioni SMB 2.x o SMB 3.0. Questa opzione è attivata per impostazione predefinita.

  Questa opzione è supportata solo sulle SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione del numero massimo di operazioni simultanee per connessione TCP**

  Il valore predefinito è 255.

- **Abilitazione o disabilitazione della funzionalità locale di utenti e gruppi Windows**

  Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione dell'autenticazione degli utenti Windows locali**

  Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione della funzionalità di copia shadow VSS**

ONTAP utilizza la funzionalità di copia shadow per eseguire backup remoti dei dati memorizzati utilizzando la soluzione Hyper-V su SMB.

Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione della profondità della directory della copia shadow**

  La configurazione di questa opzione consente di definire la profondità massima delle directory in cui creare copie shadow quando si utilizza la funzionalità di copia shadow.

  Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Attivazione o disattivazione delle funzionalità di ricerca multidominio per la mappatura dei nomi**

  Se questa opzione è attivata, quando un utente UNIX viene mappato a un utente di dominio Windows utilizzando un carattere jolly (*) nella parte di dominio del nome utente Windows (ad esempio, * joe), ONTAP ricerca l'utente specificato in tutti i domini con trust bidirezionali nel dominio principale. Il dominio principale è il dominio che contiene l'account del computer del server SMB.

  In alternativa alla ricerca di tutti i domini trusted bidirezionalmente, è possibile configurare un elenco di domini trusted preferiti. Se questa opzione è attivata e viene configurato un elenco preferito, l'elenco preferito viene utilizzato per eseguire ricerche di mappatura dei nomi di più domini.

  L'impostazione predefinita prevede l'attivazione delle ricerche di associazione dei nomi a più domini.

- **Configurazione della dimensione del settore del file system**

  La configurazione di questa opzione consente di configurare la dimensione del settore del file system in byte che ONTAP invia ai client SMB. Sono disponibili due valori validi per questa opzione: `4096` e. `512`. Il valore predefinito è `4096`. Potrebbe essere necessario impostare questo valore su `512` Se l'applicazione Windows supporta solo una dimensione di settore di 512 byte.

- **Attivazione o disattivazione del controllo dinamico degli accessi**

  L'attivazione di questa opzione consente di proteggere gli oggetti sul server SMB utilizzando il controllo dinamico dell'accesso (DAC), incluso l'utilizzo del controllo per organizzare i criteri di accesso centrali e l'utilizzo degli oggetti Criteri di gruppo per implementare i criteri di accesso centrali. L'opzione è disattivata per impostazione predefinita.

  Questa opzione è supportata solo sulle SVM.

- **Impostazione delle restrizioni di accesso per le sessioni non autenticate (limitazione anonima)**

  L'impostazione di questa opzione determina le restrizioni di accesso per le sessioni non autenticate. Le restrizioni vengono applicate agli utenti anonimi. Per impostazione predefinita, non esistono restrizioni di accesso per gli utenti anonimi.

- **Abilitazione o disabilitazione della presentazione di ACL NTFS su volumi con sicurezza efficace UNIX (volumi di sicurezza UNIX o volumi di sicurezza misti con sicurezza effettiva UNIX)**

  L'attivazione o la disattivazione di questa opzione determina il modo in cui la sicurezza dei file su file e cartelle con protezione UNIX viene presentata ai client SMB. Se abilitato, ONTAP presenta file e cartelle in volumi con protezione UNIX ai client SMB come dotati di protezione dei file NTFS con ACL NTFS. Se

disattivato, ONTAP presenta i volumi con sicurezza UNIX come volumi FAT, senza alcuna protezione dei file. Per impostazione predefinita, i volumi presentano la protezione dei file NTFS con ACL NTFS.

- **Abilitazione o disabilitazione della funzionalità SMB finta aperta**

  L'abilitazione di questa funzionalità migliora le performance di SMB 2.x e SMB 3.0 ottimizzando il modo in cui ONTAP effettua richieste aperte e ravvicinato quando si esegue una query per ottenere informazioni sugli attributi su file e directory. Per impostazione predefinita, la funzionalità SMB fake open è attivata. Questa opzione è utile solo per le connessioni effettuate con SMB 2.x o versioni successive.

- **Abilitazione o disabilitazione delle estensioni UNIX**

  L'attivazione di questa opzione attiva le estensioni UNIX su un server SMB. Le estensioni UNIX consentono di visualizzare la sicurezza in stile POSIX/UNIX tramite il protocollo SMB. Per impostazione predefinita, questa opzione è disattivata.

  Se si dispone di client SMB basati su UNIX, come i client Mac OSX, è necessario attivare le estensioni UNIX. L'abilitazione delle estensioni UNIX consente al server SMB di trasmettere le informazioni di sicurezza POSIX/UNIX tramite SMB al client basato su UNIX, che quindi traduce le informazioni di sicurezza in sicurezza POSIX/UNIX.

- **Abilitazione o disabilitazione del supporto per le ricerche di nomi brevi**

  L'attivazione di questa opzione consente al server SMB di eseguire ricerche sui nomi brevi. Una query di ricerca con questa opzione attivata tenta di associare 8.3 nomi di file con nomi di file lunghi. Il valore predefinito per questo parametro è `false`.

- **Abilitazione o disabilitazione del supporto per la pubblicità automatica delle funzionalità DFS**

  L'attivazione o la disattivazione di questa opzione determina se i server SMB pubblicizzano automaticamente le funzionalità DFS ai client SMB 2.x e SMB 3.0 che si connettono alle condivisioni. ONTAP utilizza i riferimenti DFS nell'implementazione di collegamenti simbolici per l'accesso SMB. Se attivato, il server SMB comunica sempre le funzionalità DFS indipendentemente dall'attivazione dell'accesso tramite collegamento simbolico. Se disattivato, il server SMB comunica le funzionalità DFS solo quando i client si connettono alle condivisioni in cui è attivato l'accesso al collegamento simbolico.

- **Configurazione del numero massimo di crediti SMB**

  A partire da ONTAP 9.4, configurazione di `-max-credits` L'opzione consente di limitare il numero di crediti da concedere su una connessione SMB quando client e server eseguono SMB versione 2 o successiva. Il valore predefinito è 128.

- **Abilitazione o disabilitazione del supporto per SMB multicanale**

  Attivazione di `-is-multichannel-enabled` L'opzione di ONTAP 9.4 e versioni successive consente al server SMB di stabilire più connessioni per una singola sessione SMB quando vengono implementate le NIC appropriate sul cluster e sui relativi client. In questo modo si migliora il throughput e la tolleranza agli errori. Il valore predefinito per questo parametro è `false`.

  Quando SMB Multichannel è attivato, è anche possibile specificare i seguenti parametri:

  - Numero massimo di connessioni consentite per sessione multicanale. Il valore predefinito per questo parametro è 32.
  - Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. Il valore predefinito per questo parametro è 256.

## Configurazione delle opzioni del server SMB

È possibile configurare le opzioni del server SMB in qualsiasi momento dopo aver creato un server SMB su una macchina virtuale di storage (SVM).

**Fase**

1. Eseguire l'azione desiderata:

| Se si desidera configurare le opzioni del server SMB… | Immettere il comando… |
|---|---|
| A livello di privilegi di amministratore | `vserver cifs options modify -vserver` *`vserver_name options`* |
| A livello di privilegi avanzati | a. `set -privilege advanced`<br>b. `vserver cifs options modify -vserver` *`vserver_name options`*<br>c. `set -privilege admin` |

Per ulteriori informazioni sulla configurazione delle opzioni del server SMB, consultare la pagina man del `vserver cifs options modify` comando.

## Configurare l'autorizzazione Grant UNIX group per gli utenti SMB

È possibile configurare questa opzione in modo da concedere ai gruppi le autorizzazioni di accesso ai file o alle directory anche se l'utente SMB in entrata non è il proprietario del file.

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'autorizzazione Grant UNIX group come appropriato:

| Se lo si desidera | Immettere il comando |
|---|---|
| Abilitare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file | `vserver cifs options modify –grant-unix-group-perms-to-others true` |
| Disattivare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file | `vserver cifs options modify –grant-unix-group-perms-to-others false` |

3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Tornare al livello di privilegio admin: `set -privilege admin`

## Configurare le restrizioni di accesso per gli utenti anonimi

Per impostazione predefinita, un utente anonimo e non autenticato (noto anche come *null user*) può accedere a determinate informazioni sulla rete. È possibile utilizzare un'opzione del server SMB per configurare le restrizioni di accesso per l'utente anonimo.

#### A proposito di questa attività

Il `-restrict-anonymous` L'opzione del server SMB corrisponde a. `RestrictAnonymous` Voce di registro in Windows.

Gli utenti anonimi possono elencare o enumerare determinati tipi di informazioni di sistema dagli host Windows sulla rete, inclusi i nomi e i dettagli degli utenti, i criteri degli account e i nomi di condivisione. È possibile controllare l'accesso per l'utente anonimo specificando una delle tre impostazioni di restrizione dell'accesso:

| Valore | Descrizione |
|---|---|
| `no-restriction` (impostazione predefinita) | Non specifica restrizioni di accesso per utenti anonimi. |
| `no-enumeration` | Specifica che solo l'enumerazione è limitata per gli utenti anonimi. |
| `no-access` | Specifica che l'accesso è limitato agli utenti anonimi. |

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'impostazione limita anonimo: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver` *`vserver_name`*
4. Tornare al livello di privilegio admin: `set -privilege admin`

#### Informazioni correlate

Opzioni server SMB disponibili

## Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX

#### Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per una panoramica dei dati in stile di sicurezza UNIX

Puoi scegliere come presentare la sicurezza dei file ai client SMB per i dati di sicurezza UNIX attivando o disattivando la presentazione degli ACL NTFS ai client SMB. Ogni impostazione offre vantaggi che è necessario comprendere per scegliere l'impostazione più adatta alle proprie esigenze di business.

Per impostazione predefinita, ONTAP presenta le autorizzazioni UNIX sui volumi UNIX di tipo Security ai client SMB come ACL NTFS. Esistono scenari in cui ciò è auspicabile, tra cui:

- Per visualizzare e modificare le autorizzazioni UNIX, utilizzare la scheda **Security** nella casella Proprietà di Windows.

  Non è possibile modificare le autorizzazioni da un client Windows se l'operazione non è consentita dal sistema UNIX. Ad esempio, non è possibile modificare la proprietà di un file non proprietario, perché il sistema UNIX non consente questa operazione. Questa restrizione impedisce ai client SMB di ignorare le autorizzazioni UNIX impostate sui file e sulle cartelle.

- Gli utenti stanno modificando e salvando i file sul volume UNIX di sicurezza utilizzando alcune applicazioni Windows, ad esempio Microsoft Office, in cui ONTAP deve conservare le autorizzazioni UNIX durante le operazioni di salvataggio.
- Nell'ambiente sono presenti alcune applicazioni Windows che prevedono di leggere gli ACL NTFS sui file utilizzati.

In alcuni casi, è possibile disattivare la presentazione delle autorizzazioni UNIX come ACL NTFS. Se questa funzionalità è disattivata, ONTAP presenta i volumi UNIX di sicurezza come volumi FAT ai client SMB. Esistono motivi specifici per cui potresti voler presentare i volumi UNIX di sicurezza come volumi FAT ai client SMB:

- È possibile modificare le autorizzazioni UNIX solo utilizzando i mount sui client UNIX.

  La scheda Security (sicurezza) non è disponibile quando un volume UNIX di tipo Security viene mappato su un client SMB. L'unità mappata sembra essere formattata con il file system FAT, che non dispone di permessi per i file.

- Si stanno utilizzando applicazioni su SMB che impostano ACL NTFS su file e cartelle a cui si accede, il che può verificarsi se i dati risiedono su volumi UNIX di sicurezza.

  Se ONTAP riporta il volume come FAT, l'applicazione non tenta di modificare un ACL.

**Informazioni correlate**

Configurazione degli stili di sicurezza sui volumi FlexVol

Configurazione degli stili di sicurezza sui qtree

### Abilitare o disabilitare la presentazione degli ACL NTFS per i dati di sicurezza UNIX

È possibile attivare o disattivare la presentazione degli ACL NTFS ai client SMB per i dati di sicurezza UNIX (volumi di sicurezza UNIX e volumi di sicurezza misti con protezione efficace UNIX).

**A proposito di questa attività**

Se si attiva questa opzione, ONTAP presenta file e cartelle su volumi con uno stile di sicurezza UNIX efficace ai client SMB come dotati di ACL NTFS. Se si disattiva questa opzione, i volumi vengono presentati come volumi FAT ai client SMB. L'impostazione predefinita prevede la presentazione degli ACL NTFS ai client SMB.

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'impostazione dell'opzione UNIX NTFS ACL: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver` *`vserver_name`*

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

#### In che modo ONTAP conserva le autorizzazioni UNIX

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

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

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

#### Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

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

- Modifica delle autorizzazioni UNIX

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

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

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

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

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

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

l'impostazione di propagazione desiderata.

# Gestire le impostazioni di sicurezza del server SMB

## In che modo ONTAP gestisce l'autenticazione dei client SMB

Prima che gli utenti possano creare connessioni SMB per accedere ai dati contenuti nella SVM, devono essere autenticati dal dominio a cui appartiene il server SMB. Il server SMB supporta due metodi di autenticazione, Kerberos e NTLM (NTLMv1 o NTLMv2). Kerberos è il metodo predefinito utilizzato per autenticare gli utenti del dominio.

### Autenticazione Kerberos

ONTAP supporta l'autenticazione Kerberos durante la creazione di sessioni SMB autenticate.

Kerberos è il servizio di autenticazione principale di Active Directory. Il server Kerberos o il servizio KDC (Kerberos Key Distribution Center) memorizza e recupera informazioni sui principi di sicurezza in Active Directory. A differenza del modello NTLM, i client Active Directory che desiderano stabilire una sessione con un altro computer, ad esempio il server SMB, contattano direttamente un KDC per ottenere le proprie credenziali di sessione.

### Autenticazione NTLM

L'autenticazione del client NTLM viene eseguita utilizzando un protocollo di risposta alle sfide basato sulla conoscenza condivisa di un segreto specifico dell'utente basato su una password.

Se un utente crea una connessione SMB utilizzando un account utente Windows locale, l'autenticazione viene eseguita localmente dal server SMB utilizzando NTLMv2.

## Linee guida per le impostazioni di sicurezza del server SMB in una configurazione di disaster recovery SVM

Prima di creare una SVM configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la `-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), è necessario conoscere il modo in cui le impostazioni di sicurezza del server SMB vengono gestite sulla SVM di destinazione.

- Le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione.

  Quando si crea un server SMB sulla SVM di destinazione, tutte le impostazioni di sicurezza del server SMB vengono impostate sui valori predefiniti. Quando la destinazione di disaster recovery SVM viene inizializzata, aggiornata o risincronizzata, le impostazioni di sicurezza del server SMB sull'origine non vengono replicate nella destinazione.

- È necessario configurare manualmente le impostazioni di sicurezza del server SMB non predefinite.

  Se sono state configurate impostazioni di sicurezza del server SMB non predefinite sulla SVM di origine, è necessario configurare manualmente queste stesse impostazioni sulla SVM di destinazione dopo che la destinazione diventa di lettura/scrittura (dopo che la relazione SnapMirror è stata interrotta).

## Visualizza informazioni sulle impostazioni di sicurezza del server SMB

È possibile visualizzare informazioni sulle impostazioni di sicurezza dei server SMB sulle macchine virtuali dello storage (SVM). È possibile utilizzare queste informazioni per verificare che le impostazioni di protezione siano corrette.

### A proposito di questa attività

Un'impostazione di protezione visualizzata può essere il valore predefinito per quell'oggetto o un valore non predefinito configurato utilizzando l'interfaccia CLI di ONTAP o gli oggetti Criteri di gruppo di Active Directory.

Non utilizzare `vserver cifs security show` Comando per i server SMB in modalità workgroup, perché alcune opzioni non sono valide.

### Fase

1. Eseguire una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su… | Immettere il comando… |
|---|---|
| Tutte le impostazioni di sicurezza su una SVM specificata | `vserver cifs security show -vserver` *`vserver_name`* |
| Una o più impostazioni di sicurezza specifiche sulla SVM | `vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare. |

### Esempio

L'esempio seguente mostra tutte le impostazioni di sicurezza per SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
              Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                    Is AES Encryption Enabled:        false
                       LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                   Is SMB Encryption Required:        false
                      Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Le impostazioni visualizzate dipendono dalla versione di ONTAP in esecuzione.

