Gestire SMB con la CLI

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire SMB con la CLI

Panoramica di riferimento SMB

Le funzioni di accesso ai file ONTAP sono disponibili per il protocollo SMB. È possibile attivare un server CIFS, creare condivisioni e abilitare i servizi Microsoft.

> *SMB* (Server message Block) si riferisce ai dialetti moderni del protocollo CIFS (Common Internet file System). L'interfaccia della riga di comando (CLI) di ONTAP e i tool di gestione di OnCommand sono ancora visibili in *CIFS*.

Attenersi alle seguenti procedure nei seguenti casi:

- Vuoi comprendere la gamma di funzionalità del protocollo SMB di ONTAP.
- Si desidera eseguire attività di configurazione e manutenzione meno comuni, non la configurazione SMB di base.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Supporto per server SMB

Panoramica sul supporto dei server SMB

È possibile abilitare e configurare server SMB su macchine virtuali storage (SVM) per consentire ai client SMB di accedere ai file sul cluster.

- Ogni SVM di dati nel cluster può essere associata esattamente a un dominio Active Directory.
- Non è necessario che le SVM dei dati siano associate allo stesso dominio.
- È possibile associare più SVM allo stesso dominio.

Prima di creare un server SMB, è necessario configurare le SVM e le LIF utilizzate per la distribuzione dei dati. Se la rete dati non è piatta, potrebbe essere necessario configurare anche gli IPspaces, i domini di trasmissione e le subnet. La *Guida alla gestione della rete* contiene dettagli.

Informazioni correlate

"Gestione della rete"

Modificare i server SMB

"Amministrazione del sistema"

Versioni e funzionalità SMB supportate

SMB (Server message Block) è un protocollo di condivisione file remoto utilizzato dai client e dai server Microsoft Windows. In ONTAP 9, sono supportate tutte le versioni SMB; tuttavia, il supporto predefinito SMB 1.0 dipende dalla versione di ONTAP in uso. Verificare che il server SMB ONTAP supporti i client e le funzionalità richieste

nell'ambiente.

Le informazioni più recenti sui client SMB e sui controller di dominio supportati da ONTAP sono disponibili nello strumento *matrice di interoperabilità*.

SMB 2.0 e le versioni successive sono attivate per impostazione predefinita per i server SMB ONTAP 9 e possono essere attivate o disattivate in base alle necessità. La seguente tabella mostra il supporto SMB 1.0 e la configurazione predefinita.

Funzionalità SMB 1.0:	**In queste versioni di ONTAP 9:**			
	9.0	9.1	9.2	9.3 e versioni successive
È attivato per impostazione predefinita	Sì	Sì	Sì	No
Può essere attivato o disattivato	No	Sì*9.1 P8 o versione successiva richiesta.	Sì	Sì

> Le impostazioni predefinite per le connessioni SMB 1.0 e 2.0 ai domain controller dipendono anche dalla versione di ONTAP. Ulteriori informazioni sono disponibili nella `vserver cifs security modify` pagina man. Per gli ambienti con server CIFS esistenti che eseguono SMB 1.0, è necessario eseguire la migrazione 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.

La seguente tabella mostra le funzionalità SMB supportate in ciascuna versione SMB. Alcune funzionalità SMB sono attivate per impostazione predefinita e alcune richiedono una configurazione aggiuntiva.

Questa funzionalità:	**Richiede l'abilitazione:**	**È supportato in ONTAP 9 per le seguenti versioni SMB:**				
		1.0	2.0	2.1	3.0	3.1.1
Funzionalità SMB 1.0 legacy		X	X	X	X	X
Manici durevoli			X	X	X	X
Operazioni composte			X	X	X	X
Operazioni asincrone			X	X	X	X

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
Maggiori dimensioni dei buffer di lettura e scrittura			X	X	X	X
Maggiore scalabilità			X	X	X	X
Firma SMB	X	X	X	X	X	X
Formato di file ADS (alternate Data Stream)	X	X	X	X	X	X
MTU grande (attivata per impostazione predefinita a partire da ONTAP 9.7)	X			X	X	X
Oplock del lease				X	X	X
Condivisioni a disponibilità continua	X				X	X
Handle persistenti					X	X
Testimone					X	X
CRITTOGRAFIA SMB: AES-128-CCM	X				X	X
Scale-out (richiesto dalle condivisioni CA)					X	X

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
Failover trasparente					X	X
SMB multicanale (a partire da ONTAP 9.4)	X				X	X
Integrità della preautenticazione						X
Failover del client cluster v.2 (CCFv2)						X
Crittografia SMB: AES-128-GCM (a partire da ONTAP 9.1)	X					X

Informazioni correlate

Utilizzo della firma SMB per migliorare la sicurezza della rete

Impostazione del livello minimo di sicurezza per l'autenticazione del server SMB

Configurazione della crittografia SMB richiesta sui server SMB per il trasferimento dei dati su SMB

"Report tecnico di NetApp 4543: Best practice per il protocollo SMB"

"Interoperabilità NetApp"

Funzionalità di Windows non supportate

Prima di utilizzare CIFS nella rete, è necessario conoscere alcune funzionalità di Windows non supportate da ONTAP.

ONTAP non supporta le seguenti funzionalità di Windows:

- File system crittografato (EFS)
- Registrazione degli eventi NTFS (NT file System) nel diario delle modifiche
- Servizio di replica file Microsoft (FRS)
- Servizio di indicizzazione Microsoft Windows
- Storage remoto tramite HSM (Hierarchical Storage Management)
- Gestione delle quote dai client Windows

- Semantica delle quote di Windows
- Il file LMHOSTS
- Compressione nativa NTFS

Configurare i servizi NIS o LDAP sulla SVM

Con l'accesso SMB, il mapping degli utenti a un utente UNIX viene sempre eseguito, anche quando si accede ai dati in un volume di sicurezza NTFS. Se si mappano gli utenti Windows agli utenti UNIX corrispondenti le cui informazioni sono memorizzate negli archivi di directory NIS o LDAP o se si utilizza LDAP per la mappatura dei nomi, è necessario configurare questi servizi durante l'installazione di SMB.

Prima di iniziare

È necessario personalizzare la configurazione del database dei name service in modo che corrisponda all'infrastruttura del name service.

A proposito di questa attività

Le SVM utilizzano i database dei name service ns-switch per determinare l'ordine in cui cercare le origini di un dato database dei name service. L'origine ns-switch può essere una combinazione qualsiasi di "Files", "nis" o "ldap". Per il database dei gruppi, ONTAP tenta di ottenere le appartenenze ai gruppi da tutte le origini configurate e utilizza le informazioni consolidate sull'appartenenza ai gruppi per i controlli degli accessi. Se una di queste origini non è disponibile al momento dell'ottenimento delle informazioni sul gruppo UNIX, ONTAP non può ottenere le credenziali UNIX complete e i controlli di accesso successivi potrebbero non riuscire. Pertanto, è necessario controllare sempre che tutte le sorgenti ns-switch siano configurate per il database di gruppo nelle impostazioni ns-switch.

L'impostazione predefinita prevede che il server SMB mappi tutti gli utenti Windows all'utente UNIX predefinito memorizzato in locale `passwd` database. Se si desidera utilizzare la configurazione predefinita, la configurazione dei servizi NIS o LDAP UNIX nome utente e gruppo o la mappatura utente LDAP è facoltativa per l'accesso SMB.

Fasi

1. Se le informazioni relative a utenti, gruppi e netgroup UNIX sono gestite da NIS name service, configurare NIS name service:

   a. Determinare l'ordine corrente dei servizi di gestione dei nomi utilizzando `vserver services name-service ns-switch show` comando.

      In questo esempio, i tre database (`group`, `passwd`, e. `netgroup`) che possono utilizzare `nis` come nome, l'origine del servizio utilizza solo `files` come fonte.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

```
                                                    Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            files
vs1             passwd         true            files
vs1             netgroup       true            files
vs1             namemap        true            files
```

È necessario aggiungere `nis` origine di `group` e. `passwd` e, facoltativamente, in `netgroup` database.

b. Regolare l'ordinamento del database dei name service ns-switch come desiderato utilizzando `vserver services name-service ns-switch modify` comando.

   Per ottenere prestazioni ottimali, non aggiungere un name service a un database di name service a meno che non si preveda di configurare tale name service su SVM.

   Se si modifica la configurazione per più database di name service, è necessario eseguire il comando separatamente per ogni database di name service che si desidera modificare.

   In questo esempio, `nis` e. `files` sono configurati come origini per `group` e. `passwd` database, in questo ordine. Il resto dei database dei servizi di nome non viene modificato.

   `vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis,files` `vserver services name-service ns-switch modify -vserver vs1 -database passwd -sources nis,files`

c. Verificare che l'ordine dei name service sia corretto utilizzando `vserver services name-service ns-switch show` comando.

   `vserver services name-service ns-switch show -vserver vs1`

```
                                                    Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            nis,
                                                files
vs1             passwd         true            nis,
                                                files
vs1             netgroup       true            files
vs1             namemap        true            files
```

d. Creare la configurazione NIS name service:
   `vserver services name-service nis-domain create -vserver` *`vserver_name`*

```
-domain NIS_domain_name -servers NIS_server_IPaddress,… -active true+

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```

> A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

e. Verificare che il NIS name service sia configurato correttamente e sia attivo: `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   10.0.0.60
```

2. Se le informazioni relative a utenti, gruppi e netgroup UNIX o la mappatura dei nomi sono gestite dai servizi dei nomi LDAP, configurare i servizi dei nomi LDAP utilizzando le informazioni disponibili "Gestione NFS".

Funzionamento della configurazione dello switch ONTAP name service

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX. È necessario comprendere la funzione della tabella e il modo in cui ONTAP la utilizza in modo da poterla configurare in modo appropriato per l'ambiente in uso.

La tabella ONTAP name service switch determina le origini del servizio di nomi che ONTAP consulta per recuperare le informazioni relative a un determinato tipo di informazioni sul servizio di nomi. ONTAP gestisce una tabella di switch del name service separata per ogni SVM.