L'esempio seguente mostra l'inclinazione del clock Kerberos per SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

**Informazioni correlate**

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

## Attiva o disattiva la complessità della password richiesta per gli utenti SMB locali

La complessità richiesta delle password offre una maggiore sicurezza per gli utenti SMB locali sulle vostre macchine virtuali di storage (SVM). La funzione di complessità della password richiesta è attivata per impostazione predefinita. Puoi disattivarlo e riattivarlo in qualsiasi momento.

**Prima di iniziare**

Gli utenti locali, i gruppi locali e l'autenticazione dell'utente locale devono essere abilitati sul server CIFS.

**A proposito di questa attività**

Non utilizzare `vserver cifs security modify` Comando per un server CIFS in modalità gruppo di lavoro perché alcune opzioni non sono valide.

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera che la complessità della password richiesta per gli utenti SMB locali sia… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true` |
| Disattivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false` |

2. Verificare l'impostazione di sicurezza per la complessità della password richiesta: `vserver cifs security show -vserver` *`vserver_name`*

**Esempio**

L'esempio seguente mostra che la complessità della password richiesta è abilitata per gli utenti SMB locali per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

**Informazioni correlate**

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Utilizzo di utenti e gruppi locali per l'autenticazione e l'autorizzazione

Requisiti per le password dell'utente locale

Modifica delle password degli account utente locali

## Modificare le impostazioni di sicurezza Kerberos del server CIFS

È possibile modificare alcune impostazioni di sicurezza Kerberos del server CIFS, tra cui il tempo massimo consentito di disallineamento del clock Kerberos, la durata del ticket Kerberos e il numero massimo di giorni di rinnovo del ticket.

### A proposito di questa attività

Modifica delle impostazioni Kerberos del server CIFS mediante `vserver cifs security modify` Il comando modifica le impostazioni solo sulla singola SVM (Storage Virtual Machine) specificata con `-vserver` parametro. È possibile gestire centralmente le impostazioni di sicurezza Kerberos per tutte le SVM del cluster appartenenti allo stesso dominio Active Directory utilizzando gli oggetti Criteri di gruppo (GPO) di Active Directory.

### Fasi

1. Eseguire una o più delle seguenti operazioni:

| Se si desidera… | Inserisci… |
|---|---|
| Specificare il tempo massimo consentito di inclinazione dell'orologio Kerberos in minuti (9.13.1 e successivi) o secondi (9.12.1 o precedenti). | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`*<br><br>L'impostazione predefinita è 5 minuti. |
| Specificare la durata del ticket Kerberos in ore. | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours`<br><br>L'impostazione predefinita è 10 ore. |
| Specificare il numero massimo di giorni di rinnovo del ticket. | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`*<br><br>L'impostazione predefinita è 7 giorni. |
| Specificare il timeout per i socket sui KDC dopo il quale tutti i KDC sono contrassegnati come irraggiungibili. | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`*<br><br>L'impostazione predefinita è 3 secondi. |

2. Verificare le impostazioni di sicurezza Kerberos:

   `vserver cifs security show -vserver` *`vserver_name`*

### Esempio

Nell'esempio seguente vengono apportate le seguenti modifiche alla sicurezza Kerberos: "Kerberos Clock Skew" (inclinazione clock Kerberos) è impostato su 3 minuti e "Kerberos Ticket Age" (durata ticket Kerberos) è impostato su 8 ore per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                   Kerberos Renewal Age:                    7 days
                   Kerberos KDC Timeout:                    3 seconds
                    Is Signing Required:               false
        Is Password Complexity Required:                true
   Use start_tls For AD LDAP connection:               false
              Is AES Encryption Enabled:               false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
            Is SMB Encryption Required:               false
```

**Informazioni correlate**

"Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS"

"GPO supportati"

"Applicazione di oggetti Criteri di gruppo ai server CIFS"

## Impostare il livello minimo di sicurezza per l'autenticazione del server SMB

È possibile impostare il livello di sicurezza minimo del server SMB, noto anche come *LMCompatibilityLevel*, sul server SMB per soddisfare i requisiti di sicurezza aziendali per l'accesso al client SMB. Il livello di sicurezza minimo è il livello minimo dei token di sicurezza che il server SMB accetta dai client SMB.

**A proposito di questa attività**

- I server SMB in modalità workgroup supportano solo l'autenticazione NTLM. L'autenticazione Kerberos non è supportata.
- LMCompatibilityLevel si applica solo all'autenticazione del client SMB, non all'autenticazione dell'amministratore.

È possibile impostare il livello di sicurezza minimo per l'autenticazione su uno dei quattro livelli di sicurezza supportati.

| Valore | Descrizione |
|---|---|
| `lm-ntlm-ntlmv2-krb` (impostazione predefinita) | La macchina virtuale per lo storage (SVM) accetta la protezione con autenticazione LM, NTLM, NTLMv2 e Kerberos. |

| Valore | Descrizione |
| --- | --- |
| `ntlm-ntlmv2-krb` | SVM accetta la sicurezza di autenticazione NTLM, NTLMv2 e Kerberos. SVM nega l'autenticazione LM. |
| `ntlmv2-krb` | SVM accetta la sicurezza di autenticazione NTLMv2 e Kerberos. SVM nega l'autenticazione LM e NTLM. |
| `krb` | SVM accetta solo la sicurezza con autenticazione Kerberos. SVM nega l'autenticazione LM, NTLM e NTLMv2. |

**Fasi**

1. Impostare il livello minimo di protezione per l'autenticazione: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verificare che il livello di protezione per l'autenticazione sia impostato sul livello desiderato: `vserver cifs security show -vserver` *`vserver_name`*

**Informazioni correlate**

Attivazione o disattivazione della crittografia AES per le comunicazioni basate su Kerberos

## Configurare una protezione avanzata per le comunicazioni basate su Kerberos utilizzando la crittografia AES

Per una maggiore sicurezza con la comunicazione basata su Kerberos, è possibile attivare la crittografia AES-256 e AES-128 sul server SMB. Per impostazione predefinita, quando si crea un server SMB su SVM, la crittografia AES (Advanced Encryption Standard) viene disattivata. È necessario abilitarlo per sfruttare la protezione avanzata fornita dalla crittografia AES.

La comunicazione relativa a Kerberos per SMB viene utilizzata durante la creazione del server SMB sulla SVM e durante la fase di configurazione della sessione SMB. Il server SMB supporta i seguenti tipi di crittografia per le comunicazioni Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se si desidera utilizzare il tipo di crittografia con la massima protezione per le comunicazioni Kerberos, è necessario attivare la crittografia AES per le comunicazioni Kerberos su SVM.

Quando viene creato il server SMB, il controller di dominio crea un account computer in Active Directory. A questo punto, il KDC viene a conoscenza delle funzionalità di crittografia di un determinato account di computer. Successivamente, viene selezionato un particolare tipo di crittografia per crittografare il ticket di servizio che il client presenta al server durante l'autenticazione.

A partire da ONTAP 9.12.1, è possibile specificare i tipi di crittografia da segnalare al KDC di Active Directory

(ad). È possibile utilizzare `-advertised-enc-types` opzione per attivare i tipi di crittografia consigliati ed è possibile utilizzarla per disattivare i tipi di crittografia più deboli. Scopri come "Attiva e disattiva i tipi di crittografia per le comunicazioni basate su Kerberos".

> Intel AES New Instructions (Intel AES NI) è disponibile in SMB 3.0, migliorando l'algoritmo AES e accelerando la crittografia dei dati con le famiglie di processori supportate.a partire da SMB 3.1.1, AES-128-GCM sostituisce AES-128-CCM come algoritmo hash utilizzato dalla crittografia SMB.

**Informazioni correlate**

Modifica delle impostazioni di sicurezza Kerberos del server CIFS

## Attiva o disattiva la crittografia AES per le comunicazioni basate su Kerberos

Per sfruttare al massimo la protezione della comunicazione basata su Kerberos, è necessario utilizzare la crittografia AES-256 e AES-128 sul server SMB. A partire da ONTAP 9.13.1, la crittografia AES è attivata per impostazione predefinita. Se non si desidera che il server SMB selezioni i tipi di crittografia AES per la comunicazione basata su Kerberos con Active Directory (ad) KDC, è possibile disattivare la crittografia AES.

Se la crittografia AES è attivata per impostazione predefinita e se si dispone dell'opzione per specificare i tipi di crittografia, dipende dalla versione di ONTAP in uso.

| Versione di ONTAP | La crittografia AES è abilitata … | È possibile specificare i tipi di crittografia? |
|---|---|---|
| 9.13.1 e versioni successive | Per impostazione predefinita | Sì |
| 9.12.1 | Manualmente | Sì |
| 9.11.1 e precedenti | Manualmente | No |

A partire da ONTAP 9.12.1, la crittografia AES viene attivata e disattivata tramite `-advertised-enc-types` Che consente di specificare i tipi di crittografia annunciati a ad KDC. L'impostazione predefinita è `rc4` e. `des`, Ma quando viene specificato un tipo AES, viene attivata la crittografia AES. È inoltre possibile utilizzare l'opzione per disattivare esplicitamente i tipi di crittografia RC4 e DES più deboli. In ONTAP 9.11.1 e versioni precedenti, è necessario utilizzare `-is-aes-encryption-enabled` Opzione per attivare e disattivare la crittografia AES e i tipi di crittografia non possono essere specificati.

Per migliorare la sicurezza, la macchina virtuale di storage (SVM) modifica la password dell'account della macchina in ad ogni volta che viene modificata l'opzione di sicurezza AES. La modifica della password potrebbe richiedere credenziali amministrative ad per l'unità organizzativa (OU) che contiene l'account del computer.

Se una SVM è configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la `-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione. Se è stata attivata la crittografia AES sulla SVM di origine, è necessario abilitarla manualmente.

**Esempio 1. Fasi**

**ONTAP 9.12.1 e versioni successive**

1. Eseguire una delle seguenti operazioni:

| Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256` |
| Disattivato | `vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4` |

   **Nota:** la `-is-aes-encryption-enabled` L'opzione è obsoleta in ONTAP 9.12.1 e potrebbe essere rimossa in una release successiva.

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

**Esempi**

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

**ONTAP 9.11.1 e versioni precedenti**

1. Eseguire una delle seguenti operazioni:

| Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true` |
| Disattivato | `vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false` |

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Il `is-aes-encryption-enabled` viene visualizzato il campo `true` Se la crittografia AES è attivata e. `false` se è disattivato.

**Esempi**

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

## Utilizza la firma SMB per migliorare la sicurezza di rete

### Utilizza la firma SMB per migliorare la panoramica sulla sicurezza di rete

La firma SMB aiuta a garantire che il traffico di rete tra il server SMB e il client non venga compromesso, evitando attacchi di replay. Per impostazione predefinita, ONTAP supporta la firma SMB quando richiesto dal client. Facoltativamente, l'amministratore dello storage può configurare il server SMB in modo che richieda la firma SMB.

#### In che modo i criteri di firma SMB influiscono sulla comunicazione con un server CIFS

Oltre alle impostazioni di sicurezza della firma SMB del server CIFS, due criteri di firma SMB sui client Windows controllano la firma digitale delle comunicazioni tra i client e il server CIFS. È possibile configurare l'impostazione che soddisfa i requisiti di business.

I criteri SMB dei client sono controllati tramite le impostazioni dei criteri di protezione locali di Windows, che vengono configurate utilizzando Microsoft Management Console (MMC) o gli oggetti Criteri di gruppo di Active Directory. Per ulteriori informazioni sulla firma SMB del client e sui problemi di sicurezza, consultare la documentazione di Microsoft Windows.

Di seguito sono riportate le descrizioni dei due criteri di firma SMB sui client Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Questa impostazione controlla se la funzionalità di firma SMB del client è attivata. È attivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, le comunicazioni del client con il server CIFS dipendono dall'impostazione della firma SMB sul server CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Questa impostazione specifica se il client richiede la firma SMB per comunicare con un server. È disattivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, il comportamento della firma SMB si basa sull'impostazione del criterio per `Microsoft network client: Digitally sign communications (if server agrees)` E l'impostazione sul server CIFS.

> Se l'ambiente include client Windows configurati per richiedere la firma SMB, è necessario attivare la firma SMB sul server CIFS. In caso contrario, il server CIFS non può fornire dati a questi sistemi.

I risultati effettivi delle impostazioni di firma SMB del client e del server CIFS dipendono dal fatto che le sessioni SMB utilizzino SMB 1.0 o SMB 2.x e versioni successive.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 1.0:

| Client | ONTAP - Firma non richiesta | ONTAP—Firma obbligatoria |
|---|---|---|
| Firma disattivata e non richiesta | Non firmato | Firmato |
| Firma abilitata e non richiesta | Non firmato | Firmato |
| Firma disattivata e obbligatoria | Firmato | Firmato |
| Firma abilitata e obbligatoria | Firmato | Firmato |

> I client SMB 1 di Windows meno recenti e alcuni client SMB 1 non Windows potrebbero non riuscire a connettersi se la firma è disattivata sul client ma richiesta sul server CIFS.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 2.x o SMB 3.0:

Per i client SMB 2.x e SMB 3.0, la firma SMB è sempre abilitata. Non può essere disattivato.

| Client | ONTAP - Firma non richiesta | ONTAP—Firma obbligatoria |
|---|---|---|
| Firma non richiesta | Non firmato | Firmato |
| Firma obbligatoria | Firmato | Firmato |

La seguente tabella riassume il comportamento predefinito della firma SMB del client e del server Microsoft:

| Protocollo | Algoritmo hash | Può attivare/disattivare | Può richiedere/non richiedere | Impostazione predefinita del client | Server predefinito | DC predefinito |
|---|---|---|---|---|---|---|
| SMB 1.0 | MD5 | Sì | Sì | Abilitato (non richiesto) | Disattivato (non richiesto) | Obbligatorio |
| SMB 2.x | HMAC SHA-256 | No | Sì | Non richiesto | Non richiesto | Obbligatorio |
| SMB 3.0 | AES-CMAC. | No | Sì | Non richiesto | Non richiesto | Obbligatorio |

Microsoft sconsiglia di utilizzare `Digitally sign communications (if client agrees)` oppure `Digitally sign communications (if server agrees)` Impostazioni di Criteri di gruppo. Microsoft non consiglia più di utilizzare `EnableSecuritySignature` impostazioni del registro di sistema. Queste opzioni influiscono solo sul comportamento di SMB 1 e possono essere sostituite da `Digitally sign communications (always)` Impostazione di Criteri di gruppo o l' `RequireSecuritySignature` impostazione del registro di sistema. È inoltre possibile ottenere ulteriori informazioni dal Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Basics of SMB Signing (informazioni di base sulla firma SMB) (che riguardano sia SMB1 che SMB2)]

**Impatto delle performance della firma SMB**

Quando le sessioni SMB utilizzano la firma SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM contenente il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB firmato. L'offload della firma SMB è attivato per impostazione predefinita quando è attivata la firma SMB.

Le migliori performance di firma SMB richiedono la funzionalità di offload AES-NI. Consultare Hardware Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11

che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della firma SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La maggior parte dei client Windows negozia la firma SMB per impostazione predefinita, se attivata sul server. Se si richiede la protezione SMB per alcuni client Windows e se la firma SMB causa problemi di performance, è possibile disattivare la firma SMB su qualsiasi client Windows che non richieda protezione contro gli attacchi di replay. Per informazioni sulla disattivazione della firma SMB sui client Windows, consultare la documentazione di Microsoft Windows.

#### Consigli per la configurazione della firma SMB

È possibile configurare il comportamento della firma SMB tra i client SMB e il server CIFS per soddisfare i requisiti di sicurezza. Le impostazioni scelte durante la configurazione della firma SMB sul server CIFS dipendono dai requisiti di sicurezza.

È possibile configurare la firma SMB sul client o sul server CIFS. Durante la configurazione della firma SMB, prendere in considerazione i seguenti consigli:

| Se… | Consiglio… |
|---|---|
| Si desidera aumentare la sicurezza della comunicazione tra il client e il server | Rendere necessaria la firma SMB sul client abilitando il `Require Option (Sign always)` impostazione di sicurezza sul client. |
| Si desidera che tutto il traffico SMB verso una determinata macchina virtuale di storage (SVM) sia firmato | Rendere necessaria la firma SMB sul server CIFS configurando le impostazioni di sicurezza in modo che richiedano la firma SMB. |

Per ulteriori informazioni sulla configurazione delle impostazioni di sicurezza del client Windows, consultare la documentazione Microsoft.

#### Linee guida per la firma SMB quando sono configurati LIFS di dati multipli

Se si attiva o disattiva la firma SMB richiesta sul server SMB, è necessario conoscere le linee guida per le configurazioni LIFS di dati multipli per una SVM.

Quando si configura un server SMB, potrebbero essere configurate più LIF di dati. In tal caso, il server DNS contiene più server `A` Registrare le voci per il server CIFS, utilizzando tutti lo stesso nome host del server SMB, ma ciascuna con un indirizzo IP univoco. Ad esempio, un server SMB con due LIF dati configurati potrebbe avere il seguente DNS `A` voci di record:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Il comportamento normale è che, quando si modifica l'impostazione richiesta per la firma SMB, solo le nuove connessioni dai client vengono influenzate dalla modifica dell'impostazione della firma SMB. Tuttavia, esiste un'eccezione a questo comportamento. Esiste un caso in cui un client dispone di una connessione esistente a

una condivisione e il client crea una nuova connessione alla stessa condivisione dopo la modifica dell'impostazione, mantenendo la connessione originale. In questo caso, sia la connessione SMB nuova che quella esistente adottano i nuovi requisiti per la firma SMB.

Si consideri il seguente esempio:

1. Client1 si connette a una condivisione senza la firma SMB richiesta utilizzando il percorso `O:\`.
2. L'amministratore dello storage modifica la configurazione del server SMB per richiedere la firma SMB.
3. Client1 si connette alla stessa condivisione con la firma SMB richiesta utilizzando il percorso `S:\` (mantenendo la connessione utilizzando il percorso `O:\`).
4. Il risultato è che la firma SMB viene utilizzata quando si accede ai dati su entrambi `O:\` e. `S:\` dischi.

### Attiva o disattiva la firma SMB richiesta per il traffico SMB in entrata

È possibile applicare il requisito per i client di firmare i messaggi SMB attivando la firma SMB richiesta. Se attivato, ONTAP accetta i messaggi SMB solo se dispongono di firme valide. Se si desidera consentire la firma SMB, ma non la si desidera, è possibile disattivare la firma SMB richiesta.

#### A proposito di questa attività

Per impostazione predefinita, la firma SMB richiesta è disattivata. È possibile attivare o disattivare la firma SMB richiesta in qualsiasi momento.

> La firma SMB non viene disattivata per impostazione predefinita nei seguenti casi:
>
> 1. La firma SMB richiesta è attivata e il cluster viene reinstallato su una versione di ONTAP che non supporta la firma SMB.
> 2. Il cluster viene successivamente aggiornato a una versione di ONTAP che supporta la firma SMB.
>
>  In queste circostanze, la configurazione della firma SMB originariamente configurata su una versione supportata di ONTAP viene mantenuta attraverso la reversione e il successivo aggiornamento.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), l'impostazione di protezione della firma SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a. `false` (Non-ID-Preserve), l'impostazione di protezione della firma SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la firma SMB richiesta sulla SVM di origine, è necessario attivare manualmente la firma SMB richiesta sulla SVM di destinazione.

#### Fasi

1. Eseguire una delle seguenti operazioni:

| Se si desidera che la firma SMB richiesta sia… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true` |
| Disattivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false` |

2. Verificare che la firma SMB richiesta sia attivata o disattivata determinando se il valore in `Is Signing Required` nell'output del seguente comando viene impostato il valore desiderato: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

**Esempio**

L'esempio seguente abilita la firma SMB richiesta per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

**Determinare se le sessioni SMB sono firmate**

È possibile visualizzare le informazioni sulle sessioni SMB connesse sul server CIFS. È possibile utilizzare queste informazioni per determinare se le sessioni SMB sono firmate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su… | Immettere il comando… |
|---|---|
| Tutte le sessioni firmate su una specifica macchina virtuale di storage (SVM) | `vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true` |
| Dettagli di una sessione firmata con un ID di sessione specifico sulla SVM | `vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance` |

#### Esempi

Il seguente comando visualizza le informazioni sulla sessione relative alle sessioni firmate su SVM vs1. L'output di riepilogo predefinito non visualizza il campo di output "is Session Signed":

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

Il seguente comando visualizza informazioni dettagliate sulla sessione, incluso se la sessione è firmata, in una sessione SMB con un ID sessione 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   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: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

#### Informazioni correlate

Monitoraggio delle statistiche delle sessioni firmate SMB

### Monitorare le statistiche delle sessioni firmate SMB

È possibile monitorare le statistiche delle sessioni SMB e determinare quali sessioni stabilite sono firmate e quali no.

**A proposito di questa attività**

Il `statistics` il comando al livello di privilegio avanzato fornisce `signed_sessions` Contatore che è possibile utilizzare per monitorare il numero di sessioni SMB firmate. Il `signed_sessions` il contatore è disponibile con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la firma SMB per tutte le sessioni SMB.
- `smb1` Consente di monitorare la firma SMB per le sessioni SMB 1.0.
- `smb2` Consente di monitorare la firma SMB per le sessioni SMB 2.x e SMB 3.0.

  Le statistiche SMB 3.0 sono incluse nell'output di `smb2` oggetto.

Se si desidera confrontare il numero di sessioni firmate con il numero totale di sessioni, è possibile confrontare l'output per `signed_sessions` contatore con l'output per `established_sessions` contatore.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dei dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

**Fasi**

1. Impostare il livello di privilegio su Advanced:
   `set -privilege advanced`
2. Avviare una raccolta di dati:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

   È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.
3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.
4. Visualizzare le statistiche della firma SMB:

| Se si desidera visualizzare informazioni per… | Inserisci… |
|---|---|
| Sessioni firmate | `show -sample-id sample_ID -counter signed_sessions |
| *node_name* [-node *node_name*]` | Sessioni firmate e sessioni stabilite |
| `show -sample-id *sample_ID* -counter signed_sessions | established_sessions |

   Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node`

parametro.

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

**Esempi**

L'esempio seguente mostra come monitorare le statistiche di firma SMB 2.x e SMB 3.0 su Storage Virtual Machine (SVM) vs1.

Il seguente comando passa 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
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

Il seguente comando interrompe la raccolta di dati per l'esempio:

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

Il seguente comando mostra le sessioni SMB firmate e le sessioni SMB stabilite per nodo dell'esempio:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                   Value
    -------------------------------- -------------------------
    established_sessions                                          0
    node_name                                                 node1
    signed_sessions                                               0
    established_sessions                                          1
    node_name                                                 node2
    signed_sessions                                               1
    established_sessions                                          0
    node_name                                                 node3
    signed_sessions                                               0
    established_sessions                                          0
    node_name                                                 node4
    signed_sessions                                               0
```

Il seguente comando mostra le sessioni SMB firmate per node2 dell'esempio:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                   Value
    -------------------------------- -------------------------
    node_name                                                 node2
    signed_sessions                                               1
```

Il seguente comando torna al livello di privilegio admin:

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

**Informazioni correlate**

Determinare se le sessioni SMB sono firmate

"Panoramica sulla gestione e sul monitoraggio delle performance"

## Configurare la crittografia SMB richiesta sui server SMB per il trasferimento dei dati su SMB

### Panoramica sulla crittografia SMB

La crittografia SMB per i trasferimenti di dati su SMB è un miglioramento della sicurezza che è possibile attivare o disattivare sui server SMB. È inoltre possibile configurare l'impostazione di crittografia SMB desiderata in base alla condivisione mediante un'impostazione di proprietà di condivisione.

Per impostazione predefinita, quando si crea un server SMB sulla Storage Virtual Machine (SVM), la crittografia SMB viene disattivata. È necessario abilitarlo per sfruttare la sicurezza avanzata fornita dalla crittografia SMB.

Per creare una sessione SMB crittografata, il client SMB deve supportare la crittografia SMB. I client Windows che iniziano con Windows Server 2012 e Windows 8 supportano la crittografia SMB.

La crittografia SMB sulla SVM è controllata da due impostazioni:

- Un'opzione di sicurezza per server SMB che attiva la funzionalità sulla SVM
- Una proprietà di condivisione SMB che configura l'impostazione di crittografia SMB in base alla condivisione

È possibile decidere se richiedere la crittografia per l'accesso a tutti i dati sulla SVM o se richiedere la crittografia SMB per accedere ai dati solo nelle condivisioni selezionate. Le impostazioni a livello di SVM sostituiscono quelle a livello di condivisione.

La configurazione effettiva della crittografia SMB dipende dalla combinazione delle due impostazioni ed è descritta nella tabella seguente:

| Crittografia SMB server abilitata | Share encoded data Setting Enabled (Condividi dati crittografati | Comportamento della crittografia lato server |
|---|---|---|
| Vero | Falso | La crittografia a livello di server è attivata per tutte le condivisioni di SVM. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB. |

| Crittografia SMB server abilitata | Share encoded data Setting Enabled (Condividi dati crittografati | Comportamento della crittografia lato server |
|---|---|---|
| Vero | Vero | La crittografia a livello di server è attivata per tutte le condivisioni di SVM, indipendentemente dalla crittografia a livello di condivisione. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB. |
| Falso | Vero | La crittografia a livello di condivisione è attivata per le condivisioni specifiche. Con questa configurazione, la crittografia viene eseguita dalla connessione ad albero. |
| Falso | Falso | Nessuna crittografia abilitata. |

I client SMB che non supportano la crittografia non possono connettersi a un server SMB o a una condivisione che richiede la crittografia.

Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

**Impatto delle performance della crittografia SMB**

Quando le sessioni SMB utilizzano la crittografia SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM che contiene il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB crittografato. L'offload della crittografia SMB è attivato per impostazione predefinita quando la crittografia SMB è attivata.

Le performance di crittografia SMB avanzate richiedono la funzionalità di offload AES-NI. Consultare Hardware Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11 che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della crittografia SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La crittografia SMB è disattivata per impostazione predefinita sul server SMB. È necessario attivare la crittografia SMB solo sulle condivisioni SMB o sui server SMB che richiedono la crittografia. Con la crittografia SMB, ONTAP esegue un'ulteriore elaborazione della decifratura delle richieste e della crittografia delle risposte per ogni richiesta. La crittografia SMB deve quindi essere attivata solo quando necessario.

### Attiva o disattiva la crittografia SMB richiesta per il traffico SMB in entrata

Se si desidera richiedere la crittografia SMB per il traffico SMB in entrata, è possibile attivarla sul server CIFS o a livello di condivisione. Per impostazione predefinita, la crittografia SMB non è richiesta.

#### A proposito di questa attività

È possibile attivare la crittografia SMB sul server CIFS, che si applica a tutte le condivisioni sul server CIFS. Se non si desidera la crittografia SMB richiesta per tutte le condivisioni sul server CIFS o se si desidera attivare la crittografia SMB richiesta per il traffico SMB in entrata su base share-by-share, è possibile disattivare la crittografia SMB richiesta sul server CIFS.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), l'impostazione di sicurezza della crittografia SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a. `false` (Non-ID-Preserve), l'impostazione di sicurezza della crittografia SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la crittografia SMB sulla SVM di origine, è necessario attivare manualmente la crittografia SMB del server CIFS sulla destinazione.

#### Fasi

1. Eseguire una delle seguenti operazioni:

| Se si desidera che la crittografia SMB richiesta per il traffico SMB in entrata sul server CIFS sia… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true` |
| Disattivato | `vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false` |

2. Verificare che la crittografia SMB richiesta sul server CIFS sia attivata o disattivata come desiderato: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Il `is-smb-encryption-required` viene visualizzato il campo `true` Se necessario, la crittografia SMB è attivata sul server CIFS e. `false` se è disattivato.

#### Esempio

Nell'esempio seguente viene attivata la crittografia SMB richiesta per il traffico SMB in entrata per il server CIFS su SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

### Determinare se i client sono connessi utilizzando sessioni SMB crittografate

È possibile visualizzare informazioni sulle sessioni SMB connesse per determinare se i client utilizzano connessioni SMB crittografate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

#### A proposito di questa attività

Le sessioni dei client SMB possono avere uno dei tre livelli di crittografia seguenti:

- `unencrypted`

  La sessione SMB non è crittografata. Non è stata configurata la crittografia a livello di SVM (Storage Virtual Machine) o a livello di condivisione.

- `partially-encrypted`

  La crittografia viene avviata quando si verifica la connessione ad albero. La crittografia a livello di condivisione è configurata. La crittografia a livello di SVM non è attivata.

- `encrypted`

  La sessione SMB è completamente crittografata. La crittografia a livello di SVM è attivata. La crittografia a livello di condivisione potrebbe non essere attivata. L'impostazione di crittografia a livello di SVM sostituisce l'impostazione di crittografia a livello di condivisione.

#### Fasi

1. Eseguire una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su… | Immettere il comando… |
|---|---|
| Sessioni con un'impostazione di crittografia specificata per le sessioni su una SVM specificata | `vserver cifs session show -vserver *vserver_name* {unencrypted |
| partially-encrypted | encrypted} -instance` |

| Se si desidera visualizzare informazioni su… | Immettere il comando… |
|---|---|
| L'impostazione di crittografia per un ID sessione specifico su una SVM specificata | `vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance` |

#### Esempi

Il seguente comando visualizza informazioni dettagliate sulla sessione, inclusa l'impostazione di crittografia, in una sessione SMB con ID sessione 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    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: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

### Monitorare le statistiche di crittografia SMB

È possibile monitorare le statistiche di crittografia SMB e determinare quali sessioni stabilite e quali connessioni di condivisione sono crittografate e quali no.

#### A proposito di questa attività

Il `statistics` Command al livello di privilegio avanzato fornisce i seguenti contatori, che è possibile utilizzare per monitorare il numero di sessioni SMB crittografate e condividere le connessioni:

| Nome del contatore | Descrizioni |
|---|---|
| `encrypted_sessions` | Indica il numero di sessioni SMB 3.0 crittografate |

| Nome del contatore | Descrizioni |
|---|---|
| `encrypted_share_connections` | Indica il numero di condivisioni crittografate su cui è avvenuta una connessione ad albero |
| `rejected_unencrypted_sessions` | Indica il numero di configurazioni di sessione rifiutate a causa della mancanza di funzionalità di crittografia del client |
| `rejected_unencrypted_shares` | Indica il numero di mappature di condivisione rifiutate a causa della mancanza di funzionalità di crittografia del client |

Questi contatori sono disponibili con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la crittografia SMB per tutte le sessioni SMB 3.0.

  Le statistiche SMB 3.0 sono incluse nell'output di `cifs` oggetto. Se si desidera confrontare il numero di sessioni crittografate con il numero totale di sessioni, è possibile confrontare l'output per `encrypted_sessions` contatore con l'output per `established_sessions` contatore.

  Se si desidera confrontare il numero di connessioni di condivisione crittografate con il numero totale di connessioni di condivisione, è possibile confrontare l'output per `encrypted_share_connections` contatore con l'output per `connected_shares` contatore.

- `rejected_unencrypted_sessions` Fornisce il numero di tentativi di stabilire una sessione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.
- `rejected_unencrypted_shares` Fornisce il numero di tentativi di connessione a una condivisione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

**Fasi**

1. Impostare il livello di privilegio su Advanced:
   `set -privilege advanced`
2. Avviare una raccolta di dati:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

   È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.

3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.

4. Visualizza le statistiche di crittografia SMB:

| Se si desidera visualizzare informazioni per… | Inserisci… |
|---|---|
| Sessioni crittografate | `show -sample-id *sample_ID* -counter encrypted_sessions |
| *node_name* [-node *node_name*]` | Sessioni crittografate e sessioni stabilite |
| `show -sample-id *sample_ID* -counter encrypted_sessions | established_sessions |
| *node_name* [-node *node_name*]` | Connessioni di condivisione crittografate |
| `show -sample-id *sample_ID* -counter encrypted_share_connections | *node_name* [-node *node_name*]` |
| Connessioni di condivisione crittografate e condivisioni connesse | `show -sample-id *sample_ID* -counter encrypted_share_connections |
| connected_shares | *node_name* [-node *node_name*]` |
| Sessioni non crittografate rifiutate | `show -sample-id *sample_ID* -counter rejected_unencrypted_sessions |
| *node_name* [-node *node_name*]` | Connessioni di condivisione non crittografate rifiutate |
| `show -sample-id *sample_ID* -counter rejected_unencrypted_share | *node_name* [-node *node_name*]` |

Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node` parametro.

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

**Esempi**

L'esempio seguente mostra come monitorare le statistiche di crittografia SMB 3.0 su storage virtual machine (SVM) vs1.

Il seguente comando passa 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
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

Il seguente comando interrompe la raccolta dei dati per quell'esempio:

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

Il seguente comando mostra le sessioni SMB crittografate e le sessioni SMB stabilite dal nodo dell'esempio:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  ----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

Il comando seguente mostra il numero di sessioni SMB non crittografate rifiutate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

Il comando seguente mostra il numero di condivisioni SMB connesse e di condivisioni SMB crittografate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

Il comando seguente mostra il numero di connessioni di condivisione SMB non crittografate rifiutate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    -------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

**Informazioni correlate**

Determinazione degli oggetti e dei contatori delle statistiche disponibili

"Panoramica sulla gestione e sul monitoraggio delle performance"

## Comunicazione sicura della sessione LDAP

### Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la

sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È necessario configurare le impostazioni di sicurezza del server CIFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

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

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

#### Abilitare la firma e il sealing LDAP sul server CIFS

Prima che il server CIFS possa utilizzare la firma e il sealing per una comunicazione sicura con un server LDAP di Active Directory, è necessario modificare le impostazioni di sicurezza del server CIFS per abilitare la firma e il sealing LDAP.

**Prima di iniziare**

Per determinare i valori di configurazione della protezione appropriati, rivolgersi all'amministratore del server ad.

**Fasi**

1. Configurare l'impostazione di sicurezza del server CIFS che abilita il traffico firmato e sigillato con i server LDAP di Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session -security-for-ad-ldap {none|sign|seal}`

   È possibile attivare la firma (`sign`, integrità dei dati), firma e sigillatura (`seal`, integrità dei dati e crittografia), o nessuna delle due `none`, nessuna firma o sigillatura). Il valore predefinito è `none`.

2. Verificare che l'impostazione di protezione per la firma e il sealing LDAP sia impostata correttamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX, ad esempio utenti, gruppi e netgroup, è necessario attivare l'impostazione corrispondente con `-session-security` opzione di `vserver services name-service ldap client modify` comando.

### Configurare LDAP su TLS

#### Esportare una copia del certificato della CA principale autofirmato

Per utilizzare LDAP su SSL/TLS per la protezione delle comunicazioni Active Directory, è necessario prima esportare una copia del certificato CA principale autofirmato di Active Directory Certificate Service in un file di certificato e convertirla in un file di testo ASCII. Questo file di testo viene utilizzato da ONTAP per installare il certificato sulla macchina virtuale di storage (SVM).

**Prima di iniziare**

Active Directory Certificate Service deve essere già installato e configurato per il dominio a cui appartiene il

server CIFS. Per informazioni sull'installazione e la configurazione di Active Director Certificate Services, consultare la Microsoft TechNet Library.

"Microsoft TechNet Library: technet.microsoft.com"

**Fase**

1. Ottenere un certificato CA principale del controller di dominio presente in `.pem` formato del testo.

   "Microsoft TechNet Library: technet.microsoft.com"

**Al termine**

Installare il certificato sulla SVM.

**Informazioni correlate**

"Microsoft TechNet Library"

#### Installare il certificato della CA principale autofirmato su SVM

Se è richiesta l'autenticazione LDAP con TLS durante l'associazione ai server LDAP, è necessario installare prima il certificato della CA principale autofirmato su SVM.

**A proposito di questa attività**

Quando LDAP su TLS è attivato, il client LDAP di ONTAP su SVM non supporta i certificati revocati in ONTAP 9.0 e 9.1.

A partire da ONTAP 9.2, tutte le applicazioni di ONTAP che utilizzano le comunicazioni TLS possono controllare lo stato dei certificati digitali utilizzando il protocollo OCSP (Online Certificate Status Protocol). Se OCSP è abilitato per LDAP su TLS, i certificati revocati vengono rifiutati e la connessione non riesce.

**Fasi**

1. Installare il certificato della CA principale autofirmato:

   a. Avviare l'installazione del certificato: `security certificate install -vserver vserver_name -type server-ca`

      L'output della console visualizza il seguente messaggio: `Please enter Certificate: Press <Enter> when done`

   b. Aprire il certificato `.pem` copiare il certificato con un editor di testo, incluse le righe che iniziano con `-----BEGIN CERTIFICATE-----` e terminando con `-----END CERTIFICATE-----`, quindi incollare il certificato dopo il prompt dei comandi.

   c. Verificare che il certificato sia visualizzato correttamente.

   d. Completare l'installazione premendo Invio.

2. Verificare che il certificato sia installato: `security certificate show -vserver` *`vserver_name`*

#### Attivare LDAP su TLS sul server

Prima che il server SMB possa utilizzare TLS per una comunicazione sicura con un server LDAP Active Directory, è necessario modificare le impostazioni di sicurezza del server SMB per attivare LDAP su TLS.

A partire da ONTAP 9.10.1, il binding del canale LDAP è supportato per impostazione predefinita sia per le connessioni LDAP Active Directory (ad) che per i servizi di nomi. ONTAP proverà l'associazione del canale con connessioni LDAP solo se Start-TLS o LDAPS è attivato insieme alla sicurezza della sessione impostata su Sign o Seal. Per disattivare o riabilitare l'associazione del canale LDAP con i server ad, utilizzare `-try -channel-binding-for-ad-ldap` con il `vserver cifs security modify` comando.

Per ulteriori informazioni, consulta:

- "Panoramica LDAP"
- "2020 requisiti di binding del canale LDAP e firma LDAP per Windows".

**Fasi**

1. Configurare l'impostazione di sicurezza del server SMB che consente la comunicazione LDAP sicura con i server LDAP di Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Verificare che l'impostazione di protezione LDAP su TLS sia impostata su `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX (ad esempio utenti, gruppi e netgroup), è necessario modificare anche `-use-start-tls` utilizzando l'opzione `vserver services name-service ldap client modify` comando.

# Configurare SMB multicanale per performance e ridondanza

A partire da ONTAP 9.4, è possibile configurare SMB multicanale in modo da fornire più connessioni tra ONTAP e client in una singola sessione SMB. In questo modo si migliora il throughput e la tolleranza agli errori.

**Prima di iniziare**

È possibile utilizzare la funzionalità SMB multicanale solo quando i client negoziano con SMB 3.0 o versioni successive. SMB 3.0 e versioni successive sono attivate sul server SMB ONTAP per impostazione predefinita.

**A proposito di questa attività**

I client SMB rilevano e utilizzano automaticamente più connessioni di rete se viene identificata una configurazione corretta nel cluster ONTAP.

Il numero di connessioni simultanee in una sessione SMB dipende dalle schede NIC implementate:

- **NIC 1G su client e cluster ONTAP**

  Il client stabilisce una connessione per NIC e associa la sessione a tutte le connessioni.

- **NIC da 10 G e capacità superiore su cluster client e ONTAP**

  Il client stabilisce fino a quattro connessioni per NIC e associa la sessione a tutte le connessioni. Il client può stabilire connessioni su più NIC da 10 G e capacità maggiore.

È inoltre possibile modificare i seguenti parametri (privilegio avanzato):

- **`-max-connections-per-session`**

  Numero massimo di connessioni consentite per sessione multicanale. L'impostazione predefinita è 32 connessioni.

  Se si desidera attivare più connessioni rispetto a quelle predefinite, è necessario apportare modifiche simili alla configurazione del client, che ha anche un valore predefinito di 32 connessioni.

- **`-max-lifs-per-session`**

  Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. L'impostazione predefinita è 256 interfacce di rete.

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Abilitare SMB Multichannel sul server SMB: `vserver cifs options modify -vserver` *`vserver_name`* `-is-multichannel-enabled true`
3. Verificare che ONTAP stia segnalando sessioni multicanale SMB: `vserver cifs session show` *`options`*
4. Tornare al livello di privilegio admin: `set -privilege admin`