Tipi di database

La tabella memorizza un elenco di name service separato per ciascuno dei seguenti tipi di database:

Tipo di database	Definisce le origini del servizio nome per…	Le origini valide sono…
host	Conversione dei nomi host in indirizzi IP	file, dns
gruppo	Ricerca di informazioni sul gruppo di utenti	file, nis, ldap
password	Ricerca delle informazioni dell'utente	file, nis, ldap

Tipo di database	Definisce le origini del servizio nome per…	Le origini valide sono…
netgroup	Ricerca di informazioni sul netgroup	file, nis, ldap
mappa dei nomi	Mappatura dei nomi utente	file, ldap

Tipi di origine

Le origini specificano quale nome di origine del servizio utilizzare per recuperare le informazioni appropriate.

Specifica tipo di origine…	Per cercare informazioni in…	Gestito dalle famiglie di comandi…

file	File di origine locali	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	`vserver services name-service nis-domain`
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	`vserver services name-service ldap`
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	`vserver services name-service dns`

Anche se si prevede di utilizzare NIS o LDAP per l'accesso ai dati e l'autenticazione dell'amministrazione SVM, è comunque necessario includere `files` E configurare gli utenti locali come fallback nel caso in cui l'autenticazione NIS o LDAP non riesca.

Protocolli utilizzati per accedere a fonti esterne

Per accedere ai server per le origini esterne, ONTAP utilizza i seguenti protocolli:

Origine esterna del name service	Protocollo utilizzato per l'accesso
NIS	UDP
DNS	UDP

Origine esterna del name service	Protocollo utilizzato per l'accesso
LDAP	TCP

Esempio

Nell'esempio seguente viene visualizzata la configurazione dello switch name service per SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Per cercare informazioni su utenti o gruppi, ONTAP consulta solo i file di origine locali. Se la query non restituisce alcun risultato, la ricerca non riesce.

Per cercare informazioni sui netgroup, ONTAP consulta prima i server NIS esterni. Se la query non restituisce alcun risultato, viene selezionato il file netgroup locale.

Non sono presenti voci di name service per la mappatura dei nomi nella tabella per SVM svm_1. Pertanto, ONTAP consulta solo i file di origine locali per impostazione predefinita.

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` b. `vserver cifs options modify -vserver` *`vserver_name options`* 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.

Valore	Descrizione
`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`*

Se si desidera visualizzare informazioni su…	Immettere il comando…
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

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`* 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` 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`* 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`* 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.
`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.
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.

Crittografia SMB server abilitata	Share encoded data Setting Enabled (Condividi dati crittografati	Comportamento della crittografia lato server
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`
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
`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

Nome del contatore	Descrizioni
`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

Se si desidera visualizzare informazioni per…	Inserisci…
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,...]` 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,...]` 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` È possibile specificare ulteriori proprietà di condivisione da aggiungere utilizzando un elenco delimitato da virgole. 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` È possibile specificare ulteriori proprietà di condivisione da rimuovere utilizzando un elenco delimitato da virgole. 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`*
Tutte le impostazioni dell'oggetto Criteri di gruppo	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informazioni correlate

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

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

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

Visualizzazione di informazioni sui criteri di accesso centrale

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`

Se si desidera…	Utilizzare questo comando…
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` *`LIF_IP_address`* È l'indirizzo IPv6 del LIF dei dati.

Impostare l'accesso ai file utilizzando SMB

Configurare gli stili di sicurezza

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

Quali sono gli stili di sicurezza e i loro effetti

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

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

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

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

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

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

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

l'autorizzazione di condivisione effettiva.

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

Dove e quando impostare gli stili di sicurezza

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

Decidere quale stile di sicurezza utilizzare sulle SVM

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

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

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

Come funziona l'ereditarietà dello stile di sicurezza

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

Gli stili di sicurezza vengono ereditati nel modo seguente:

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

In che modo ONTAP conserva le autorizzazioni UNIX

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

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

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

Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

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

- Modifica delle autorizzazioni UNIX

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

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

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

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

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

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

Configurare gli stili di sicurezza sui volumi root SVM

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

Fasi

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

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

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

Configurare gli stili di sicurezza sui volumi FlexVol

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

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

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

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

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

Configurare gli stili di sicurezza sui qtree

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

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

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

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

Creare e gestire volumi di dati in spazi dei nomi NAS

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

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

Creare volumi di dati con punti di giunzione specificati

È possibile specificare il punto di giunzione quando si crea un volume di dati. Il volume risultante viene montato automaticamente nel punto di giunzione ed è immediatamente disponibile per la configurazione dell'accesso NAS.

Prima di iniziare

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

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

Fasi

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

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

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

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

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

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

Esempio

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

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

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

Creare volumi di dati senza specificare punti di giunzione

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

condivisioni SMB o le esportazioni NFS per quel volume.

Prima di iniziare

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

Fasi

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

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

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

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

Esempio

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

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

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

Montare o smontare i volumi esistenti nello spazio dei nomi NAS

È necessario montare un volume sullo spazio dei nomi NAS prima di poter configurare l'accesso del client NAS ai dati contenuti nei volumi SVM (Storage Virtual Machine). È possibile montare un volume su un punto di giunzione se non è attualmente montato. È anche possibile smontare i volumi.

A proposito di questa attività

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

NAS.

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

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

Fasi

1. Eseguire l'azione desiderata:

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

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

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

Esempi

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

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

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

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

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

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

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

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

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

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

Fasi

1. Eseguire l'azione desiderata:

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

Esempi

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

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

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

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

Configurare le mappature dei nomi

Panoramica sulla configurazione delle mappature dei nomi

ONTAP utilizza la mappatura dei nomi per mappare le identità CIFS alle identità UNIX, le identità Kerberos alle identità UNIX e le identità UNIX alle identità CIFS. Queste informazioni sono necessarie per ottenere le credenziali dell'utente e fornire l'accesso corretto ai file, indipendentemente dal fatto che si stia connettendo da un client NFS o

CIFS.

Esistono due eccezioni per le quali non è necessario utilizzare la mappatura dei nomi:

- Si configura un ambiente UNIX puro e non si prevede di utilizzare l'accesso CIFS o lo stile di sicurezza NTFS sui volumi.
- Viene configurato l'utente predefinito da utilizzare.

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

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

Tuttavia, è possibile mappare un gruppo di singoli utenti a un utente specifico. Ad esempio, è possibile mappare tutti gli utenti ad che iniziano o terminano con la parola SALES a un utente UNIX specifico e all'UID dell'utente.

Come funziona la mappatura dei nomi

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

- Per la mappatura da Windows a UNIX

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

- Per la mappatura da UNIX a Windows

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

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

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

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

Multidominio ricerca le mappature dei nomi utente da UNIX a Windows

ONTAP supporta le ricerche su più domini durante la mappatura degli utenti UNIX agli

utenti Windows. In tutti i domini attendibili rilevati vengono ricercate le corrispondenze del modello di sostituzione fino a quando non viene restituito un risultato corrispondente. In alternativa, è possibile configurare un elenco di domini attendibili preferiti, che viene utilizzato al posto dell'elenco di domini attendibili rilevati e che viene ricercato in ordine fino a quando non viene restituito un risultato corrispondente.

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

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

- *Fiducia bidirezionale*

  Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server CIFS ha un trust bidirezionale con un altro dominio, il dominio principale può autenticare e autorizzare un utente appartenente al dominio attendibile e viceversa.

  Le ricerche di associazione dei nomi utente da UNIX a Windows possono essere eseguite solo su domini con trust bidirezionali tra il dominio principale e l'altro dominio.

- *Fiducia in uscita*

  Con un trust in uscita, il dominio principale considera attendibile l'altro dominio. In questo caso, il dominio principale può autenticare e autorizzare un utente appartenente al dominio trusted in uscita.

  Un dominio con un trust in uscita con il dominio principale viene *not* ricercato quando si eseguono ricerche di mappatura da utente UNIX a nome utente Windows.

- *Fiducia in entrata*

  Con un trust inbound, l'altro dominio considera attendibile il dominio principale del server CIFS. In questo caso, il dominio principale non può autenticare o autorizzare un utente appartenente al dominio trusted in entrata.

  Un dominio con un trust in entrata con il dominio principale viene *not* ricercato quando si eseguono ricerche di associazione tra utenti UNIX e nomi utente Windows.

Modalità di utilizzo dei caratteri jolly (*) per configurare le ricerche su più domini per la mappatura dei nomi

Le ricerche di mappatura dei nomi multidominio sono facilitate dall'utilizzo di caratteri jolly nella sezione dominio del nome utente di Windows. Nella tabella seguente viene illustrato come utilizzare i caratteri jolly nella parte di dominio di una voce di mappatura dei nomi per abilitare le ricerche su più domini:

Schema	Sostituzione	Risultato
root	amministratore	L'utente UNIX "root" viene mappato all'utente "Administrator". Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente "Administrator".
*	*	Gli utenti UNIX validi vengono mappati ai corrispondenti utenti Windows. Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente a tale nome. Il modello è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.

Come vengono eseguite le ricerche di nomi multidominio

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

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

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

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

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

Regole di conversione del mapping dei nomi

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

come in UNIX `sed` programma.

Creare una mappatura dei nomi

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

A proposito di questa attività

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

Fase

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

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

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

Esempi

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

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

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

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

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

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

Configurare l'utente predefinito

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

A proposito di questa attività

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

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

Comandi per la gestione delle mappature dei nomi

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

Se si desidera…	Utilizzare questo comando…
Creare una mappatura dei nomi	`vserver name-mapping create`
Inserire una mappatura dei nomi in una posizione specifica	`vserver name-mapping insert`
Visualizza mappature dei nomi	`vserver name-mapping show`

Se si desidera…	Utilizzare questo comando…
Scambiare la posizione di due mappature dei nomi Lo swap non è consentito quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	`vserver name-mapping swap`
Modificare una mappatura dei nomi	`vserver name-mapping modify`
Eliminare una mappatura dei nomi	`vserver name-mapping delete`
Convalidare la corretta mappatura dei nomi	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Configurare le ricerche di mappatura dei nomi di più domini

Attivare o disattivare le ricerche di mappatura dei nomi multidominio

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

A proposito di questa attività

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

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

Fasi

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

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

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

Informazioni correlate

Opzioni server SMB disponibili

Reimpostare e riscoprire i domini attendibili

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

Fase

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

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

Informazioni correlate

Visualizzazione delle informazioni sui domini attendibili rilevati

Visualizza informazioni sui domini attendibili rilevati

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

A proposito di questa attività

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

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

Fase

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

   `vserver cifs domain trusts show -vserver vs1`

```
   Node: node1
Vserver: vs1

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

   Node: node2
Vserver: vs1

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

Informazioni correlate

Reimpostazione e riscoperta di domini attendibili

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

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

A proposito di questa attività

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

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

Fase

1. Eseguire una delle seguenti operazioni:

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

Esempi

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

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

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

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

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

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

Informazioni correlate

Visualizzazione delle informazioni sull'elenco di domini attendibili preferiti

Visualizzare le informazioni relative all'elenco di domini attendibili preferiti

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

preferito in alternativa all'elenco di domini attendibili rilevati automaticamente.

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

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

Informazioni correlate

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

Creare e configurare le condivisioni SMB

Panoramica sulla creazione e la configurazione delle condivisioni SMB

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

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

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

Informazioni correlate

Gestire l'accesso ai file utilizzando SMB

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

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

Quali sono le condivisioni amministrative predefinite

Quando si crea un server CIFS sulla macchina virtuale di storage (SVM), vengono create automaticamente le condivisioni amministrative predefinite. È necessario comprendere quali sono le condivisioni predefinite e come vengono utilizzate.

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

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

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

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

Come vengono utilizzate le condivisioni predefinite ipc e admin

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

- condivisione ipc

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

- Quota amministrativa (solo ONTAP 9.7 e versioni precedenti)

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

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

Modalità di utilizzo della condivisione predefinita

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

Di seguito sono riportate le caratteristiche della quota:

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

Questo utente è il BUILTIN/amministratore. Per impostazione predefinita, il BUILTIN/amministratore può eseguire il mapping alla condivisione e visualizzare, creare, modificare o eliminare file e cartelle nella directory principale mappata. Prestare attenzione durante la gestione di file e cartelle in questa directory.

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

Informazioni correlate

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

Requisiti di naming delle condivisioni SMB

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

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

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

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

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

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

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

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

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

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

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

```
dir

 Directory of Z:\

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

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

Utilizzare le proprietà di condivisione SMB

Utilizza la panoramica delle proprietà di condivisione SMB

È possibile personalizzare le proprietà delle condivisioni SMB.

Le proprietà di condivisione disponibili sono le seguenti:

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

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

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

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

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

Prima di iniziare

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

A proposito di questa attività

Linee guida per l'aggiunta di proprietà di condivisione:

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

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

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

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

Linee guida per la rimozione delle proprietà di condivisione:

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

Fasi

1. Immettere il comando appropriato:

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

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

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

Esempi

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

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

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

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

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

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

Informazioni correlate

Comandi per la gestione delle condivisioni SMB

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

Quando si crea una condivisione dalla riga di comando di ONTAP ai dati con protezione

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

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

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

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

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

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

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

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

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

Informazioni correlate

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

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

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

Fase

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

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

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

Esempio

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

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

Informazioni correlate

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

Visualizzare le informazioni sulle condivisioni SMB utilizzando MMC

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

A proposito di questa attività

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

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

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

Le seguenti funzioni non sono supportate in MMC per ONTAP:

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

Nei casi in cui l’operazione non è supportata, potrebbe verificarsi un’operazione `remote procedure call`

`failed` errori.

"Domande frequenti: Utilizzo di Windows MMC con ONTAP"

Fasi

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

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

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

   MMC si connette a SVM.

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

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

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

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

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

Comandi per la gestione delle condivisioni SMB

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

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

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

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

Accesso sicuro ai file utilizzando gli ACL di condivisione SMB

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

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

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

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

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

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

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

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

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

- È possibile specificare solo le autorizzazioni di Windows.

Creare elenchi di controllo degli accessi di condivisione SMB

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

A proposito di questa attività

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

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

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

Fasi

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

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

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

Esempio

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

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

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

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

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

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

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

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

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

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

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

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

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

Proteggere l'accesso ai file utilizzando i permessi

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

È possibile configurare le autorizzazioni standard per i file NTFS su file e cartelle utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows.

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

   a. Selezionare una lettera **Drive**.

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

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

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

   c. Fare clic su **fine**.

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

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

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

6. Fare clic su **Avanzate**.

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

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

   Viene visualizzata la finestra Permissions (autorizzazioni).

8. Eseguire le azioni desiderate:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Informazioni correlate

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

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

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

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

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

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

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

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

Fasi

1. Creare un descrittore di protezione NTFS.

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

2. Aggiungere DACL al descrittore di protezione NTFS.

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

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

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

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

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

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

- Permessi di esportazione

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

- Autorizzazioni di condivisione
- Permessi del file

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

  - NTFS
  - ACL NFSv4 UNIX
  - Bit di modalità UNIX

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

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

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

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

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

Aggiunte alle credenziali CIFS

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

- Identità del dispositivo

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

- Dichiarazioni dei dispositivi

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

- Richieste dell'utente

  Asserzioni su un'identità di sicurezza dell'utente. Ad esempio, un utente può affermare che il proprio account ad è membro di una specifica unità organizzativa.

Policy di accesso centrale

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

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

Staging dei criteri di accesso centralizzato con auditing avanzato

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

Informazioni correlate

GPO supportati

Applicazione di oggetti Criteri di gruppo ai server CIFS

Attivazione o disattivazione del supporto GPO su un server CIFS

Visualizzazione delle informazioni sulle configurazioni dell’oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

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

Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi

"Controllo SMB e NFS e tracciamento della sicurezza"

Funzionalità Dynamic Access Control supportata

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

Supportato per Dynamic Access Control

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

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

Non supportato per Dynamic Access Control

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

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

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

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

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

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

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

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

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

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

Attiva o disattiva la panoramica del controllo dinamico degli accessi

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

A proposito di questa attività

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

Questa opzione è disponibile solo al livello di privilegio avanzato.

Fase

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

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

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

Informazioni correlate

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

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

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

A proposito di questa attività

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

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

Fasi

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

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

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

Prima di iniziare

- Active Directory deve essere configurato per utilizzare criteri di accesso centrali.

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

A proposito di questa attività

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

"Microsoft TechNet Library"

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

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

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Attivazione o disattivazione del controllo dinamico degli accessi

Visualizza informazioni sulla sicurezza del controllo dinamico degli accessi

È possibile visualizzare informazioni sulla sicurezza del controllo dinamico degli accessi (DAC) sui volumi NTFS e sui dati con protezione effettiva NTFS su volumi misti di tipo sicurezza. Ciò include informazioni su ACE condizionali, ACE di risorse e ACE di policy di accesso centrale. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

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

Fase

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

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

Esempi

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

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

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

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

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Considerazioni sul revert per il controllo dinamico degli accessi

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

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

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

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

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

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

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

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

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

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

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

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

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

"Microsoft TechNet: Scenario dei criteri di accesso centrale"

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

- **Utilizzo di GPO sul server SMB**

  Applicazione di oggetti Criteri di gruppo ai server SMB

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

  "Controllo SMB e NFS e tracciamento della sicurezza"

Accesso sicuro alle PMI tramite policy di esportazione

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

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

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

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

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

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

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

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

Se i criteri di esportazione per SMB sono attivati e un client effettua una richiesta di accesso non consentita dalla policy di esportazione applicabile, la richiesta non riesce e viene visualizzato un messaggio di autorizzazione negata. Se un client non corrisponde a nessuna regola nella policy di esportazione del volume, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati. Ciò è vero anche se le autorizzazioni di condivisione e file consentirebbero altrimenti l'accesso. Ciò significa che è necessario configurare la policy di esportazione in modo da consentire in modo minimo quanto segue sui volumi contenenti condivisioni SMB:

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

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

Scopri di più "configurazione e gestione delle policy di esportazione".

Come funzionano le regole di esportazione

Le regole di esportazione sono gli elementi funzionali di una policy di esportazione. Le regole di esportazione consentono di associare le richieste di accesso client a un volume a parametri specifici configurati per determinare come gestire le richieste di accesso client.

Un criterio di esportazione deve contenere almeno una regola di esportazione per consentire l'accesso ai client. Se un criterio di esportazione contiene più di una regola, le regole vengono elaborate nell'ordine in cui appaiono nel criterio di esportazione. L'ordine delle regole è determinato dal numero di indice delle regole. Se una regola corrisponde a un client, vengono utilizzate le autorizzazioni di tale regola e non vengono elaborate ulteriori regole. Se nessuna regola corrisponde, al client viene negato l'accesso.

È possibile configurare le regole di esportazione per determinare le autorizzazioni di accesso del client utilizzando i seguenti criteri:

- Il protocollo di accesso al file utilizzato dal client che invia la richiesta, ad esempio NFSv4 o SMB.
- Identificatore del client, ad esempio nome host o indirizzo IP.

  La dimensione massima di `-clientmatch` il campo è composto da 4096 caratteri.

- Il tipo di protezione utilizzato dal client per autenticare, ad esempio Kerberos v5, NTLM o AUTH_SYS.

Se una regola specifica più criteri, il client deve corrispondere a tutti i criteri affinché la regola venga applicata.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv3 e il client ha l'indirizzo IP 10.1.17.37.

Anche se il protocollo di accesso client corrisponde, l'indirizzo IP del client si trova in una subnet diversa da quella specificata nella regola di esportazione. Pertanto, la corrispondenza dei client non riesce e questa regola non si applica a questo client.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv4 e il client ha l'indirizzo IP 10.1.16.54.