**Esempio**

Nell'esempio seguente vengono visualizzate informazioni su tutte le sessioni SMB, che mostrano più connessioni per una singola sessione:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate su una sessione SMB con id sessione 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

# Configurare le mappature predefinite dell'utente Windows su UNIX sul server SMB

## Configurare l'utente UNIX predefinito

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

#### A proposito di questa attività

Per impostazione predefinita, il nome dell'utente UNIX predefinito è "pcuser", il che significa che, per impostazione predefinita, è attivata la mappatura dell'utente all'utente UNIX predefinito. È possibile specificare un altro nome da utilizzare come utente UNIX predefinito. Il nome specificato deve esistere nei database del servizio di nomi configurati per la macchina virtuale di storage (SVM). Se questa opzione è impostata su una stringa nulla, nessuno può accedere al server CIFS come utente predefinito UNIX. In altri termini, ogni utente deve disporre di un account nel database delle password prima di poter accedere al server CIFS.

Per consentire a un utente di connettersi al server CIFS utilizzando l'account utente UNIX predefinito, l'utente deve soddisfare i seguenti prerequisiti:

- L'utente viene autenticato.
- L'utente si trova nel database utenti Windows locale del server CIFS, nel dominio principale del server

CIFS o in un dominio attendibile (se le ricerche di mappatura dei nomi multidominio sono attivate sul server CIFS).

- Il nome utente non è esplicitamente associato a una stringa nulla.

**Fasi**

1. Configurare l'utente UNIX predefinito:

| Se si desidera … | Inserire … |
|---|---|
| Utilizzare l'utente UNIX predefinito "pcuser" | `vserver cifs options modify -default -unix-user pcuser` |
| Utilizzare un altro account utente UNIX come utente predefinito | `vserver cifs options modify -default -unix-user` *`user_name`* |
| Disattiva l'utente UNIX predefinito | `vserver cifs options modify -default -unix-user ""` |

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verificare che l'utente UNIX predefinito sia configurato correttamente: `vserver cifs options show -vserver` *`vserver_name`*

   Nell'esempio seguente, sia l'utente UNIX predefinito che l'utente UNIX guest su SVM vs1 sono configurati per utilizzare l'utente UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

## Configurare l'utente UNIX guest

La configurazione dell'opzione utente UNIX guest implica che gli utenti che accedono da domini non attendibili vengono mappati all'utente UNIX guest e possono connettersi al server CIFS. In alternativa, se si desidera che l'autenticazione degli utenti da domini non attendibili non venga eseguita correttamente, non configurare l'utente UNIX guest. L'impostazione predefinita prevede che gli utenti di domini non attendibili non possano connettersi al server CIFS (l'account UNIX guest non è configurato).

**A proposito di questa attività**

Durante la configurazione dell'account UNIX guest, tenere presente quanto segue:

- Se il server CIFS non è in grado di autenticare l'utente rispetto a un controller di dominio per il dominio principale, un dominio attendibile o il database locale e questa opzione è attivata, il server CIFS considera l'utente come un utente guest e lo associa all'utente UNIX specificato.
- Se questa opzione è impostata su una stringa nulla, l'utente UNIX guest viene disattivato.
- È necessario creare un utente UNIX da utilizzare come utente UNIX guest in uno dei database del servizio nomi delle macchine virtuali di storage (SVM).
- Un utente che ha effettuato l'accesso come utente guest è automaticamente membro del gruppo BUILTIN/guest sul server CIFS.
- L'opzione 'homedirs-public' si applica solo agli utenti autenticati. Un utente che ha effettuato l'accesso come ospite non dispone di una home directory e non può accedere alle home directory di altri utenti.

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera… | Inserisci… |
|---|---|
| Configurare l'utente UNIX guest | `vserver cifs options modify -guest -unix-user` *`unix_name`* |
| Disattivare l'utente UNIX guest | `vserver cifs options modify -guest -unix-user ""` |

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verificare che l'utente UNIX guest sia configurato correttamente: `vserver cifs options show -vserver` *`vserver_name`*

   Nell'esempio seguente, sia l'utente UNIX predefinito che l'utente UNIX guest su SVM vs1 sono configurati per utilizzare l'utente UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

### Mappare il gruppo di amministratori alla directory principale

Se nell'ambiente sono presenti solo client CIFS e la macchina virtuale di storage (SVM) è stata impostata come sistema di storage multiprotocollo, è necessario disporre di almeno un account Windows con privilegi root per accedere ai file sulla SVM; In caso contrario, non è possibile gestire SVM perché non si dispone di diritti utente sufficienti.

#### A proposito di questa attività

Tuttavia, se il sistema storage è stato configurato come solo NTFS, il `/etc` La directory dispone di un ACL a livello di file che consente al gruppo di amministratori di accedere ai file di configurazione di ONTAP.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'opzione del server CIFS che associa il gruppo di amministratori alla directory principale in base alle esigenze:

| Se si desidera… | Quindi… |
|---|---|
| Associare i membri del gruppo di amministratori alla directory principale | `vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to -root-enabled true` Tutti gli account del gruppo di amministratori sono considerati root, anche se non si dispone di un `/etc/usermap.cfg` voce che esegue il mapping degli account alla directory principale. Se si crea un file utilizzando un account che appartiene al gruppo di amministratori, il file è di proprietà di root quando si visualizza il file da un client UNIX. |
| Disattiva il mapping dei membri del gruppo di amministratori alla directory principale | `vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to -root-enabled false` Gli account nel gruppo di amministratori non vengono più mappati alla directory principale. È possibile mappare esplicitamente solo un singolo utente a root. |

3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver` *`vserver_name`*
4. Tornare al livello di privilegio admin: `set -privilege admin`

## Visualizza informazioni sui tipi di utenti connessi nelle sessioni SMB

È possibile visualizzare informazioni sul tipo di utenti connessi tramite sessioni SMB. In questo modo è possibile garantire che solo il tipo di utente appropriato si connetta tramite sessioni SMB sulla macchina virtuale di storage (SVM).

#### A proposito di questa attività

I seguenti tipi di utenti possono connettersi tramite sessioni SMB:

- `local-user`

  Autenticato come utente CIFS locale

- `domain-user`

  Autenticato come utente di dominio (dal dominio principale del server CIFS o da un dominio attendibile)

- `guest-user`

  Autenticato come utente ospite

- `anonymous-user`

  Autenticato come utente anonimo o nullo

**Fasi**

1. Determinare il tipo di utente connesso in una sessione SMB: `vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

| Se si desidera visualizzare le informazioni sul tipo di utente per le sessioni stabilite… | Immettere il seguente comando… |
|---|---|
| Per tutte le sessioni con un tipo di utente specificato | `vserver cifs session show -vserver *vserver_name* -user-type {local-user |
| domain-user | guest-user |
| anonymous-user}` | Per un utente specifico |

**Esempi**

Il seguente comando visualizza le informazioni sulla sessione relative al tipo di utente per le sessioni su SVM vs1 stabilite dall'utente "` iepubs` user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

# Opzioni di comando per limitare il consumo eccessivo di risorse del client Windows

Opzioni di `vserver cifs options modify` Il comando consente di controllare il consumo di risorse per i client Windows. Questo può essere utile se i client non rientrano nei limiti normali di consumo delle risorse, ad esempio se sono presenti un numero insolitamente elevato di file aperti, sessioni aperte o richieste di notifica delle modifiche.

Le seguenti opzioni di `vserver cifs options modify` Sono stati aggiunti comandi per controllare il consumo di risorse del client Windows. Se si supera il valore massimo di una di queste opzioni, la richiesta viene rifiutata e viene inviato un messaggio EMS. Viene inoltre inviato un messaggio di avviso EMS quando viene raggiunto il 80% del limite configurato per queste opzioni.

- `-max-opens-same-file-per-tree`

  Numero massimo di apertura sullo stesso file per albero CIFS

- `-max-same-user-sessions-per-connection`

  Numero massimo di sessioni aperte dallo stesso utente per connessione

- `-max-same-tree-connect-per-session`

  Numero massimo di connessioni ad albero sulla stessa condivisione per sessione

- `-max-watches-set-per-tree`

  Numero massimo di orologi (noto anche come *change notifes*) stabiliti per albero

Vedere le pagine man per i limiti predefiniti e per visualizzare la configurazione corrente.

A partire da ONTAP 9.4, i server SMB versione 2 o successiva possono limitare il numero di richieste in sospeso (*SMB credits*) che il client può inviare al server con una connessione SMB. La gestione dei crediti SMB viene avviata dal client e controllata dal server.

Il numero massimo di richieste in sospeso che possono essere concesse su una connessione SMB è controllato da `-max-credits` opzione. Il valore predefinito per questa opzione è 128.

# Migliora le performance del client con gli oplock tradizionali e in leasing

## Migliora le performance del client con una panoramica degli oplock tradizionali e del lease

Gli oplock tradizionali (blocchi opportunistici) e gli oplock di lease consentono a un client SMB in alcuni scenari di condivisione file di eseguire il caching lato client delle informazioni di Read-ahead, write-behind e lock. Un client può quindi leggere o scrivere su un file senza ricordare regolarmente al server che ha bisogno di accedere al file in questione. Ciò migliora le performance riducendo il traffico di rete.

Gli oplock di leasing sono una forma avanzata di oplock disponibili con il protocollo SMB 2.1 e versioni successive. Gli oplock del lease consentono a un client di ottenere e preservare lo stato di caching del client in più SMB aperti che hanno origine da sé.

Gli oplock possono essere controllati in due modi:

- Da una proprietà di condivisione, utilizzando `vserver cifs share create` quando viene creata la condivisione, oppure il `vserver share properties` comando dopo la creazione.
- Da una proprietà qtree, utilizzando `volume qtree create` quando viene creato il qtree, oppure il `volume qtree oplock` comandi dopo la creazione.

## Considerazioni sulla perdita di dati della cache in scrittura quando si utilizzano gli oplock

In alcuni casi, se un processo ha un oplock esclusivo su un file e un secondo processo tenta di aprire il file, il primo processo deve invalidare i dati memorizzati nella cache e svuotare le scritture e i blocchi. Il client deve quindi rinunciare all'oplock e all'accesso al file. Se si verifica un errore di rete durante questo svuotamento, i dati di scrittura memorizzati nella cache potrebbero andare persi.

- Possibilità di perdita di dati

  Qualsiasi applicazione che dispone di dati memorizzati nella cache in scrittura può perdere tali dati nei seguenti casi:

  - La connessione viene effettuata utilizzando SMB 1.0.
  - Ha un oplock esclusivo sul file.
  - Viene richiesto di interrompere l'oplock o chiudere il file.
  - Durante il processo di cancellazione della cache di scrittura, il sistema di rete o di destinazione genera un errore.
- Gestione degli errori e completamento della scrittura

  La cache stessa non ha alcun tipo di gestione degli errori, come fanno le applicazioni. Quando l'applicazione esegue una scrittura nella cache, la scrittura viene sempre completata. Se la cache, a sua volta, esegue una scrittura nel sistema di destinazione su una rete, deve presumere che la scrittura sia completata perché in caso contrario, i dati vengono persi.

## Attiva o disattiva gli oplock durante la creazione di condivisioni SMB

Gli oplock consentono ai client di bloccare i file e memorizzare nella cache i contenuti localmente, aumentando le performance per le operazioni sui file. Gli oplock sono abilitati sulle condivisioni SMB che risiedono su storage virtual machine (SVM). In alcuni casi, è possibile disattivare gli oplock. È possibile attivare o disattivare gli oplock in base alla condivisione.

#### A proposito di questa attività

Se gli oplock sono attivati sul volume che contiene una condivisione ma la proprietà di oplock share per tale condivisione è disattivata, gli oplock sono disattivati per quella condivisione. La disattivazione degli oplock in

una condivisione ha la precedenza sull'impostazione dell'oplock del volume. La disattivazione degli oplock sulla condivisione disattiva gli oplock opportunistici e lease.

È possibile specificare altre proprietà di condivisione oltre a specificare la proprietà di condivisione oplock utilizzando un elenco delimitato da virgole. È inoltre possibile specificare altri parametri di condivisione.

**Fasi**

1. Eseguire l'azione appropriata:

| Se si desidera… | Quindi… |
| --- | --- |
| Abilitare gli oplock su una condivisione durante la creazione della condivisione | Immettere il seguente comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]`<br>Se si desidera che la condivisione abbia solo le proprietà di condivisione predefinite, che sono `oplocks`, `browsable`, e. `changenotify` attivato, non è necessario specificare `-share -properties` Parametro durante la creazione di una condivisione SMB. Se si desidera una combinazione di proprietà di condivisione diversa da quella predefinita, è necessario specificare `-share-properties` parametro con l'elenco delle proprietà di condivisione da utilizzare per la condivisione. |
| Disattiva gli oplock su una condivisione durante la creazione della condivisione | Immettere il seguente comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]`<br>Quando si disattivano gli oplock, è necessario specificare un elenco di proprietà di condivisione durante la creazione della condivisione, ma non è necessario specificare `oplocks` proprietà. |

**Informazioni correlate**

Attivazione o disattivazione degli oplock sulle condivisioni SMB esistenti

Monitoraggio dello stato dell'oplock

## Comandi per attivare o disattivare gli oplock su volumi e qtree

Gli oplock consentono ai client di bloccare i file e memorizzare nella cache i contenuti localmente, aumentando le performance per le operazioni sui file. È necessario conoscere i comandi per attivare o disattivare gli oplock su volumi o qtree. È inoltre necessario sapere quando è possibile attivare o disattivare gli oplock su volumi e qtree.

- Gli oplock sono attivati sui volumi per impostazione predefinita.
- Non è possibile disattivare gli oplock quando si crea un volume.
- È possibile attivare o disattivare gli oplock sui volumi esistenti per le SVM in qualsiasi momento.
- È possibile abilitare gli oplock sui qtree per le SVM.

  L'impostazione della modalità oplock è una proprietà di qtree ID 0, il qtree predefinito di tutti i volumi. Se non si specifica un'impostazione di oplock durante la creazione di un qtree, il qtree eredita l'impostazione di oplock del volume padre, che viene attivata per impostazione predefinita. Tuttavia, se si specifica un'impostazione di oplock sul nuovo qtree, questa ha la precedenza sull'impostazione di oplock sul volume.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Abilitare gli oplock sui volumi o sui qtree | `volume qtree oplocks` con `-oplock-mode` parametro impostato su `enable` |
| Disattiva gli oplock sui volumi o sui qtree | `volume qtree oplocks` con `-oplock-mode` parametro impostato su `disable` |

**Informazioni correlate**

Monitoraggio dello stato dell'oplock

## Attiva o disattiva gli oplock sulle condivisioni SMB esistenti

Per impostazione predefinita, gli oplock sono attivati sulle condivisioni SMB sulle macchine virtuali di storage (SVM). In alcuni casi, potrebbe essere necessario disattivare gli oplock; in alternativa, se in precedenza sono stati disattivati gli oplock in una condivisione, potrebbe essere necessario riattivarli.

**A proposito di questa attività**

Se gli oplock sono attivati sul volume che contiene una condivisione, ma la proprietà di oplock share per tale condivisione è disattivata, gli oplock sono disattivati per quella condivisione. La disattivazione degli oplock su una condivisione ha la precedenza sull'attivazione degli oplock sul volume. Disattivando gli oplock sulla condivisione, vengono disattivati gli oplock opportunistici e lease. È possibile attivare o disattivare gli oplock sulle condivisioni esistenti in qualsiasi momento.

**Fase**

1. Eseguire l'azione appropriata:

| Se si desidera… | Quindi… |
| --- | --- |
| Abilitare gli oplock su una condivisione modificando una condivisione esistente | Immettere il seguente comando: `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks`<br><br>È possibile specificare ulteriori proprietà di condivisione da aggiungere utilizzando un elenco delimitato da virgole.<br><br>Le nuove proprietà aggiunte vengono aggiunte all'elenco esistente di proprietà di condivisione. Tutte le proprietà di condivisione precedentemente specificate rimangono attive. |
| Disattivare gli oplock su una condivisione modificando una condivisione esistente | Immettere il seguente comando: `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks`<br><br>È possibile specificare ulteriori proprietà di condivisione da rimuovere utilizzando un elenco delimitato da virgole.<br><br>Le proprietà di condivisione rimosse vengono eliminate dall'elenco esistente di proprietà di condivisione; tuttavia, le proprietà di condivisione configurate in precedenza e non rimosse rimangono attive. |

**Esempi**

Il seguente comando abilita gli oplock per la condivisione denominata "Engineering" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

Il seguente comando disattiva gli oplock per la condivisione denominata “Engineering” su SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

**Informazioni correlate**

Attivazione o disattivazione degli oplock durante la creazione di condivisioni SMB

Monitoraggio dello stato dell’oplock

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

## Monitorare lo stato dell’oplock

È possibile monitorare e visualizzare informazioni sullo stato dell’oplock. È possibile utilizzare queste informazioni per determinare quali file dispongono di oplock, quali sono il livello di oplock e il livello di oplock state e se viene utilizzato il leasing di oplock. È inoltre possibile determinare le informazioni sui blocchi che potrebbero essere necessari per interrompere manualmente.

**A proposito di questa attività**

È possibile visualizzare le informazioni relative a tutti gli oplock in forma di riepilogo o in un elenco dettagliato. È inoltre possibile utilizzare parametri opzionali per visualizzare informazioni su un sottoinsieme più piccolo di blocchi esistenti. Ad esempio, è possibile specificare che l’output restituisca blocchi solo con l’indirizzo IP del client specificato o con il percorso specificato.

È possibile visualizzare le seguenti informazioni sugli oplock tradizionali e di lease:

- SVM, nodo, volume e LIF su cui è stabilito l’oplock
- Blocca UUID
- Indirizzo IP del client con l’oplock
- Percorso in cui viene stabilito l’oplock
- Protocollo di blocco (SMB) e tipo (oplock)
- Stato di blocco
- Livello di oplock
- Stato di connessione e tempo di scadenza SMB
- Aprire ID gruppo se viene concesso un oplock di leasing

Vedere `vserver oplocks show` pagina man per una descrizione dettagliata di ciascun parametro.

**Fasi**

1. Visualizzare lo stato dell'oplock utilizzando `vserver locks show` comando.

**Esempi**

Il seguente comando visualizza le informazioni predefinite relative a tutti i blocchi. L'oplock sul file visualizzato viene concesso con un `read-batch` livello di oplock:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

Nell'esempio seguente vengono visualizzate informazioni più dettagliate sul blocco di un file con il percorso `/data2/data2_2/intro.pptx`. Un oplock del lease viene concesso sul file con un `batch` Livello di oplock per un client con un indirizzo IP di `10.3.1.3`:

> Quando si visualizzano informazioni dettagliate, il comando fornisce un output separato per le informazioni di oplock e sharlock. Questo esempio mostra solo l'output della sezione oplock.