Il protocollo di accesso client corrisponde e l'indirizzo IP del client si trova nella subnet specificata. Pertanto, la corrispondenza dei client viene eseguita correttamente e questa regola si applica a questo client. Il client ottiene l'accesso in lettura/scrittura indipendentemente dal tipo di protezione.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Pertanto, entrambi i client ottengono l'accesso in sola lettura. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

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

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

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

Regola di esportazione solo per l'accesso SMB

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

- Nome policy: Cifs1
- Numero indice: 1
- Client match (corrispondenza client): Corrisponde solo ai client sulla rete 192.168.1.0/24
- Protocol (protocollo): Consente solo l'accesso SMB
- Accesso di sola lettura: Ai client che utilizzano l'autenticazione NTLM o Kerberos

- Accesso in lettura/scrittura: Ai client che utilizzano l'autenticazione Kerberos

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

Regola di esportazione per accesso SMB e NFS

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

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

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

Regola di esportazione per l'accesso SMB utilizzando solo NTLM

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

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

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

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

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

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

Prima di iniziare

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

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

A proposito di questa attività

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

Fasi

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

Esempio

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

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

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

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

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

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

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

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

Comportamento di Access Guard a livello di storage

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

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

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

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

  - Sicurezza del file

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

  - Sicurezza della directory

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

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

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

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

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

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

  È progettato per essere modificato solo dagli amministratori dello storage.

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

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

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

Ordine dei controlli di accesso

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

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

Casi di utilizzo di Storage-Level Access Guard

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

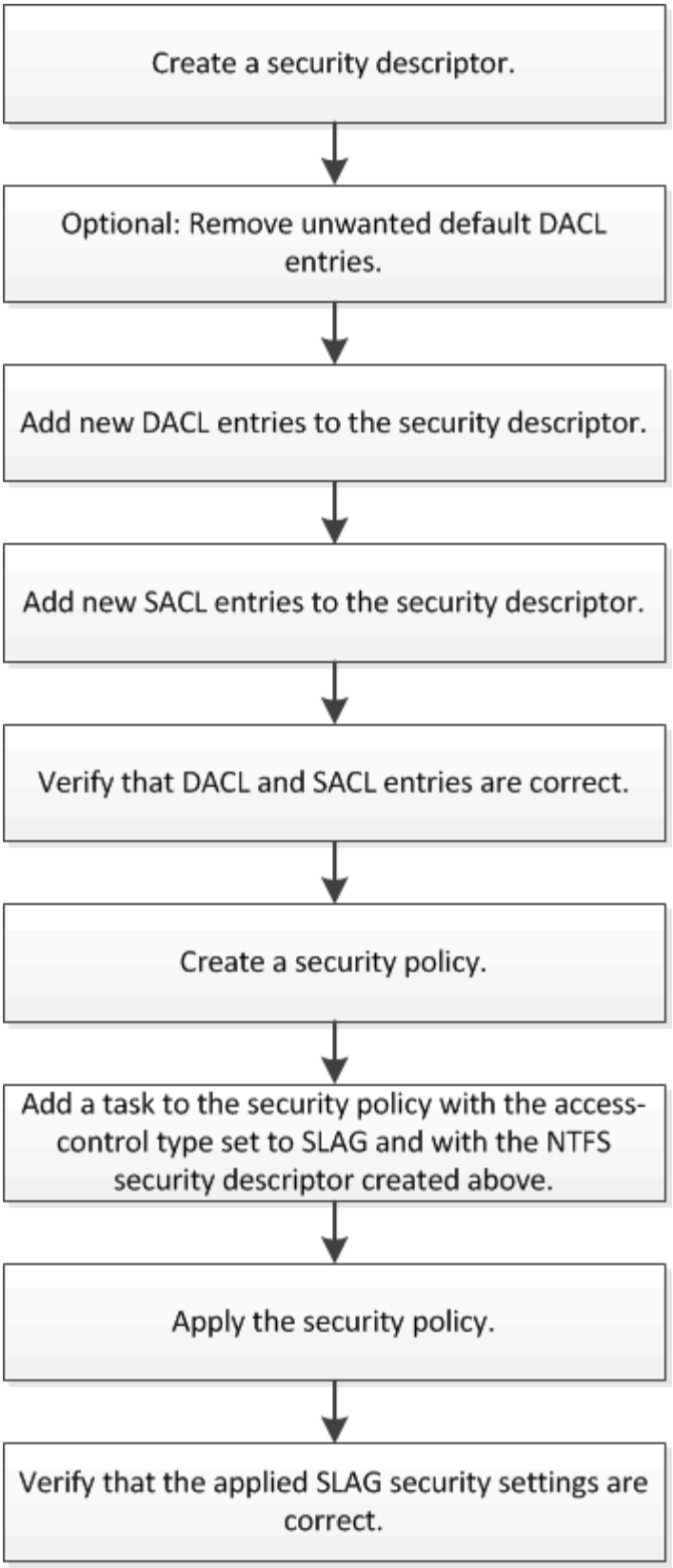
I casi di utilizzo tipici di questa funzionalità includono i seguenti scenari:

- Protezione della proprietà intellettuale attraverso il controllo e il controllo dell'accesso di tutti gli utenti` a livello di storage
- Storage per le società di servizi finanziari, inclusi gruppi bancari e commerciali

- Servizi governativi con storage di file separato per singoli reparti
- Le università proteggono tutti i file degli studenti