```
cluster1::> vserver lock 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: ff1cbf29-bfef-4d91-ae06-062bf69212c3
             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
```

**Informazioni correlate**

Attivazione o disattivazione degli oplock durante la creazione di condivisioni SMB

Attivazione o disattivazione degli oplock sulle condivisioni SMB esistenti

Comandi per attivare o disattivare gli oplock su volumi e qtree

# Applicare oggetti Criteri di gruppo ai server SMB

## Panoramica sull'applicazione degli oggetti Criteri di gruppo ai server SMB

Il server SMB supporta gli oggetti Criteri di gruppo (GPO), un insieme di regole note come *attributi dei criteri di gruppo* che si applicano ai computer in un ambiente Active Directory. È possibile utilizzare gli oggetti Criteri di gruppo per gestire centralmente le impostazioni di tutte le macchine virtuali di storage (SVM) nel cluster appartenente allo stesso dominio Active Directory.

Quando gli oggetti Criteri di gruppo sono attivati sul server SMB, ONTAP invia query LDAP al server Active

Directory per richiedere informazioni sull'oggetto Criteri di gruppo. Se esistono definizioni di GPO applicabili al server SMB, il server Active Directory restituisce le seguenti informazioni di GPO:

- Nome dell'oggetto Criteri di gruppo
- Versione attuale dell'oggetto Criteri di gruppo
- Posizione della definizione dell'oggetto Criteri di gruppo
- Elenchi di UUID (universally unique identifier) per set di criteri GPO

**Informazioni correlate**

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

"Controllo SMB e NFS e tracciamento della sicurezza"

## GPO supportati

Sebbene non tutti gli oggetti Criteri di gruppo (GPO) siano applicabili alle SVM (Storage Virtual Machine) abilitate per CIFS, le SVM sono in grado di riconoscere ed elaborare il relativo set di GPO.

I seguenti GPO sono attualmente supportati sulle SVM:

- Impostazioni avanzate di configurazione dei criteri di controllo:

  Accesso a oggetti: Staging dei criteri di accesso centrale

  Specifica il tipo di eventi da sottoporre a verifica per lo staging dei criteri di accesso centrale (CAP), incluse le seguenti impostazioni:

  - Non eseguire audit
  - Controllare solo gli eventi di successo
  - Controllare solo gli eventi di errore
  - Controllare gli eventi di successo e di guasto

  > Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

  Impostare utilizzando `Audit Central Access Policy Staging` in `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Per utilizzare le impostazioni dell'oggetto Criteri di gruppo per la configurazione avanzata dei criteri di controllo, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni del Registro di sistema:

  - Intervallo di aggiornamento dei criteri di gruppo per SVM abilitato CIFS

    Impostare utilizzando `Registry` GPO.

- Offset casuale di refresh dei criteri di gruppo

  Impostare utilizzando `Registry` GPO.

- Pubblicazione hash per BranchCache

  La pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde alla modalità operativa BranchCache. Sono supportate le seguenti tre modalità operative:

  - Per-share
  - All-share
  - Disattivato tramite `Registry` GPO.

- Supporto della versione hash per BranchCache

  Sono supportate le seguenti tre impostazioni di versione hash:

  - BranchCache versione 1
  - BranchCache versione 2
  - BranchCache versioni 1 e 2 impostate tramite `Registry` GPO.

> Per utilizzare le impostazioni dell'oggetto Criteri di gruppo BranchCache, è necessario configurare BranchCache sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se BranchCache non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni di sicurezza
  - Policy di audit e registro eventi
    - Controllare gli eventi di accesso

      Specifica il tipo di eventi di accesso da sottoporre a verifica, incluse le seguenti impostazioni:

      - Non eseguire audit
      - Controllare solo gli eventi di successo
      - Verifica degli eventi di guasto
      - Controllare gli eventi di successo e di guasto impostati utilizzando `Audit logon events` in `Local Policies/Audit Policy` GPO.

        > Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

    - Controllare l'accesso agli oggetti

      Specifica il tipo di accesso a oggetti da sottoporre a controllo, incluse le seguenti impostazioni:

      - Non eseguire audit
      - Controllare solo gli eventi di successo
      - Verifica degli eventi di guasto

- Controllare gli eventi di successo e di guasto impostati utilizzando `Audit object access` in `Local Policies/Audit Policy` GPO.

> Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

- Metodo di conservazione dei log

  Specifica il metodo di conservazione del registro di controllo, incluse le seguenti impostazioni:

  - Sovrascrivere il registro eventi quando la dimensione del file di registro supera la dimensione massima
  - Non sovrascrivere il registro eventi (cancellare manualmente il registro) impostato utilizzando `Retention method for security log` in `Event Log` GPO.

- Dimensione massima del log

  Specifica la dimensione massima del registro di controllo.

  Impostare utilizzando `Maximum security log size` in `Event Log` GPO.

> Per utilizzare le impostazioni dell'oggetto Criteri di gruppo dei criteri di controllo e del registro eventi, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

◦ Sicurezza del file system

Specifica un elenco di file o directory su cui viene applicata la protezione dei file tramite un GPO.

Impostare utilizzando `File System` GPO.

> Il percorso del volume in cui è configurato l'oggetto Criteri di gruppo di protezione del file system deve esistere all'interno della SVM.

◦ Policy Kerberos

- Massima inclinazione dell'orologio

  Specifica la tolleranza massima in minuti per la sincronizzazione dell'orologio del computer.

  Impostare utilizzando `Maximum tolerance for computer clock synchronization` in `Account Policies/Kerberos Policy` GPO.

- Età massima del biglietto

  Specifica la durata massima in ore per il ticket utente.

  Impostare utilizzando `Maximum lifetime for user ticket` in `Account Policies/Kerberos Policy` GPO.

- Età massima per il rinnovo del biglietto

Specifica la durata massima in giorni per il rinnovo del ticket utente.

Impostare utilizzando `Maximum lifetime for user ticket renewal` in `Account Policies/Kerberos Policy` GPO.

- Assegnazione dei diritti dell'utente (diritti di privilegio)
  - Assuma la proprietà

    Specifica l'elenco di utenti e gruppi che hanno il diritto di assumere la proprietà di qualsiasi oggetto a protezione diretta.

    Impostare utilizzando `Take ownership of files or other objects` in `Local Policies/User Rights Assignment` GPO.

  - Privilegio di sicurezza

    Specifica l'elenco di utenti e gruppi che possono specificare le opzioni di controllo per l'accesso a oggetti di singole risorse, come file, cartelle e oggetti Active Directory.

    Impostare utilizzando `Manage auditing and security log` in `Local Policies/User Rights Assignment` GPO.

  - Modifica del privilegio di notifica (ignora il controllo incrociato)

    Specifica l'elenco di utenti e gruppi che possono attraversare gli alberi di directory anche se gli utenti e i gruppi potrebbero non disporre delle autorizzazioni per la directory attraversata.

  Lo stesso privilegio è richiesto per gli utenti per ricevere notifiche delle modifiche apportate a file e directory. Impostare utilizzando `Bypass traverse checking` in `Local Policies/User Rights Assignment` GPO.

- Valori del Registro di sistema
  - Firma obbligatoria

    Specifica se la firma SMB richiesta è attivata o disattivata.

  Impostare utilizzando `Microsoft network server: Digitally sign communications (always)` in `Security Options` GPO.

- Limitare l'anonimato

  Specifica quali sono le restrizioni per gli utenti anonimi e include le seguenti tre impostazioni dell'oggetto Criteri di gruppo:

  - Nessuna enumerazione degli account SAM (Security account Manager):

    Questa impostazione di protezione determina le autorizzazioni aggiuntive concesse per le connessioni anonime al computer. Questa opzione viene visualizzata come `no-enumeration` In ONTAP, se abilitato.

    Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts` in `Local Policies/Security Options` GPO.

- Nessuna enumerazione di account e condivisioni SAM

  Questa impostazione di protezione determina se è consentita l'enumerazione anonima di account e condivisioni SAM. Questa opzione viene visualizzata come `no-enumeration` In ONTAP, se abilitato.

  Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts and shares` in `Local Policies/Security Options` GPO.

- Limitare l'accesso anonimo alle condivisioni e alle named pipe

  Questa impostazione di sicurezza limita l'accesso anonimo alle condivisioni e alle pipe. Questa opzione viene visualizzata come `no-access` In ONTAP, se abilitato.

  Impostare utilizzando `Network access: Restrict anonymous access to Named Pipes and Shares` in `Local Policies/Security Options` GPO.

  Quando si visualizzano informazioni sui criteri di gruppo definiti e applicati, il `Resultant restriction for anonymous user` Il campo di output fornisce informazioni sulla restrizione risultante delle tre impostazioni di restrizione anonime dell'oggetto Criteri di gruppo. Le possibili restrizioni risultanti sono le seguenti:

° `no-access`

All'utente anonimo viene negato l'accesso alle condivisioni e alle named pipe specificate e non è possibile utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è attivato.

° `no-enumeration`

L'utente anonimo ha accesso alle condivisioni e alle named pipe specificate, ma non può utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Sia il `Network access: Do not allow anonymous enumeration of SAM accounts` o il `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti GPO sono abilitati.

° `no-restriction`

L'utente anonimo ha accesso completo e può utilizzare l'enumerazione. Questa restrizione risultante si verifica se vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Entrambi i modelli `Network access: Do not allow anonymous enumeration of SAM accounts` e. `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti Criteri di gruppo sono disattivati.
  - Gruppi con restrizioni

È possibile configurare gruppi con restrizioni per gestire centralmente l'appartenenza a gruppi integrati o definiti dall'utente. Quando si applica un gruppo con restrizioni tramite un criterio di gruppo, l'appartenenza di un gruppo locale del server CIFS viene impostata automaticamente in modo che corrisponda alle impostazioni dell'elenco di appartenenze definite nel criterio di gruppo applicato.

Impostare utilizzando `Restricted Groups` GPO.

- Impostazioni dei criteri di accesso centrale

  Specifica un elenco di criteri di accesso centrale. I criteri di accesso centrale e le relative regole dei criteri di accesso centrale determinano le autorizzazioni di accesso per più file sulla SVM.

**Informazioni correlate**

Attivazione o disattivazione del supporto GPO su un server CIFS

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

"Controllo SMB e NFS e tracciamento della sicurezza"

Modifica delle impostazioni di sicurezza Kerberos del server CIFS

Utilizzo di BranchCache per memorizzare nella cache SMB i contenuti vengono condivisi in una filiale

Utilizzo della firma SMB per migliorare la sicurezza della rete

Configurazione del controllo incrociato bypass

Configurazione delle restrizioni di accesso per utenti anonimi

## Requisiti per l'utilizzo degli oggetti Criteri di gruppo con il server SMB

Per utilizzare gli oggetti Criteri di gruppo (GPO) con il server SMB, il sistema deve soddisfare diversi requisiti.

- SMB deve essere concesso in licenza sul cluster. La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.
- Un server SMB deve essere configurato e collegato a un dominio Active Directory di Windows.
- Lo stato dell'amministratore del server SMB deve essere attivo.
- Gli oggetti Criteri di gruppo devono essere configurati e applicati all'unità organizzativa (OU) di Windows Active Directory contenente l'oggetto computer server SMB.
- Il supporto GPO deve essere attivato sul server SMB.

## Attivare o disattivare il supporto GPO su un server CIFS

È possibile attivare o disattivare il supporto degli oggetti Criteri di gruppo (GPO) su un server CIFS. Se si attiva il supporto GPO su un server CIFS, gli oggetti Criteri di gruppo applicabili definiti nel criterio di gruppo, ovvero il criterio applicato all'unità organizzativa (OU) che contiene l'oggetto computer server CIFS, vengono applicati al server CIFS.

**A proposito di questa attività**

I GPO non possono essere abilitati sui server CIFS in modalità workgroup.

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera… | Immettere il comando… |
|---|---|
| Abilitare gli oggetti Criteri di gruppo | `vserver cifs group-policy modify -vserver vserver_name -status enabled` |
| Disattivare gli oggetti Criteri di gruppo | `vserver cifs group-policy modify -vserver vserver_name -status disabled` |

2. Verificare che il supporto GPO sia nello stato desiderato: `vserver cifs group-policy show -vserver +vserver_name_`

   Lo stato dei criteri di gruppo per i server CIFS in modalità gruppo di lavoro viene visualizzato come “disabled”.

**Esempio**

L’esempio seguente abilita il supporto GPO su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

**Informazioni correlate**

GPO supportati

Requisiti per l’utilizzo degli oggetti Criteri di gruppo con il server CIFS

Come vengono aggiornati gli oggetti Criteri di gruppo sul server CIFS

Aggiornamento manuale delle impostazioni dell’oggetto Criteri di gruppo sul server CIFS

Visualizzazione delle informazioni sulle configurazioni dell’oggetto Criteri di gruppo

## Modalità di aggiornamento degli oggetti Criteri di gruppo sul server SMB

### Come vengono aggiornati gli oggetti Criteri di gruppo nella panoramica del server CIFS

Per impostazione predefinita, ONTAP recupera e applica le modifiche dell’oggetto Criteri di gruppo ogni 90 minuti. Le impostazioni di sicurezza vengono aggiornate ogni 16 ore.

Se si desidera aggiornare gli oggetti Criteri di gruppo per applicare le nuove impostazioni dei criteri dell'oggetto Criteri di gruppo prima che ONTAP li aggiorni automaticamente, è possibile attivare un aggiornamento manuale su un server CIFS con un comando ONTAP.

- Per impostazione predefinita, tutti gli oggetti Criteri di gruppo vengono verificati e aggiornati in base alle necessità ogni 90 minuti.

  Questo intervallo è configurabile e può essere impostato utilizzando `Refresh interval` e. `Random offset` Impostazioni dell'oggetto Criteri di gruppo.

  ONTAP interroga Active Directory per le modifiche apportate agli oggetti Criteri di gruppo. Se i numeri di versione dell'oggetto Criteri di gruppo registrati in Active Directory sono superiori a quelli del server CIFS, ONTAP recupera e applica i nuovi oggetti Criteri di gruppo. Se i numeri di versione sono gli stessi, gli oggetti Criteri di gruppo sul server CIFS non vengono aggiornati.

- Gli oggetti Criteri di gruppo delle impostazioni di sicurezza vengono aggiornati ogni 16 ore.

  ONTAP recupera e applica gli oggetti Criteri di gruppo delle impostazioni di protezione ogni 16 ore, indipendentemente dal fatto che questi oggetti Criteri di gruppo siano stati modificati o meno.

  > Il valore predefinito di 16 ore non può essere modificato nella versione corrente di ONTAP. Si tratta di un'impostazione predefinita del client Windows.

- Tutti gli oggetti Criteri di gruppo possono essere aggiornati manualmente con un comando ONTAP.

  Questo comando simula le finestre `gpupdate.exe`/force` command.

**Informazioni correlate**

Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

## Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

Se si desidera aggiornare immediatamente le impostazioni dell'oggetto Criteri di gruppo (GPO) sul server CIFS, è possibile aggiornare manualmente le impostazioni. È possibile aggiornare solo le impostazioni modificate oppure forzare un aggiornamento per tutte le impostazioni, incluse quelle applicate in precedenza ma non modificate.

**Fase**

1. Eseguire l'azione appropriata:

| Se si desidera eseguire l'aggiornamento… | Immettere il comando… |
|---|---|
| Impostazioni GPO modificate | `vserver cifs group-policy update -vserver` *`vserver_name`* |

| Se si desidera eseguire l'aggiornamento… | Immettere il comando… |
|---|---|
| Tutte le impostazioni dell'oggetto Criteri di gruppo | `vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true` |

#### Informazioni correlate

Come vengono aggiornati gli oggetti Criteri di gruppo sul server CIFS

## Visualizza informazioni sulle configurazioni dell'oggetto Criteri di gruppo

È possibile visualizzare informazioni sulle configurazioni degli oggetti Criteri di gruppo (GPO) definite in Active Directory e sulle configurazioni degli oggetti Criteri di gruppo applicate al server CIFS.

#### A proposito di questa attività

È possibile visualizzare informazioni su tutte le configurazioni GPO definite in Active Directory del dominio a cui appartiene il server CIFS oppure solo sulle configurazioni GPO applicate a un server CIFS.

#### Fasi

1. Visualizzare le informazioni sulle configurazioni dell'oggetto Criteri di gruppo eseguendo una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su tutte le configurazioni di Criteri di gruppo… | Immettere il comando… |
|---|---|
| Definito in Active Directory | `vserver cifs group-policy show-defined -vserver vserver_name` |
| Applicato a una SVM (Storage Virtual Machine) abilitata per CIFS | `vserver cifs group-policy show-applied -vserver vserver_name` |

#### Esempio

Nell'esempio seguente vengono visualizzate le configurazioni GPO definite in Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

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