Workflow per configurare Storage-Level Access Guard

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



Informazioni correlate

Configurazione di Storage-Level Access Guard

Configurare Storage-Level Access Guard

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

Fasi

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

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

   ```
   Vserver: vs1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
 Vserver: vs1
  Policy: policy1

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

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

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

    Il processo di applicazione della policy di sicurezza è pianificato.

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

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

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

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


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

Informazioni correlate

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

Workflow per configurare Storage-Level Access Guard

Visualizzazione di informazioni su Storage-Level Access Guard

Rimozione di Storage-Level Access Guard

Matrice DI SCORIE efficace

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

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

Visualizza informazioni su Storage-Level Access Guard

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

A proposito di questa attività

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

Fase

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

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

Esempi

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

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

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


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

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

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

Rimuovere Storage-Level Access Guard

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

Fasi

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

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

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

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

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

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

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

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

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

Gestire l’accesso ai file utilizzando SMB

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

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

Concetti relativi a utenti e gruppi locali

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

- **Utente locale**

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

  Gli account utente possono essere utilizzati in diversi modi:

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

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

I gruppi hanno diversi utilizzi:

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

- **Dominio locale**

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

- **Identificatore di sicurezza (SID)**

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

- **Autenticazione NTLM**

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

- **Cluster Replicated Database (RDB)**

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

Motivi per la creazione di utenti locali e gruppi locali

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

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

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

  Nelle configurazioni dei gruppi di lavoro sono richiesti utenti locali.

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

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

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

  User Rights Management è la capacità di un amministratore del server SMB di controllare i diritti degli

utenti e dei gruppi sulla SVM. È possibile assegnare i privilegi a un utente assegnando i privilegi all'account dell'utente o facendo in modo che l'utente sia membro di un gruppo locale che dispone di tali privilegi.

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

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

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

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

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

Informazioni correlate

Come funziona l'autenticazione utente locale

Elenco dei privilegi supportati

Come funziona l'autenticazione utente locale

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

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

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

- La parte di dominio corrisponde

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

- La porzione di dominio non corrisponde

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

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

- La porzione di dominio non è specificata

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

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

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

Informazioni correlate

Attivazione o disattivazione dell'autenticazione utente locale

Come vengono costruiti i token di accesso degli utenti

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

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

- Accesso utente locale

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

- Login utente di dominio

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

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

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

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

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

È necessario conoscere le linee guida per la configurazione di SnapMirror su volumi di

proprietà di SVM che contengono gruppi locali.

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

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

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

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

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

Come utilizzare Microsoft Management Console con utenti e gruppi locali

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

Linee guida per il ripristino

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

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

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

Quali sono i privilegi locali

Elenco dei privilegi supportati

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

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

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

Informazioni correlate

- Assegnare privilegi locali
- Configurazione del controllo incrociato bypass

Assegnare privilegi

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

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

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

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

Informazioni correlate

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

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

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

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

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

- Nessun account Guest locale.

Informazioni correlate

Gruppi BUILTIN predefiniti e privilegi predefiniti

Requisiti per le password dell'utente locale

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

La password deve soddisfare i seguenti criteri:

- Deve essere composto da almeno sei caratteri
- Non deve contenere il nome dell'account utente
- Deve contenere almeno tre caratteri delle seguenti quattro categorie:
  - Caratteri maiuscoli inglesi (Dalla A alla Z)

- Caratteri minuscoli inglesi (da a a z)
- Base 10 cifre (da 0 a 9)
- Caratteri speciali:

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

Informazioni correlate

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

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Modifica delle password degli account utente locali

Gruppi BUILTIN predefiniti e privilegi predefiniti

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

La seguente tabella descrive i gruppi predefiniti:

Gruppo BUILTIN predefinito	Privilegi predefiniti
`BUILTIN\Administrators`RID 544 Quando viene creato per la prima volta, il locale `Administrator` L'account, con un RID di 500, viene automaticamente reso membro di questo gruppo. Quando la macchina virtuale di storage (SVM) viene unita a un dominio, il `domain\Domain Admins` il gruppo viene aggiunto al gruppo. Se SVM lascia il dominio, il `domain\Domain Admins` il gruppo viene rimosso dal gruppo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo hanno le seguenti caratteristiche: • Può creare e gestire utenti e gruppi locali. • Impossibile aggiungere se stessi o altri oggetti a `BUILTIN\Administrators` gruppo.	`SeChangeNotifyPrivilege`

Gruppo BUILTIN predefinito	Privilegi predefiniti
`BUILTIN\Backup Operators`RID 551 Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo possono sovrascrivere i permessi di lettura e scrittura su file o cartelle se vengono aperti con finalità di backup.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Quando creato per la prima volta, questo gruppo non ha membri (oltre a quelli impliciti `Authenticated Users` gruppo speciale). Quando la SVM viene unita a un dominio, la `domain\Domain Users` il gruppo viene aggiunto a questo gruppo. Se SVM lascia il dominio, il `domain\Domain Users` il gruppo viene rimosso da questo gruppo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Questo gruppo include tutti gli utenti, inclusi gli utenti guest (ma non gli utenti anonimi). Si tratta di un gruppo implicito con un'appartenenza implicita.	`SeChangeNotifyPrivilege`

Informazioni correlate

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

Elenco dei privilegi supportati

Configurazione del controllo incrociato bypass

Attiva o disattiva la funzionalità di utenti e gruppi locali

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

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

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

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

Informazioni correlate

Modificare gli account utente locali

Modificare i gruppi locali

Aggiungere privilegi a utenti o gruppi locali o di dominio

Attivare o disattivare utenti e gruppi locali

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

A proposito di questa attività

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

Fasi

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

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

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

Esempio

L'esempio seguente abilita le funzionalità di utenti e gruppi locali su SVM vs1:

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

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

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

Informazioni correlate

Attiva o disattiva l'autenticazione utente locale

Attivare o disattivare gli account utente locali

Attiva o disattiva l'autenticazione utente locale

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

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

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

Esempio

L'esempio seguente abilita l'autenticazione dell'utente locale su SVM vs1:

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

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

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

Informazioni correlate

Come funziona l'autenticazione utente locale

Attivazione o disattivazione di utenti e gruppi locali

Gestire gli account utente locali

Modificare gli account utente locali

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

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

Esempio

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

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

Attivare o disattivare gli account utente locali

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

A proposito di questa attività

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

Fase

1. Eseguire l'azione appropriata:

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

Modificare le password dell'account utente locale

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

Fase

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

Esempio

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

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

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

Informazioni correlate

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

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Visualizza le informazioni sugli utenti locali

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

A proposito di questa attività

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

Fase

1. Eseguire una delle seguenti operazioni:

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

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

Esempio

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

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

Visualizza le informazioni sulle appartenenze ai gruppi per gli utenti locali

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

A proposito di questa attività

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

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Visualizza le informazioni di appartenenza dell'utente locale per un utente locale specificato	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Visualizza le informazioni di appartenenza dell'utente locale per il gruppo locale di cui l'utente locale è membro	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Visualizzazione delle informazioni di appartenenza degli utenti locali associati a una specifica SVM (Storage Virtual Machine)	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Visualizza informazioni dettagliate per tutti gli utenti locali su una SVM specificata	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Esempio

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

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

Eliminare gli account utente locali

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

A proposito di questa attività

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

- Il file system non viene modificato.

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

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

Fasi

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

Esempio

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

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


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

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

Gestire i gruppi locali

Modificare i gruppi locali

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

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

Esempi

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

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

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

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

Visualizza informazioni sui gruppi locali

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

Fase

1. Eseguire una delle seguenti operazioni:

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

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

Esempio

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

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

Gestire l'appartenenza al gruppo locale

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

tale gruppo.

A proposito di questa attività

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

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

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

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

Fase

1. Aggiungere o rimuovere un membro di un gruppo.

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

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

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

Nell'esempio seguente vengono rimossi gli utenti locali "SMB_SERVER` sue" e "SMB_SERVER `Sjames"

dal gruppo locale "MB_SERVER engineering" su SVM vs1:

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

Informazioni correlate

Visualizzazione delle informazioni sui membri dei gruppi locali

Visualizza le informazioni sui membri dei gruppi locali

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

Fase

1. Eseguire una delle seguenti operazioni:

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

Esempio

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

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

Eliminare un gruppo locale

È possibile eliminare un gruppo locale dalla macchina virtuale di storage (SVM) se non è

più necessario per determinare i diritti di accesso ai dati associati a tale SVM o se non è più necessario per assegnare i diritti utente (privilegi) di SVM ai membri del gruppo.

A proposito di questa attività

Quando si eliminano gruppi locali, tenere presente quanto segue:

- Il file system non viene modificato.

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

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

Fasi

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

Esempio

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

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

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

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

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

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

A proposito di questa attività

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

Fasi

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

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

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

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

Esempio

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

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

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

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

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

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

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

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

Gestire i privilegi locali

Aggiungere privilegi a utenti o gruppi locali o di dominio

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

Fasi

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

Esempio

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

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

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

Rimuovere i privilegi da utenti o gruppi locali o di dominio

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

personalizzare i privilegi massimi di utenti e gruppi.

Prima di iniziare

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

A proposito di questa attività

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

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

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

Fasi

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

Esempio

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

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

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

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

Ripristinare i privilegi per utenti e gruppi locali o di dominio

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

A proposito di questa attività

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

Fasi

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

Esempi

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

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

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

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

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

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

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

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

Visualizza le informazioni sugli override dei privilegi

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

Fase

1. Eseguire una delle seguenti operazioni:

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

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

Esempio

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

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

Configurare il controllo incrociato del bypass

Configurare la panoramica del controllo incrociato del bypass

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

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

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

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

Configurare il controllo incrociato del bypass

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

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

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

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

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

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

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

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

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

Informazioni correlate

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

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

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

Creare elenchi di controllo degli accessi di condivisione SMB

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

Elenco dei privilegi supportati

Aggiungere privilegi a utenti o gruppi locali o di dominio

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

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

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

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

Esempio

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

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

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

Informazioni correlate

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

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

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

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

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

Esempio

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

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

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

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

Informazioni correlate

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

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

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

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

Visualizzazione delle informazioni sulla sicurezza dei file

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

- NTFS
- UNIX
- Misto

Visualizzazione delle informazioni sui criteri di controllo

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

- SMB (tutte le versioni)
- NFSv4.x

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

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

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

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

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

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

Informazioni correlate

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

Visualizzazione di informazioni su Storage-Level Access Guard

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

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi di sicurezza NTFS, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli attributi DOS. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

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

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

Fase

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

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

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

Esempi

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

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

                                 Vserver: vs1
                               File Path: /vol4
                       File Inode Number: 64
                          Security Style: ntfs
                         Effective Style: ntfs
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

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

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

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
```

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

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

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

```
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

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

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

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

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

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


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

Informazioni correlate

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

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

Visualizza informazioni sulla sicurezza dei file su volumi misti di sicurezza

È possibile visualizzare informazioni sulla sicurezza di file e directory su volumi misti di sicurezza, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

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

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

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

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

Fase

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

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

Esempi

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

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

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

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

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

                                 Vserver: vs1
                               File Path: /data
                       File Inode Number: 544
                          Security Style: mixed
                         Effective Style: ntfs
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

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

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

Informazioni correlate

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

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

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

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi UNIX di tipo Security, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati

per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

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

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

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

- I campi di output del proprietario e del gruppo nell'output ACL non sono validi nel caso dei descrittori di protezione NFSv4.

  Sono significativi solo per i descrittori di protezione NTFS.

- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Con dettagli più dettagliati	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` In SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` In SVM vs1 sotto forma di maschera espansa:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: 0x10
                      ...0 .... .... .... = Offline
                      .... ..0. .... .... = Sparse
                      .... .... 0... .... = Normal
                      .... .... ..0. .... = Archive
                      .... .... ...1 .... = Directory
                      .... .... .... .0.. = System
                      .... .... .... ..0. = Hidden
                      .... .... .... ...0 = Read Only
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                  Unix Mode Bits in Text: rwx------
                                    ACLs: -
```

Informazioni correlate

Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security

Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza

Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

  I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

Fase

1. Visualizzare le impostazioni dei criteri di controllo di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Come elenco dettagliato	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` In SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/datavol1` In SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Visualizza informazioni sui criteri di audit NFSv4 sui volumi FlexVol utilizzando la CLI

È possibile visualizzare informazioni sui criteri di controllo di NFSv4 sui volumi FlexVol utilizzando l'interfaccia CLI di ONTAP, inclusi gli stili di sicurezza e gli stili di sicurezza

effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo dell'accesso al sistema (SACL). È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle directory di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo SACL NFSv4 per le policy di controllo.
- I file e le directory di un volume misto di sicurezza con stile UNIX possono applicare criteri di controllo NFSv4.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NFSv4.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL normali di file NFSv4, directory e SACL NTFS di Storage-Level Access Guard.
- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

Fasi

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Con dettagli più dettagliati	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/lab` In SVM vs1. Questo percorso di sicurezza UNIX ha un SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

È possibile utilizzare il carattere jolly (*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o volume root.

Il carattere jolly (**) può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory. Se si desidera visualizzare le informazioni di un particolare file o directory denominata "*"**, è necessario fornire il percorso completo tra virgolette doppie ("``").

Esempio

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso `/1/` Di SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                   Vserver: vs1
                 File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                   Vserver: vs1
                 File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Il seguente comando visualizza le informazioni di un file denominato "*" sotto il percorso `/vol1/a` Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la CLI

Gestisci la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la panoramica CLI

È possibile gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su macchine virtuali storage (SVM) utilizzando la CLI.

È possibile gestire la sicurezza dei file NTFS e le policy di controllo dai client SMB o utilizzando la CLI. Tuttavia, l’utilizzo della CLI per configurare le policy di controllo e sicurezza dei file elimina la necessità di utilizzare un client remoto per gestire la sicurezza dei file. L’utilizzo della CLI può ridurre significativamente il tempo necessario per applicare la protezione a molti file e cartelle utilizzando un singolo comando.

È possibile configurare Access Guard a livello di storage, un altro livello di sicurezza applicato da ONTAP ai volumi SVM. Storage-Level Access Guard si applica agli accessi da tutti i protocolli NAS all’oggetto storage a cui è applicato Storage-Level Access Guard.