```
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache : version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
```

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

Nell’esempio seguente vengono visualizzate le configurazioni GPO applicate a SVM vs1 abilitato CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
```

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

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

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

**Informazioni correlate**

Attivazione o disattivazione del supporto GPO su un server CIFS

## Visualizzare informazioni dettagliate sugli oggetti GPO di gruppo con restrizioni

È possibile visualizzare informazioni dettagliate sui gruppi con restrizioni definiti come oggetti Criteri di gruppo (GPO) in Active Directory e applicati al server CIFS.

**A proposito di questa attività**

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del criterio di gruppo
- Versione dei criteri di gruppo
- Collegamento

  Specifica il livello di configurazione dei criteri di gruppo. I valori di output possibili includono:

  - `Local` Quando il criterio di gruppo è configurato in ONTAP

- `Site` quando il criterio di gruppo è configurato a livello di sito nel controller di dominio
- `Domain` quando il criterio di gruppo è configurato a livello di dominio nel controller di dominio
- `OrganizationalUnit` Quando il criterio di gruppo è configurato a livello di unità organizzativa (OU) nel controller di dominio
- `RSOP` per l'insieme risultante di criteri derivati da tutti i criteri di gruppo definiti a vari livelli

- Nome del gruppo con restrizioni
- Gli utenti e i gruppi che appartengono al gruppo con restrizioni e che non ne fanno parte
- L'elenco dei gruppi a cui viene aggiunto il gruppo con restrizioni

  Un gruppo può essere un membro di gruppi diversi dai gruppi elencati qui.

**Fase**

1. Visualizzare le informazioni su tutti gli oggetti Criteri di gruppo con restrizioni eseguendo una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su tutti gli oggetti Criteri di gruppo con restrizioni… | Immettere il comando… |
|---|---|
| Definito in Active Directory | `vserver cifs group-policy restricted-group show-defined -vserver vserver_name` |
| Applicato a un server CIFS | `vserver cifs group-policy restricted-group show-applied -vserver vserver_name` |

**Esempio**

Nell'esempio seguente vengono visualizzate informazioni sugli oggetti Criteri di gruppo con restrizioni definiti nel dominio Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

Nell'esempio seguente vengono visualizzate informazioni sui GPO a gruppi limitati applicati a SVM vs1 abilitato a CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

**Informazioni correlate**

## Visualizza informazioni sui criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sui criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sui criteri di accesso centrale applicati al server CIFS tramite oggetti Criteri di gruppo (GPO).

**A proposito di questa attività**

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome SVM
- Nome della policy di accesso centrale
- SID
- Descrizione
- Tempo di creazione
- Tempo di modifica
- Regole dei membri

> I server CIFS in modalità gruppo di lavoro non vengono visualizzati perché non supportano gli oggetti Criteri di gruppo.

**Fase**

1. Visualizzare le informazioni sui criteri di accesso centrale eseguendo una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su tutti i criteri di accesso centrale… | Immettere il comando… |
|---|---|
| Definito in Active Directory | `vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`* |
| Applicato a un server CIFS | `vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`* |

**Esempio**

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale definiti in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Nell’esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale applicati alle macchine virtuali dello storage (SVM) sul cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

**Informazioni correlate**

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

## Visualizza informazioni sulle regole dei criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sulle regole dei criteri di accesso centrale applicate al server CIFS attraverso gli oggetti Criteri di gruppo (GPO) dei criteri di accesso centrale.

### A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale definite e applicate. Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del server virtuale
- Nome della regola di accesso centrale
- Descrizione
- Tempo di creazione
- Tempo di modifica
- Permessi correnti
- Permessi proposti
- Risorse di destinazione

| Se si desidera visualizzare informazioni su tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale… | Immettere il comando… |
|---|---|
| Definito in Active Directory | `vserver cifs group-policy central-access-rule show-defined -vserver vserver_name` |
| Applicato a un server CIFS | `vserver cifs group-policy central-access-rule show-applied -vserver vserver_name` |

### Esempio

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale applicati alle macchine virtuali di storage (SVM) sul cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

**Informazioni correlate**

Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso (DAC)

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

# Comandi per la gestione delle password degli account dei computer dei server SMB

È necessario conoscere i comandi per la modifica, la reimpostazione e la disattivazione delle password e per la configurazione delle pianificazioni degli aggiornamenti automatici. È inoltre possibile configurare una pianificazione sul server SMB per aggiornarla automaticamente.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Modificare o reimpostare la password dell'account di dominio e conoscerla | `vserver cifs domain password change` |
| Reimpostare la password dell'account di dominio e non si conosce la password | `vserver cifs domain password reset` |
| Configurare i server SMB per la modifica automatica della password dell'account del computer | `vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true` |
| Disattiva le modifiche automatiche della password dell'account del computer sui server SMB | `vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false` |

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

# Gestire le connessioni dei controller di dominio

## Visualizza le informazioni sui server rilevati

È possibile visualizzare le informazioni relative ai server LDAP e ai controller di dominio rilevati sul server CIFS.

### Fase

1. Per visualizzare le informazioni relative ai server rilevati, immettere il seguente comando: `vserver cifs domain discovered-servers show`

### Esempio

L'esempio seguente mostra i server rilevati per SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

**Informazioni correlate**

Ripristino e riscoperta dei server

Interruzione o avvio del server CIFS

## Reimpostare e riscoprire i server

La reimpostazione e la riscoperta dei server sul server CIFS consentono al server CIFS di eliminare le informazioni memorizzate sui server LDAP e sui controller di dominio. Dopo aver scartato le informazioni sul server, il server CIFS acquisisce nuovamente le informazioni correnti su questi server esterni. Questa operazione può essere utile quando i server connessi non rispondono in modo appropriato.

**Fasi**

1. Immettere il seguente comando: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Visualizzare le informazioni sui server appena rilevati: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

**Esempio**

Nell'esempio riportato di seguito vengono ripristinati e riutilizzati i server per la macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

**Informazioni correlate**

Visualizzazione delle informazioni sui server rilevati

Interruzione o avvio del server CIFS

## Gestire il rilevamento dei controller di dominio

A partire da ONTAP 9.3, è possibile modificare il processo predefinito in base al quale vengono rilevati i controller di dominio (DC). In questo modo, è possibile limitare il rilevamento al sito o a un pool di controller di dominio preferiti, con conseguente miglioramento delle performance a seconda dell'ambiente.

**A proposito di questa attività**

Per impostazione predefinita, il processo di rilevamento dinamico rileva tutti i controller di dominio disponibili, inclusi i controller di dominio preferiti, tutti i controller di dominio nel sito locale e tutti i controller di dominio remoti. Questa configurazione può portare a latenza nell'autenticazione e nell'accesso alle condivisioni in alcuni ambienti. Se il pool di controller di dominio che si desidera utilizzare è già stato determinato o se i controller di dominio remoti sono inadeguati o inaccessibili, è possibile modificare il metodo di ricerca.

In ONTAP 9.3 e versioni successive, il `discovery-mode` del parametro `cifs domain discovered-servers` il comando consente di selezionare una delle seguenti opzioni di ricerca:

- Vengono rilevati tutti i controller di dominio del dominio.
- Vengono rilevati solo i controller di dominio nel sito locale.

  Il `default-site` È possibile definire un parametro per il server SMB in modo da utilizzare questa modalità con le LIF non assegnate a un sito in siti e servizi.

- Il rilevamento dei server non viene eseguito, la configurazione dei server SMB dipende solo dai controller di dominio preferiti.

  Per utilizzare questa modalità, è necessario prima definire i controller di dominio preferiti per il server SMB.

#### Fase

1. Specificare l'opzione di ricerca desiderata: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Opzioni per `mode` parametro:

   - `all`

     Rilevare tutti i controller di dominio disponibili (impostazione predefinita).

   - `site`

     Limita il rilevamento DC al tuo sito.

   - `none`

     Utilizzare solo i controller di dominio preferiti e non eseguire il rilevamento.

## Aggiungere i domain controller preferiti

ONTAP rileva automaticamente i controller di dominio tramite DNS. In alternativa, è possibile aggiungere uno o più domain controller all'elenco dei domain controller preferiti per un dominio specifico.

#### A proposito di questa attività

Se esiste già un elenco di controller di dominio preferito per il dominio specificato, il nuovo elenco viene Unito all'elenco esistente.

#### Fase

1. Per aggiungere all'elenco dei domain controller preferiti, immettere il seguente comando: `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Specifica il nome della SVM (Storage Virtual Machine).

   `-domain` *`domain_name`* Specifica il nome Active Directory completo del dominio a cui appartengono i controller di dominio specificati.

   `-preferred-dc` *`IP_address`*,… Specifica uno o più indirizzi IP dei domain controller preferiti, come elenco delimitato da virgole, in ordine di preferenza.

#### Esempio

Il seguente comando aggiunge i domain controller 172.17.102.25 e 172.17.102.24 all'elenco dei domain controller preferiti che il server SMB su SVM vs1 utilizza per gestire l'accesso esterno al dominio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

**Informazioni correlate**

Comandi per la gestione dei domain controller preferiti

## Comandi per la gestione dei domain controller preferiti

È necessario conoscere i comandi per aggiungere, visualizzare e rimuovere i domain controller preferiti.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Aggiungere un domain controller preferito | `vserver cifs domain preferred-dc add` |
| Visualizzare i domain controller preferiti | `vserver cifs domain preferred-dc show` |
| Rimuovere un domain controller preferito | `vserver cifs domain preferred-dc remove` |

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

**Informazioni correlate**

Aggiunta di domain controller preferiti

## Abilitare le connessioni SMB2 ai controller di dominio

A partire da ONTAP 9.1, è possibile abilitare SMB versione 2.0 per la connessione a un controller di dominio. Questa operazione è necessaria se SMB 1.0 è stato disattivato nei controller di dominio. A partire da ONTAP 9.2, SMB2 è attivato per impostazione predefinita.

**A proposito di questa attività**

Il `smb2-enabled-for-dc-connections` L'opzione Command (comando) attiva l'impostazione predefinita di sistema per la release di ONTAP in uso. L'impostazione predefinita di sistema per ONTAP 9.1 è attivata per SMB 1.0 e disattivata per SMB 2.0. L'impostazione predefinita di sistema per ONTAP 9.2 è Enabled (attivato) per SMB 1.0 e Enabled (attivato) per SMB 2.0. Se il controller di dominio non riesce a negoziare inizialmente SMB 2.0, utilizza SMB 1.0.

SMB 1.0 può essere disattivato da ONTAP a un controller di dominio. In ONTAP 9.1, se SMB 1.0 è stato disattivato, SMB 2.0 deve essere attivato per comunicare con un controller di dominio.

Scopri di più su:

- "Verifica delle versioni SMB abilitate".
- "Versioni e funzionalità SMB supportate".

> Se `-smb1-enabled-for-dc-connections` è impostato su `false` mentre `-smb1-enabled` è impostato su `true`, ONTAP nega le connessioni SMB 1.0 come client, ma continua ad accettare connessioni SMB 1.0 in entrata come server.

**Fasi**

1. Prima di modificare le impostazioni di sicurezza SMB, verificare quali versioni SMB sono abilitate: `vserver cifs security show`
2. Scorrere l'elenco per visualizzare le versioni SMB.
3. Eseguire il comando appropriato utilizzando `smb2-enabled-for-dc-connections` opzione.

| Se vuoi che SMB2 sia… | Immettere il comando… |
|---|---|
| Attivato | `vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true` |
| Disattivato | `vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false` |

### Abilitare le connessioni crittografate ai controller di dominio

A partire da ONTAP 9.8, è possibile specificare che le connessioni ai controller di dominio siano crittografate.

#### A proposito di questa attività

ONTAP richiede la crittografia per le comunicazioni del controller di dominio (DC) quando `-encryption -required-for-dc-connection` l'opzione è impostata su `true`; il valore predefinito è `false`. Quando l'opzione è impostata, per le connessioni ONTAP-DC verrà utilizzato solo il protocollo SMB3, in quanto la crittografia è supportata solo da SMB3.

Quando sono richieste comunicazioni DC crittografate, il `-smb2-enabled-for-dc-connections` L'opzione viene ignorata, perché ONTAP negozia solo le connessioni SMB3. Se un controller di dominio non supporta SMB3 e la crittografia, ONTAP non si connetterà con esso.

#### Fase

1. Abilitare la comunicazione crittografata con il controller di dominio: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

## Utilizza sessioni null per accedere allo storage in ambienti non Kerberos

### Utilizza sessioni null per accedere alla panoramica dello storage in ambienti non Kerberos

L'accesso a sessione nulla fornisce le autorizzazioni per le risorse di rete, ad esempio i dati del sistema di storage, e per i servizi basati su client eseguiti nel sistema locale. Una sessione nulla si verifica quando un processo client utilizza l'account "System `s`" per accedere a una risorsa di rete. La configurazione della sessione Null è specifica per l'autenticazione non Kerberos.

## Modalità con cui il sistema storage fornisce l'accesso alla sessione Null

Poiché le condivisioni di sessione null non richiedono l'autenticazione, i client che richiedono l'accesso di sessione null devono avere i propri indirizzi IP mappati sul sistema di storage.

Per impostazione predefinita, i client di sessione Null non mappati possono accedere a determinati servizi di sistema ONTAP, ad esempio l'enumerazione delle condivisioni, ma non possono accedere ai dati del sistema di storage.

> ONTAP supporta i valori di impostazione anonimi del Registro di sistema con Windows RestrictAnonymous `-restrict-anonymous` opzione. Ciò consente di controllare in che misura gli utenti Null non mappati possono visualizzare o accedere alle risorse di sistema. Ad esempio, è possibile disattivare l'enumerazione delle condivisioni e l'accesso alla condivisione IPC (la condivisione named pipe nascosta). Il `vserver cifs options modify` e. `vserver cifs options show` le pagine man forniscono ulteriori informazioni su `-restrict-anonymous` opzione.

Se non diversamente configurato, un client che esegue un processo locale che richiede l'accesso al sistema di storage attraverso una sessione Null è membro solo di gruppi non restrittivi, come "Everyone". Per limitare l'accesso a sessioni Null alle risorse del sistema di storage selezionate, è possibile creare un gruppo a cui appartengono tutti i client di sessione Null; la creazione di questo gruppo consente di limitare l'accesso al sistema di storage e di impostare le autorizzazioni delle risorse del sistema di storage che si applicano specificamente ai client di sessione Null.

ONTAP fornisce una sintassi di mappatura in `vserver name-mapping` Set di comandi per specificare l'indirizzo IP dei client che hanno consentito l'accesso alle risorse del sistema di storage utilizzando una sessione utente nulla. Dopo aver creato un gruppo per utenti Null, è possibile specificare le restrizioni di accesso per le risorse del sistema di storage e le autorizzazioni delle risorse che si applicano solo alle sessioni Null. L'utente nullo viene identificato come accesso anonimo. Gli utenti Null non hanno accesso ad alcuna home directory.

A qualsiasi utente nullo che accede al sistema di storage da un indirizzo IP mappato vengono concesse autorizzazioni utente mappate. Prendere in considerazione le precauzioni appropriate per impedire l'accesso non autorizzato ai sistemi di storage mappati con utenti nulli. Per la massima protezione, posizionare il sistema di storage e tutti i client che richiedono l'accesso al sistema di storage utente nullo su una rete separata, per eliminare la possibilità di indirizzo IP "spoofing".

**Informazioni correlate**

Configurazione delle restrizioni di accesso per utenti anonimi

## Concedere agli utenti Null l'accesso alle condivisioni del file system

È possibile consentire l'accesso alle risorse del sistema di storage da parte di client di sessione Null assegnando un gruppo da utilizzare da parte di client di sessione Null e registrando gli indirizzi IP dei client di sessione Null da aggiungere all'elenco dei client del sistema di storage autorizzati ad accedere ai dati utilizzando sessioni Null.

**Fasi**

1. Utilizzare `vserver name-mapping create` Comando per mappare l'utente Null a qualsiasi utente Windows valido, con un qualificatore IP.

Il seguente comando associa l'utente null a user1 con un nome host valido google.com:

```
vserver name-mapping create –direction win-unix  -position 1 –pattern
"ANONYMOUS LOGON" –replacement user1 – hostname google.com
```

Il seguente comando associa l'utente null a user1 con un indirizzo IP valido 10.238.2.54/32:

```
vserver name-mapping create –direction win-unix  -position 2 –pattern
"ANONYMOUS LOGON" –replacement user1 –address 10.238.2.54/32
```

2. Utilizzare `vserver name-mapping show` per confermare la mappatura dei nomi.

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                         Replacement: user1
```

3. Utilizzare `vserver cifs options modify –win-name-for-null-user` Comando per assegnare l'appartenenza a Windows all'utente Null.

   Questa opzione è applicabile solo quando esiste una mappatura nome valida per l'utente Null.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilizzare `vserver cifs options show` Per confermare la mappatura dell'utente nullo all'utente o al gruppo Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

# Gestire gli alias NetBIOS per i server SMB

## Panoramica sulla gestione degli alias NetBIOS per i server SMB

Gli alias NetBIOS sono nomi alternativi per il server SMB che i client SMB possono utilizzare quando si connettono al server SMB. La configurazione degli alias NetBIOS per un server SMB può essere utile quando si consolidano i dati da altri file server nel server SMB e si desidera che il server SMB risponda ai nomi dei file server originali.

È possibile specificare un elenco di alias NetBIOS quando si crea il server SMB o in qualsiasi momento dopo la creazione del server SMB. È possibile aggiungere o rimuovere alias NetBIOS dall'elenco in qualsiasi momento. È possibile connettersi al server SMB utilizzando uno dei nomi presenti nell'elenco degli alias NetBIOS.

#### Informazioni correlate

Visualizzazione di informazioni su connessioni NetBIOS su TCP

## Aggiungere un elenco di alias NetBIOS al server SMB

Se si desidera che i client SMB si connettano al server SMB utilizzando un alias, è possibile creare un elenco di alias NetBIOS oppure aggiungere alias NetBIOS a un elenco esistente di alias NetBIOS.

#### A proposito di questa attività

- Il nome alias NetBIOS può contenere fino a 15 caratteri.
- È possibile configurare fino a 200 alias NetBIOS sul server SMB.
- I seguenti caratteri non sono consentiti:

  @ * ( ) = + [ ] | ; : " , < > / ?

#### Fasi

1. Aggiungere gli alias NetBIOS:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - È possibile specificare uno o più alias NetBIOS utilizzando un elenco delimitato da virgole.
   - Gli alias NetBIOS specificati vengono aggiunti all'elenco esistente.
   - Se l'elenco è vuoto, viene creato un nuovo elenco di alias NetBIOS.
2. Verificare che gli alias NetBIOS siano stati aggiunti correttamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

**Informazioni correlate**

Rimozione degli alias NetBIOS dall'elenco degli alias NetBIOS

Visualizzazione dell'elenco degli alias NetBIOS sui server CIFS

## Rimuovere gli alias NetBIOS dall'elenco degli alias NetBIOS

Se non sono necessari alias NetBIOS specifici per un server CIFS, è possibile rimuovere tali alias NetBIOS dall'elenco. È inoltre possibile rimuovere tutti gli alias NetBIOS dall'elenco.

**A proposito di questa attività**

È possibile rimuovere più alias NetBIOS utilizzando un elenco delimitato da virgole. È possibile rimuovere tutti gli alias NetBIOS su un server CIFS specificando – come valore per `-netbios-aliases` parametro.

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera rimuovere… | Inserisci… |
|---|---|
| Alias NetBIOS specifici dall'elenco | `vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...` |
| Tutti gli alias NetBIOS dall'elenco | `vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -` |

   `vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1`

2. Verificare che gli alias NetBIOS specificati siano stati rimossi: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

   `vserver cifs show -vserver vs1 -display-netbios-aliases`

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

## Visualizza l'elenco degli alias NetBIOS sui server CIFS

È possibile visualizzare l'elenco degli alias NetBIOS. Ciò può essere utile quando si desidera determinare l'elenco di nomi sui quali i client SMB possono stabilire connessioni al server CIFS.

**Fase**

1. Eseguire una delle seguenti operazioni:

| Se si desidera visualizzare informazioni su… | Inserisci… |
|---|---|
| Alias NetBIOS di un server CIFS | `vserver cifs show -display-netbios -aliases` |
| L'elenco degli alias NetBIOS come parte delle informazioni dettagliate sul server CIFS | `vserver cifs show -instance` |

Nell'esempio seguente vengono visualizzate informazioni sugli alias NetBIOS di un server CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Nell'esempio seguente viene visualizzato l'elenco degli alias NetBIOS come parte delle informazioni dettagliate sul server CIFS:

```
vserver cifs show -instance
```

```
                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Per ulteriori informazioni, consulta la pagina man per i comandi.

**Informazioni correlate**

Aggiunta di un elenco di alias NetBIOS al server CIFS

## Determinare se i client SMB sono connessi utilizzando alias NetBIOS

È possibile determinare se i client SMB sono connessi utilizzando alias NetBIOS e, in tal caso, quale alias NetBIOS viene utilizzato per stabilire la connessione. Ciò può essere utile per la risoluzione dei problemi di connessione.

### A proposito di questa attività

È necessario utilizzare `-instance` Parametro per visualizzare l'alias NetBIOS (se presente) associato a una connessione SMB. Se il nome del server CIFS o un indirizzo IP viene utilizzato per effettuare la connessione SMB, l'output di `NetBIOS Name` il campo è - (trattino).