Access Guard a livello di storage può essere configurato e gestito solo dalla CLI di ONTAP. Non è possibile gestire le impostazioni di Storage-Level Access Guard dai client SMB. Inoltre, se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, non viene visualizzata la protezione Storage-Level Access Guard. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX). Pertanto, Storage-Level Access Guard offre un ulteriore livello di sicurezza per l’accesso ai dati, impostato e gestito in modo indipendente dall’amministratore dello storage.

> Anche se sono supportate solo le autorizzazioni di accesso NTFS per Storage-Level Access Guard, ONTAP può eseguire controlli di sicurezza per l'accesso via NFS ai dati sui volumi in cui viene applicato Storage-Level Access Guard se l'utente UNIX esegue il mapping a un utente Windows sulla SVM proprietaria del volume.

Volumi NTFS di tipo Security

Tutti i file e le cartelle contenuti nei volumi e nei qtree di sicurezza NTFS dispongono di un'efficace protezione NTFS. È possibile utilizzare `vserver security file-directory` Famiglia di comandi per implementare i seguenti tipi di protezione sui volumi NTFS di tipo Security:

- Permessi dei file e policy di controllo per file e cartelle contenuti nel volume
- Protezione degli accessi a livello di storage sui volumi

Volumi misti di sicurezza

I volumi e i qtree misti in stile di sicurezza possono contenere alcuni file e cartelle con una protezione efficace UNIX e che utilizzano autorizzazioni per i file UNIX, i criteri di controllo Mbit di modalità o ACL NFSv4.x e NFSv4.x, nonché alcuni file e cartelle con una protezione effettiva NTFS e che utilizzano le autorizzazioni per i file NTFS e i criteri di controllo. È possibile utilizzare `vserver security file-directory` famiglia di comandi per applicare i seguenti tipi di protezione a dati misti di tipo sicurezza:

- Permessi dei file e policy di controllo per file e cartelle con NTFS efficace in stile di sicurezza nel volume misto o nel qtree
- Access Guard a livello di storage per i volumi con sicurezza efficace NTFS e UNIX

Volumi UNIX di tipo Security

I volumi e le qtree UNIX di sicurezza contengono file e cartelle con protezione efficace UNIX (ovvero i bit di modalità o gli ACL NFSv4.x). Se si desidera utilizzare il, tenere presente quanto segue `vserver security file-directory` Famiglia di comandi per implementare la sicurezza su volumi UNIX di tipo Security:

- Il `vserver security file-directory` La famiglia di comandi non può essere utilizzata per gestire la sicurezza dei file UNIX e le policy di controllo su qtree e volumi di sicurezza UNIX.
- È possibile utilizzare `vserver security file-directory` Famiglia di comandi per configurare Storage-Level Access Guard su volumi UNIX di tipo Security, a condizione che SVM con il volume di destinazione contenga un server CIFS.

Informazioni correlate

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la CLI

Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

Casi di utilizzo dell'interfaccia CLI per impostare la sicurezza di file e cartelle

Poiché è possibile applicare e gestire la sicurezza di file e cartelle in locale senza il coinvolgimento di un client remoto, è possibile ridurre significativamente il tempo necessario per impostare la protezione in blocco su un gran numero di file o cartelle.

È possibile utilizzare la CLI per impostare la sicurezza di file e cartelle nei seguenti casi di utilizzo:

- Storage di file in ambienti aziendali di grandi dimensioni, ad esempio lo storage di file nelle home directory
- Migrazione dei dati
- Modifica del dominio Windows
- Standardizzazione delle policy di controllo e sicurezza dei file nei file system NTFS

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

È necessario conoscere alcuni limiti quando si utilizza la CLI per impostare la sicurezza di file e cartelle.

- Il `vserver security file-directory` La famiglia di comandi non supporta l'impostazione degli ACL NFSv4.

  È possibile applicare i descrittori di protezione NTFS solo a file e cartelle NTFS.

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

I descrittori di protezione contengono gli elenchi di controllo degli accessi che determinano le azioni che un utente può eseguire su file e cartelle e le operazioni controllate quando un utente accede a file e cartelle.

- **Autorizzazioni**

  Le autorizzazioni sono consentite o negate dal proprietario di un oggetto e determinano le azioni che un oggetto (utenti, gruppi o oggetti computer) può eseguire su file o cartelle specifici.

- **Descrittori di sicurezza**

  I descrittori di protezione sono strutture di dati che contengono informazioni di sicurezza che definiscono le autorizzazioni associate a un file o a una cartella.

- **ACL (Access Control List)**

  Gli elenchi di controllo degli accessi sono gli elenchi contenuti in un descrittore di protezione che contengono informazioni sulle azioni che gli utenti, i gruppi o gli oggetti computer possono eseguire nel file o nella cartella a cui è applicato il descrittore di protezione. Il descrittore di protezione può contenere i seguenti due tipi di ACL:

  - DACL (Discretionary Access Control List)
  - SACL (System Access Control List)

- **Elenchi di controllo degli accessi discrezionali (DACL)**

  I DACL contengono l'elenco dei SIDS per gli utenti, i gruppi e gli oggetti computer ai quali è consentito o negato l'accesso per eseguire azioni su file o cartelle. I DACL contengono zero o più voci di controllo degli accessi (ACE).

- **System access control list (SACL)**

  I SACL contengono l'elenco di SIDS per gli utenti, i gruppi e gli oggetti computer per i quali vengono

registrati eventi di controllo riusciti o non riusciti. I SACL contengono zero o più voci di controllo degli accessi (ACE).

- **Voci di controllo di accesso (ACE)**

  Gli assi sono singole voci in DACL o SACL:

  - Una voce di controllo dell'accesso DACL specifica i diritti di accesso consentiti o negati per determinati utenti, gruppi o oggetti computer.
  - Una voce di controllo dell'accesso SACL specifica gli eventi di successo o di errore da registrare quando si controllano le azioni specifiche eseguite da utenti, gruppi o oggetti computer specifici.

- **Ereditarietà delle autorizzazioni**

  L'ereditarietà delle autorizzazioni descrive il modo in cui le autorizzazioni definite nei descrittori di protezione vengono propagate a un oggetto da un oggetto padre. Solo le autorizzazioni ereditabili vengono ereditate dagli oggetti figlio. Quando si impostano le autorizzazioni sull'oggetto padre, è possibile decidere se cartelle, sottocartelle e file possono ereditare tali autorizzazioni con "applicabile a. `this-folder`, `sub-folders`e `files`".

Informazioni correlate

"Controllo SMB e NFS e tracciamento della sicurezza"

Configurazione e applicazione dei criteri di controllo a file e cartelle NTFS mediante l'interfaccia CLI

Linee guida per l'applicazione di policy di directory di file che utilizzano utenti o gruppi locali sulla destinazione di disaster recovery SVM

Prima di applicare i criteri di directory dei file alla destinazione di disaster recovery SVM (Storage Virtual Machine) in una configurazione di eliminazione dell'ID, è necessario tenere presenti alcune linee guida se la configurazione dei criteri di directory dei file utilizza utenti o gruppi locali nel descrittore di protezione o nelle voci DACL o SACL.

È possibile configurare una configurazione di disaster recovery per una SVM in cui la SVM di origine sul cluster di origine replica i dati e la configurazione dalla SVM di origine a una SVM di destinazione su un cluster di destinazione.

È possibile configurare uno dei due tipi di disaster recovery SVM:

- Identità preservata

  Con questa configurazione, l'identità di SVM e del server CIFS viene preservata.

- Identità scartata

  Con questa configurazione, l'identità di SVM e del server CIFS non viene preservata. In questo scenario, il nome di SVM e del server CIFS sulla SVM di destinazione è diverso da SVM e dal nome del server CIFS sulla SVM di origine.

Linee guida per le configurazioni di identità scartate

In una configurazione con eliminazione dell'identità, per un'origine SVM che contiene configurazioni di utente, gruppo e privilegi locali, il nome del dominio locale (nome del server CIFS locale) deve essere modificato in

modo che corrisponda al nome del server CIFS sulla destinazione SVM. Ad esempio, se il nome SVM di origine è “vs1” e il nome del server CIFS è “CIFS1” e il nome SVM di destinazione è “vs1_dst” e il nome del server CIFS è “CIFS1_DST”, il nome del dominio locale di un utente locale denominato “CIFS1` user1” viene automaticamente modificato in "`CIFST_DVM_1".

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Anche se i nomi degli utenti e dei gruppi locali vengono modificati automaticamente nei database degli utenti e dei gruppi locali, i nomi degli utenti o dei gruppi locali non vengono modificati automaticamente nelle configurazioni dei criteri delle directory dei file (criteri configurati sulla CLI tramite `vserver security file-directory` famiglia di comandi).

Ad esempio, per “vs1”, se è stata configurata una voce DACL in cui si trova `-account` Il parametro è impostato su "`CIFS1` user1", l’impostazione non viene modificata automaticamente sulla SVM di destinazione per riflettere il nome del server CIFS di destinazione.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

È necessario utilizzare `vserver security file-directory modify` Comandi per modificare manualmente il nome del server CIFS nel nome del server CIFS di destinazione.

Componenti di configurazione dei criteri di directory dei file che contengono parametri dell'account

Esistono tre componenti di configurazione dei criteri di directory dei file che possono utilizzare le impostazioni dei parametri che possono contenere utenti o gruppi locali:

- Descrittore di sicurezza

  È possibile specificare il proprietario del descrittore di protezione e il gruppo primario del proprietario del descrittore di protezione. Se il descrittore di protezione utilizza un utente o un gruppo locale per le voci del proprietario e del gruppo primario, è necessario modificare il descrittore di protezione per utilizzare la SVM di destinazione nel nome dell'account. È possibile utilizzare `vserver security file-directory ntfs modify` per apportare le modifiche necessarie ai nomi degli account.

- Voci DACL

  Ogni voce DACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i DACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci DACL esistenti, è necessario rimuovere eventuali voci DACL con utenti o gruppi locali dai descrittori di protezione, creare nuove voci DACL con i nomi account di destinazione corretti e associare queste nuove voci DACL ai descrittori di protezione appropriati.