### Fase

1. Eseguire l'azione desiderata:

| Se si desidera visualizzare le informazioni NetBIOS per… | Inserisci… |
|---|---|
| Connessioni SMB | `vserver cifs session show -instance` |
| Connessioni che utilizzano un alias NetBIOS specificato: | `vserver cifs session show -instance -netbios-name` *`netbios_name`* |

Nell'esempio seguente vengono visualizzate informazioni sull'alias NetBIOS utilizzato per stabilire la connessione SMB con ID sessione 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                  Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

# Gestire varie attività del server SMB

## Arrestare o avviare il server CIFS

È possibile arrestare il server CIFS su una SVM, che può essere utile quando si eseguono attività mentre gli utenti non accedono ai dati tramite le condivisioni SMB. È possibile riavviare l'accesso SMB avviando il server CIFS. Arrestando il server CIFS, è anche possibile modificare i protocolli consentiti sulla macchina virtuale di storage (SVM).

**Fasi**

1. Eseguire una delle seguenti operazioni:

| Se si desidera… | Immettere il comando… |
|---|---|
| Arrestare il server CIFS | `vserver cifs stop -vserver *vserver_name* [-foreground {true |
| false}]` | Avviare il server CIFS |
| `vserver cifs start -vserver *vserver_name* [-foreground {true | false}]` |

`-foreground` specifica se il comando deve essere eseguito in primo piano o in background. Se non si inserisce questo parametro, viene impostato su `true`e il comando viene eseguito in primo piano.

2. Verificare che lo stato amministrativo del server CIFS sia corretto utilizzando `vserver cifs show` comando.

**Esempio**

I seguenti comandi avviano il server CIFS su SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                            Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                  NetBIOS Domain/Workgroup Name: DOMAIN
                    Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

**Informazioni correlate**

Visualizzazione delle informazioni sui server rilevati

Ripristino e riscoperta dei server

## Spostare i server CIFS in diverse unità organizzative

Il processo di creazione del server CIFS utilizza l'unità organizzativa predefinita (OU) CN=computer durante l'installazione, a meno che non si specifichi un'unità organizzativa diversa. Dopo l'installazione, è possibile spostare i server CIFS in diverse unità organizzative.

**Fasi**

1. Sul server Windows, aprire la struttura **utenti e computer di Active Directory**.
2. Individuare l'oggetto Active Directory per la macchina virtuale di storage (SVM).
3. Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Sposta**.
4. Selezionare l'unità organizzativa che si desidera associare alla SVM

**Risultati**

L'oggetto SVM viene posizionato nell'unità organizzativa selezionata.

## Modificare il dominio DNS dinamico sulla SVM prima di spostare il server SMB

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS del server SMB in DNS quando si sposta il server SMB in un altro dominio, è necessario modificare il DNS dinamico (DDNS) sulla macchina virtuale di storage (SVM) prima di spostare il server SMB.

#### Prima di iniziare

I servizi dei nomi DNS devono essere modificati sulla SVM per utilizzare il dominio DNS che contiene i record di posizione del servizio per il nuovo dominio che conterrà l'account del computer del server SMB. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory.

#### A proposito di questa attività

Sebbene DDNS (se configurato su SVM) aggiunga automaticamente i record DNS per i LIF dei dati al nuovo dominio, i record DNS per il dominio originale non vengono cancellati automaticamente dal server DNS originale. È necessario eliminarli manualmente.

Per completare le modifiche DDNS prima di spostare il server SMB, consultare il seguente argomento:

"Configurare i servizi DNS dinamici"

## Aggiungere una SVM a un dominio Active Directory

È possibile unire una macchina virtuale di storage (SVM) a un dominio Active Directory senza eliminare il server SMB esistente modificando il dominio utilizzando `vserver cifs modify` comando. È possibile riconnessione al dominio corrente o aggiungerne uno nuovo.

#### Prima di iniziare

- La SVM deve già disporre di una configurazione DNS.
- La configurazione DNS per la SVM deve essere in grado di servire il dominio di destinazione.

  I server DNS devono contenere i record di posizione del servizio (SRV) per i server LDAP e controller di dominio del dominio.

#### A proposito di questa attività

- Lo stato amministrativo del server CIFS deve essere impostato su "dOwn" per procedere con la modifica del dominio Active Directory.
- Se il comando viene completato correttamente, lo stato amministrativo viene automaticamente impostato su "up".
- Quando si unisce un dominio, il completamento di questo comando potrebbe richiedere alcuni minuti.

#### Fasi

1. Unire la SVM al dominio del server CIFS: `vserver cifs modify -vserver *vserver_name* -domain *domain_name* -status-admin down`

   Per ulteriori informazioni, vedere la pagina man di `vserver cifs modify` comando. Per riconfigurare il DNS per il nuovo dominio, consultare la pagina man del `vserver dns modify` comando.

   Per creare un account macchina Active Directory per il server SMB, è necessario fornire il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer a `ou= *example* ou` container all'interno di `*example*`dominio .com.

   A partire da ONTAP 9.7, l'amministratore ad può fornire un URI a un file keytab in alternativa a un nome e una password a un account Windows con privilegi. Quando si riceve l'URI, includerlo in `-keytab-uri` con il `vserver cifs` comandi.

2. Verificare che il server CIFS si trovi nel dominio Active Directory desiderato: `vserver cifs show`

**Esempio**

Nell'esempio seguente, il server SMB "CIFSSERVER1" su SVM vs1 si unisce al dominio example.com utilizzando l'autenticazione keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

## Visualizza informazioni su connessioni NetBIOS su TCP

È possibile visualizzare informazioni sulle connessioni NetBIOS su TCP (NBT). Ciò può essere utile per la risoluzione dei problemi relativi a NetBIOS.

**Fase**

1. Utilizzare `vserver cifs nbtstat` Comando per visualizzare informazioni su NetBIOS su connessioni TCP.

> NBNS (NetBIOS name service) su IPv6 non supportato.

**Esempio**

L'esempio seguente mostra le informazioni sul servizio nome NetBIOS visualizzate per "cluster1":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

### Comandi per la gestione dei server SMB

È necessario conoscere i comandi per la creazione, la visualizzazione, la modifica, l'arresto, l'avvio, Ed eliminazione dei server SMB. Sono inoltre disponibili comandi per reimpostare e riscoprire i server, modificare o reimpostare le password degli account dei computer, pianificare le modifiche per le password degli account dei computer e aggiungere o rimuovere alias NetBIOS.

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Creare un server SMB | `vserver cifs create` |
| Visualizzare le informazioni su un server SMB | `vserver cifs show` |
| Modificare un server SMB | `vserver cifs modify` |

| | |
|---|---|
| Spostare un server SMB in un altro dominio | `vserver cifs modify` |
| Arrestare un server SMB | `vserver cifs stop` |
| Avviare un server SMB | `vserver cifs start` |
| Eliminare un server SMB | `vserver cifs delete` |
| Reimpostare e riscoprire i server per il server SMB | `vserver cifs domain discovered-servers reset-servers` |
| Modificare la password dell'account del computer del server SMB | `vserver cifs domain password change` |
| Reimpostare la password dell'account del computer del server SMB | `vserver cifs domain password change` |
| Pianificare le modifiche automatiche delle password per l'account del computer del server SMB | `vserver cifs domain password schedule modify` |
| Aggiungere alias NetBIOS per il server SMB | `vserver cifs add-netbios-aliases` |
| Rimuovere gli alias NetBIOS per il server SMB | `vserver cifs remove-netbios-aliases` |

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

**Informazioni correlate**

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

## Attivare il servizio NetBIOS name

A partire da ONTAP 9, il servizio nomi NetBIOS (NBNS, a volte chiamato Windows Internet Name Service o WINS) è disattivato per impostazione predefinita. In precedenza, le SVM (Storage Virtual Machine) abilitate per CIFS inviavano trasmissioni di registrazione dei nomi indipendentemente dal fatto che WINS fosse abilitato o meno in una rete. Per limitare tali trasmissioni alle configurazioni in cui è richiesto NBNS, è necessario abilitare NBNS esplicitamente per i nuovi server CIFS.

**Prima di iniziare**

- Se si utilizza già NBNS e si esegue l'aggiornamento a ONTAP 9, non è necessario completare questa attività. NBNS continuerà a funzionare come prima.
- NBNS è abilitato su UDP (porta 137).
- NBNS su IPv6 non supportato.

**Fasi**

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

```
set -privilege advanced
```

2. Abilitare NBNS su un server CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Tornare al livello di privilegio admin.

```
set -privilege admin
```

# Utilizza IPv6 per l'accesso SMB e i servizi SMB

## Requisiti per l'utilizzo di IPv6

Prima di poter utilizzare IPv6 sul server SMB, è necessario sapere quali versioni di ONTAP e SMB lo supportano e quali sono i requisiti di licenza.

### Requisiti di licenza ONTAP

Non è richiesta alcuna licenza speciale per IPv6 quando SMB è concesso in licenza. La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

### Requisiti di versione del protocollo SMB

- Per le SVM, ONTAP supporta IPv6 su tutte le versioni del protocollo SMB.

> NBNS (NetBIOS name service) su IPv6 non supportato.

## Supporto per IPv6 con accesso SMB e servizi CIFS

Se si desidera utilizzare IPv6 sul server CIFS, è necessario conoscere il modo in cui ONTAP supporta IPv6 per l'accesso SMB e la comunicazione di rete per i servizi CIFS.

### Supporto di client e server Windows

ONTAP fornisce supporto per server e client Windows che supportano IPv6. Di seguito viene descritto il supporto IPv6 del client e del server Microsoft Windows:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e versioni successive supportano IPv6 sia per la condivisione di file SMB che per i servizi Active Directory, inclusi i servizi DNS, LDAP, CLDAP e Kerberos.

Se gli indirizzi IPv6 sono configurati, Windows 7 e Windows Server 2008 e versioni successive utilizzano IPv6 per impostazione predefinita per i servizi Active Directory. Sono supportate sia l'autenticazione NTLM che Kerberos su connessioni IPv6.

Tutti i client Windows supportati da ONTAP possono connettersi alle condivisioni SMB utilizzando gli indirizzi IPv6.

Per informazioni aggiornate sui client Windows supportati da ONTAP, vedere la "Matrice di interoperabilità".

I domini NT non sono supportati per IPv6.

**Supporto di servizi CIFS aggiuntivi**

Oltre al supporto IPv6 per le condivisioni di file SMB e i servizi Active Directory, ONTAP fornisce il supporto IPv6 per:

- Servizi lato client, tra cui cartelle offline, profili di roaming, reindirizzamento cartelle e versioni precedenti
- Servizi lato server, tra cui home directory dinamiche (funzionalità home directory), symlink e Widelink, BranchCache, offload delle copie ODX, riferimenti automatici dei nodi, E versioni precedenti
- Servizi di gestione dell'accesso ai file, tra cui l'utilizzo di utenti e gruppi locali di Windows per il controllo degli accessi e la gestione dei diritti, l'impostazione delle autorizzazioni dei file e dei criteri di controllo mediante la CLI, il tracciamento della sicurezza, la gestione dei blocchi dei file e il monitoraggio dell'attività SMB
- Audit multiprotocollo NAS
- FPolicy
- Condivisioni continuamente disponibili, protocollo Witness e VSS remoto (utilizzato con configurazioni Hyper-V su SMB)

**Supporto del servizio di autenticazione e dei nomi**

IPv6 supporta le comunicazioni con i seguenti name service:

- Controller di dominio
- Server DNS
- Server LDAP
- Server KDC
- Server NIS

## Modalità di utilizzo di IPv6 da parte dei server CIFS per la connessione a server esterni

Per creare una configurazione che soddisfi i requisiti, è necessario conoscere il modo in cui i server CIFS utilizzano IPv6 quando si effettua la connessione a server esterni.

- Selezione dell'indirizzo di origine

  Se si tenta di connettersi a un server esterno, l'indirizzo di origine selezionato deve essere dello stesso tipo dell'indirizzo di destinazione. Ad esempio, se ci si connette a un indirizzo IPv6, la macchina virtuale di storage (SVM) che ospita il server CIFS deve disporre di una LIF dati o LIF di gestione che abbia un

indirizzo IPv6 da utilizzare come indirizzo di origine. Analogamente, se ci si connette a un indirizzo IPv4, la SVM deve disporre di una LIF dati o LIF di gestione che abbia un indirizzo IPv4 da utilizzare come indirizzo di origine.

- Per i server rilevati dinamicamente utilizzando il DNS, il rilevamento dei server viene eseguito come segue:
  - Se IPv6 è disattivato nel cluster, vengono rilevati solo gli indirizzi dei server IPv4.
  - Se IPv6 è attivato nel cluster, vengono rilevati gli indirizzi dei server IPv4 e IPv6. Entrambi i tipi possono essere utilizzati in base all'idoneità del server a cui appartiene l'indirizzo e alla disponibilità di dati IPv6 o IPv4 o LIF di gestione. Il rilevamento dinamico dei server viene utilizzato per rilevare i controller di dominio e i servizi associati, come LSA, NETLOGON, Kerberos e LDAP.
- Connettività del server DNS

  Se SVM utilizza IPv6 durante la connessione a un server DNS, dipende dalla configurazione dei servizi di nomi DNS. Se i servizi DNS sono configurati per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione DNS name Services può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server DNS continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione dei servizi dei nomi DNS.

- Connettività al server LDAP

  Se SVM utilizza IPv6 durante la connessione a un server LDAP, dipende dalla configurazione del client LDAP. Se il client LDAP è configurato per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione del client LDAP può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server LDAP continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione del client LDAP.

  > La configurazione del client LDAP viene utilizzata per la configurazione di LDAP per i servizi nome utente, gruppo e netgroup UNIX.

- Connettività del server NIS

  La possibilità che SVM utilizzi IPv6 durante la connessione a un server NIS dipende dalla configurazione dei servizi dei nomi NIS. Se i servizi NIS sono configurati per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione NIS name Services può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server NIS continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione dei servizi NIS.

  > I NIS name service vengono utilizzati per memorizzare e gestire gli oggetti utente, gruppo, netgroup e nome host UNIX.

**Informazioni correlate**

Abilitazione di IPv6 per SMB (solo amministratori di cluster)

Monitoraggio e visualizzazione delle informazioni sulle sessioni SMB IPv6

## Abilitare IPv6 per SMB (solo amministratori di cluster)

Le reti IPv6 non sono abilitate durante l'installazione del cluster. Per utilizzare IPv6 per SMB, un amministratore del cluster deve abilitare IPv6 al termine della configurazione del cluster. Quando l'amministratore del cluster attiva IPv6, viene attivato per l'intero cluster.

**Fase**

1. Attiva IPv6: `network options ipv6 modify -enabled true`

   Per ulteriori informazioni sull'attivazione di IPv6 nel cluster e sulla configurazione di LIF IPv6, consultare la *Guida alla gestione di rete*.

   IPv6 è attivato. È possibile configurare le LIF dei dati IPv6 per l'accesso SMB.

**Informazioni correlate**

Monitoraggio e visualizzazione delle informazioni sulle sessioni SMB IPv6

"Gestione della rete"

## Disattiva IPv6 per SMB

Anche se IPv6 è attivato sul cluster utilizzando un'opzione di rete, non è possibile disattivare IPv6 per SMB utilizzando lo stesso comando. Al contrario, ONTAP disattiva IPv6 quando l'amministratore del cluster disattiva l'ultima interfaccia abilitata per IPv6 sul cluster. È necessario comunicare con l'amministratore del cluster in merito alla gestione delle interfacce abilitate per IPv6.

Per ulteriori informazioni sulla disattivazione di IPv6 nel cluster, consultare la *Guida alla gestione di rete*.

**Informazioni correlate**

"Gestione della rete"

## Monitorare e visualizzare informazioni sulle sessioni SMB IPv6

È possibile monitorare e visualizzare le informazioni sulle sessioni SMB connesse tramite reti IPv6. Queste informazioni sono utili per determinare quali client si connettono utilizzando IPv6 e altre informazioni utili sulle sessioni SMB IPv6.

**Fase**

1. Eseguire l'azione desiderata:

| Se si desidera determinare se… | Immettere il comando… |
|---|---|
| Le sessioni SMB a una macchina virtuale di storage (SVM) sono connesse tramite IPv6 | `vserver cifs session show -vserver` *`vserver_name`* `-instance` |
| IPv6 viene utilizzato per le sessioni SMB attraverso un indirizzo LIF specificato | `vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance`<br><br>*`LIF_IP_address`* È l'indirizzo IPv6 del LIF dei dati. |