- Voci SACL

  Ogni voce SACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i SACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci SACL esistenti, è necessario rimuovere eventuali voci SACL con

utenti o gruppi locali dai descrittori di protezione, creare nuove voci SACL con i nomi account di destinazione corretti e associare queste nuove voci SACL ai descrittori di protezione appropriati.

Prima di applicare il criterio, è necessario apportare le modifiche necessarie agli utenti o ai gruppi locali utilizzati nella configurazione del criterio della directory dei file; in caso contrario, il processo di applicazione non riesce.

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Creare un descrittore di protezione NTFS

La creazione di un descrittore di sicurezza NTFS (policy di sicurezza dei file) è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo degli accessi NTFS (ACL) a file e cartelle che risiedono nelle macchine virtuali di storage (SVM). È possibile associare il descrittore di protezione al percorso di file o cartelle in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Aggiungere le voci di controllo dell'accesso DACL NTFS al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) al descrittore di protezione NTFS è il secondo passo nella configurazione e nell'applicazione di ACL NTFS a un file o a una cartella. Ciascuna voce identifica l'oggetto a cui è consentito o negato l'accesso e definisce le operazioni che l'oggetto può o non può eseguire nei file o nelle cartelle definiti nell'ACE.

A proposito di questa attività

È possibile aggiungere uno o più ACE al DACL del descrittore di protezione.

Se il descrittore di protezione contiene un DACL con ACE esistenti, il comando aggiunge il nuovo ACE al DACL. Se il descrittore di protezione non contiene un DACL, il comando crea il DACL e aggiunge il nuovo ACE.

È possibile personalizzare le voci DACL specificando i diritti che si desidera consentire o negare per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)

> Se non si specificano i diritti per la voce DACL, l'impostazione predefinita è impostare i diritti su `Full Control`.

È possibile personalizzare le voci DACL specificando come applicare l'ereditarietà.

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere una voce DACL a un descrittore di protezione: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verificare che la voce DACL sia corretta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                    Vserver: vs1
         Security Descriptor Name: sd1
                   Allow or Deny: deny
             Account Name or SID: DOMAIN\joe
                   Access Rights: full-control
          Advanced Access Rights: -
                        Apply To: this-folder
                   Access Rights: full-control
```

Creare policy di sicurezza

La creazione di una policy di sicurezza dei file per le SVM è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare i criteri di protezione a ogni SVM (contenente volumi di sicurezza NTFS o volumi di sicurezza misti).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può

essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

Quando si aggiungono attività ai criteri di protezione, è necessario specificare i seguenti quattro parametri richiesti:

- Nome SVM
- Nome policy
- Percorso
- Descrittore di sicurezza da associare al percorso

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori

informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Applicare le policy di sicurezza

L'applicazione di una policy di sicurezza dei file alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificare la sicurezza del file applicata

È possibile verificare le impostazioni di sicurezza del file per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione abbiano le impostazioni desiderate.

A proposito di questa attività

Specificare il nome della SVM contenente i dati e il percorso del file e delle cartelle in cui si desidera verificare le impostazioni di sicurezza. È possibile utilizzare il opzionale `-expand-mask` per visualizzare informazioni dettagliate sulle impostazioni di sicurezza.

Fase

1. Visualizzare le impostazioni di sicurezza di file e cartelle: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   ```

```
-expand-mask true
```

```
         Vserver: vs1
               File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
```

```
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
```

```
                                .... ...0 .... .... .... .... .... .... =
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI

È necessario eseguire diversi passaggi per applicare i criteri di controllo a file e cartelle NTFS quando si utilizza l'interfaccia utente di ONTAP. Innanzitutto, si crea un descrittore di protezione NTFS e si aggiungono SACL al descrittore di protezione. Quindi, creare una policy di sicurezza e aggiungere attività di policy. Quindi, applicare il criterio di protezione a una macchina virtuale di storage (SVM).

A proposito di questa attività

Dopo aver applicato il criterio di protezione, è possibile monitorare il processo di criteri di protezione e verificare le impostazioni per il criterio di controllo applicato.

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Informazioni correlate

Protezione dell'accesso ai file mediante Storage-Level Access Guard

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

"Controllo SMB e NFS e tracciamento della sicurezza"

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Creare un descrittore di protezione NTFS

La creazione di un criterio di audit del descrittore di protezione NTFS è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo di accesso (ACL) NTFS a file e cartelle che risiedono all'interno delle SVM. Il descrittore di protezione verrà associato al percorso del file o della cartella in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Se si desidera utilizzare i parametri avanzati, impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Creare un descrittore di sicurezza: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verificare che la configurazione del descrittore di protezione sia corretta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                          Vserver: vs1
                              Security Descriptor Name: sd1
                     Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se si è nel livello di privilegio avanzato, tornare al livello di privilegio admin: `set -privilege admin`

Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) SACL (elenco di controllo di accesso al sistema) al descrittore di protezione NTFS è la seconda fase della creazione di criteri di controllo NTFS per file o cartelle in SVM. Ogni voce identifica l'utente o il gruppo che si desidera controllare. La voce SACL definisce se si desidera controllare i tentativi di accesso riusciti o non riusciti.

A proposito di questa attività

È possibile aggiungere uno o più ACE al SACL del descrittore di protezione.

Se il descrittore di protezione contiene un SACL con ACE esistenti, il comando aggiunge il nuovo ACE al SACL. Se il descrittore di protezione non contiene un SACL, il comando crea il SACL e aggiunge il nuovo ACE.

È possibile configurare le voci SACL specificando i diritti da controllare per gli eventi di successo o di errore per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)

> Se non si specificano i diritti per la voce SACL, l'impostazione predefinita è `Full Control`.

È possibile personalizzare le voci SACL specificando come applicare l'ereditarietà con `apply to` parametro.

Se non si specifica questo parametro, l'impostazione predefinita prevede l'applicazione di questa voce SACL a questa cartella, sottocartelle e file.

Fasi

1. Aggiungere una voce SACL a un descrittore di protezione: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verificare che la voce SACL sia corretta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                   Vserver: vs1
                     Security Descriptor Name: sd1
         Access type for Specified Access Rights: failure
                         Account Name or SID: DOMAIN\joe
                               Access Rights: full-control
                      Advanced Access Rights: -
                                    Apply To: this-folder
                               Access Rights: full-control
   ```

Creare policy di sicurezza

La creazione di un criterio di audit per le macchine virtuali di storage (SVM) è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare la policy di sicurezza a ciascuna macchina virtuale di storage (SVM) (contenente volumi di sicurezza NTFS o volumi misti di sicurezza).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver
   vs1
   ```

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Applicare le policy di sicurezza

L'applicazione di un criterio di audit alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificare la policy di audit applicata

È possibile verificare il criterio di controllo per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione dispongano delle impostazioni di sicurezza di controllo desiderate.

A proposito di questa attività

Si utilizza `vserver security file-directory show` comando per visualizzare le informazioni sui criteri di controllo. Specificare il nome della SVM che contiene i dati e il percorso dei dati di cui si desidera visualizzare le informazioni sui criteri di controllo del file o della cartella.

Fase

1. Visualizzare le impostazioni dei criteri di controllo: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Esempio

Il seguente comando visualizza le informazioni di policy di audit applicate al percorso "/corp" in SVM vs1. Il percorso ha applicato sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerazioni per la gestione dei processi di policy di sicurezza

Se esiste un processo di policy di sicurezza, in determinate circostanze non è possibile modificare tale policy o le attività assegnate a tale policy. È necessario comprendere in quali condizioni è possibile o meno modificare le policy di sicurezza in modo che i tentativi di modifica vengano eseguiti correttamente. Le modifiche al criterio includono l'aggiunta, la rimozione o la modifica delle attività assegnate al criterio e l'eliminazione o la modifica del criterio.

Non è possibile modificare un criterio di protezione o un'attività assegnata a tale criterio se esiste un processo per tale criterio e tale processo si trova nei seguenti stati:

- Il lavoro è in esecuzione o in corso.
- Il processo viene messo in pausa.
- Il lavoro viene ripreso e si trova in esecuzione.
- Se il processo è in attesa di eseguire il failover su un altro nodo.

Nei seguenti casi, se esiste un processo per un criterio di protezione, è possibile modificare correttamente tale criterio di protezione o un'attività assegnata a tale criterio:

- Il processo di policy viene arrestato.
- Il processo di policy è stato completato correttamente.

Comandi per la gestione dei descrittori di sicurezza NTFS

Esistono comandi ONTAP specifici per la gestione dei descrittori di protezione. È possibile creare, modificare, eliminare e visualizzare informazioni sui descrittori di protezione.

Se si desidera…	Utilizzare questo comando…
Creare descrittori di protezione NTFS	`vserver security file-directory ntfs create`
Modificare i descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs modify`
Visualizza informazioni sui descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs show`
Eliminare i descrittori di protezione NTFS	`vserver security file-directory ntfs delete`

Vedere le pagine man per `vserver security file-directory ntfs` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS DACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi DACL (Access Control). È possibile aggiungere ACE ai DACL NTFS in qualsiasi momento. È inoltre possibile gestire i DACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei DACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai DACL NTFS	`vserver security file-directory ntfs dacl add`

Se si desidera…	Utilizzare questo comando…
Modificare gli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl modify`
Visualizza le informazioni sugli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl show`
Rimuovere gli ACE esistenti dai DACL NTFS	`vserver security file-directory ntfs dacl remove`

Vedere le pagine man per `vserver security file-directory ntfs dacl` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS SACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi SACL (ACE). È possibile aggiungere ACE ai SACL NTFS in qualsiasi momento. È inoltre possibile gestire i SACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei SACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai SACL NTFS	`vserver security file-directory ntfs sacl add`
Modificare gli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl modify`
Visualizza le informazioni sugli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl show`
Rimuovere gli ACE esistenti dai SACL NTFS	`vserver security file-directory ntfs sacl remove`

Vedere le pagine man per `vserver security file-directory ntfs sacl` per ulteriori informazioni.

Comandi per la gestione delle policy di sicurezza

Esistono comandi ONTAP specifici per la gestione delle policy di sicurezza. È possibile visualizzare informazioni sui criteri ed eliminare i criteri. Non è possibile modificare un criterio di protezione.

Se si desidera…	Utilizzare questo comando…
Creare policy di sicurezza	`vserver security file-directory policy create`

Se si desidera…	Utilizzare questo comando…
Visualizzare informazioni sulle policy di sicurezza	`vserver security file-directory policy show`
Eliminare le policy di sicurezza	`vserver security file-directory policy delete`

Vedere le pagine man per `vserver security file-directory policy` per ulteriori informazioni.

Comandi per la gestione delle attività dei criteri di protezione

Sono disponibili comandi ONTAP per aggiungere, modificare, rimuovere e visualizzare informazioni sulle attività dei criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Aggiungere attività di policy di sicurezza	`vserver security file-directory policy task add`
Modificare le attività dei criteri di protezione	`vserver security file-directory policy task modify`
Visualizza informazioni sulle attività dei criteri di protezione	`vserver security file-directory policy task show`
Rimuovere le attività dei criteri di protezione	`vserver security file-directory policy task remove`

Vedere le pagine man per `vserver security file-directory policy task` per ulteriori informazioni.

Comandi per la gestione dei processi di policy di sicurezza

Sono disponibili comandi ONTAP per mettere in pausa, riprendere, arrestare e visualizzare informazioni sui processi relativi ai criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Sospendere i processi di policy di sicurezza	`vserver security file-directory job pause -vserver vserver_name -id integer`
Riprendere i processi di policy di sicurezza	`vserver security file-directory job resume -vserver vserver_name -id integer`

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni sui processi di policy di sicurezza	`vserver security file-directory job show -vserver vserver_name` È possibile determinare l'ID lavoro di un lavoro utilizzando questo comando.
Arrestare i processi di policy di sicurezza	`vserver security file-directory job stop -vserver vserver_name -id integer`

Vedere le pagine man per `vserver security file-directory job` per ulteriori informazioni.

Configurare la cache dei metadati per le condivisioni SMB

Come funziona il caching dei metadati SMB

Il caching dei metadati consente il caching degli attributi dei file sui client SMB 1.0 per fornire un accesso più rapido agli attributi di file e cartelle. È possibile attivare o disattivare il caching degli attributi in base alla condivisione. È inoltre possibile configurare il time-to-live per le voci memorizzate nella cache se è attivata la cache dei metadati. La configurazione del caching dei metadati non è necessaria se i client si connettono alle condivisioni tramite SMB 2.x o SMB 3.0.

Quando questa opzione è attivata, la cache dei metadati SMB memorizza i dati di attributi di percorso e file per un periodo di tempo limitato. Ciò può migliorare le performance delle PMI per i client SMB 1.0 con carichi di lavoro comuni.

Per alcune attività, SMB crea una quantità significativa di traffico che può includere più query identiche per i metadati di percorso e file. È possibile ridurre il numero di query ridondanti e migliorare le performance per i client SMB 1.0 utilizzando il caching dei metadati SMB per recuperare le informazioni dalla cache.

> Sebbene improbabile, è possibile che la cache dei metadati serva informazioni obsolete ai client SMB 1.0. Se il tuo ambiente non può permettersi questo rischio, non dovresti attivare questa funzionalità.

Attivare la cache dei metadati SMB

È possibile migliorare le performance SMB per i client SMB 1.0 attivando la cache dei metadati SMB. Per impostazione predefinita, il caching dei metadati SMB è disattivato.

Fase

1. Eseguire l'azione desiderata:

Se si desidera…	Immettere il comando…
Attiva il caching dei metadati SMB quando crei una condivisione	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`

Se si desidera…	Immettere il comando…
Abilitare il caching dei metadati SMB su una condivisione esistente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informazioni correlate

Configurazione della durata delle voci della cache dei metadati SMB

Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente

Configurare la durata delle voci della cache dei metadati SMB

È possibile configurare la durata delle voci della cache dei metadati SMB per ottimizzare le prestazioni della cache dei metadati SMB nel proprio ambiente. L'impostazione predefinita è 10 secondi.

Prima di iniziare

È necessario aver attivato la funzione cache dei metadati SMB. Se il caching dei metadati SMB non è attivato, l'impostazione TTL della cache SMB non viene utilizzata.

Fase

1. Eseguire l'azione desiderata:

Se si desidera configurare la durata delle voci della cache dei metadati SMB quando…	Immettere il comando…
Creare una condivisione	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modificare una condivisione esistente	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

È possibile specificare ulteriori proprietà e opzioni di configurazione della condivisione quando si creano o modificano le condivisioni. Per ulteriori informazioni, consulta le pagine man.

Gestire i blocchi dei file

Informazioni sul blocco dei file tra protocolli

Il blocco dei file è un metodo utilizzato dalle applicazioni client per impedire a un utente di accedere a un file precedentemente aperto da un altro utente. Il modo in cui ONTAP blocca i file dipende dal protocollo del client.

Se il client è un client NFS, i blocchi sono avvisi; se il client è un client SMB, i blocchi sono obbligatori.

A causa delle differenze tra i blocchi di file NFS e SMB, un client NFS potrebbe non riuscire ad accedere a un file precedentemente aperto da un'applicazione SMB.

Quando un client NFS tenta di accedere a un file bloccato da un'applicazione SMB, si verifica quanto segue:

- In volumi misti o NTFS, operazioni di manipolazione dei file come `rm`, `rmdir`, e. `mv` Può causare il malfunzionamento dell'applicazione NFS.
- Le operazioni di lettura e scrittura NFS sono negate rispettivamente dalle modalità aperta di negazione-lettura e di negazione-scrittura di SMB.
- Le operazioni di scrittura NFS non riescono quando l'intervallo scritto del file è bloccato con un esclusivo bytelock SMB.
- Scollega
  - Per i file system NTFS, sono supportate operazioni di eliminazione SMB e CIFS.

    Il file verrà rimosso dopo l'ultima chiusura.
  - Le operazioni di scollegamento NFS non sono supportate.

    Non è supportato perché sono necessarie semantiche NTFS e SMB e l'ultima operazione Delete-on-Close non è supportata per NFS.
  - Per i filesystem UNIX, è supportata l'operazione di scollegamento.

    È supportato perché sono richieste semantiche NFS e UNIX.
- Rinominare
  - Per i file system NTFS, se il file di destinazione viene aperto da SMB o CIFS, il file di destinazione può essere rinominato.
  - La ridenominazione NFS non è supportata.

    Non è supportato perché sono necessarie semantiche NTFS e SMB.

Nei volumi UNIX di sicurezza, le operazioni di sconnessione e ridenominazione NFS ignorano lo stato di blocco SMB e consentono l'accesso al file. Tutte le altre operazioni NFS sui volumi UNIX di sicurezza rispettano lo stato di blocco SMB.

Come ONTAP tratta i bit di sola lettura

Il bit di sola lettura viene impostato file per file per indicare se un file è scrivibile (disattivato) o di sola lettura (abilitato).

I client SMB che utilizzano Windows possono impostare un bit di sola lettura per ogni file. I client NFS non impostano un bit di sola lettura per ogni file perché i client NFS non eseguono operazioni di protocollo che utilizzano un bit di sola lettura per ogni file.

ONTAP può impostare un bit di sola lettura su un file quando un client SMB che utilizza Windows crea tale file. ONTAP può anche impostare un bit di sola lettura quando un file viene condiviso tra client NFS e client SMB. Alcuni software, se utilizzati dai client NFS e dai client SMB, richiedono l'abilitazione del bit di sola lettura.

Affinché ONTAP mantenga le autorizzazioni di lettura e scrittura appropriate su un file condiviso tra client NFS

e client SMB, tratta il bit di sola lettura in base alle seguenti regole:

- NFS considera qualsiasi file con il bit di sola lettura abilitato come se non abbia alcun bit di permesso di scrittura abilitato.
- Se un client NFS disattiva tutti i bit di permesso di scrittura e almeno uno di questi bit era stato precedentemente attivato, ONTAP attiva il bit di sola lettura per quel file.
- Se un client NFS attiva qualsiasi bit di autorizzazione di scrittura, ONTAP disattiva il bit di sola lettura per quel file.
- Se il bit di sola lettura per un file è attivato e un client NFS tenta di rilevare le autorizzazioni per il file, i bit di autorizzazione per il file non vengono inviati al client NFS; invece, ONTAP invia i bit di autorizzazione al client NFS con i bit di autorizzazione di scrittura mascherati.
- Se il bit di sola lettura per un file è attivato e un client SMB disattiva il bit di sola lettura, ONTAP attiva il bit di autorizzazione di scrittura del proprietario per il file.
- I file con il bit di sola lettura abilitato sono scrivibili solo da root.

> Le modifiche alle autorizzazioni dei file hanno effetto immediato sui client SMB, ma potrebbero non avere effetto immediato sui client NFS se il client NFS attiva il caching degli attributi.

In che modo ONTAP si differenzia da Windows per la gestione dei blocchi sui componenti del percorso di condivisione

A differenza di Windows, ONTAP non blocca ogni componente del percorso di un file aperto mentre il file è aperto. Questo comportamento influisce anche sui percorsi di condivisione SMB.

Poiché ONTAP non blocca ogni componente del percorso, è possibile rinominare un componente del percorso sopra il file aperto o la condivisione, che può causare problemi per alcune applicazioni o causare l'invalidità del percorso di condivisione nella configurazione SMB. Questo può rendere la condivisione inaccessibile.

Per evitare problemi causati dalla ridenominazione dei componenti del percorso, è possibile applicare impostazioni di sicurezza che impediscono agli utenti o alle applicazioni di rinominare le directory critiche.

Visualizza informazioni sui blocchi

È possibile visualizzare informazioni sui blocchi di file correnti, inclusi i tipi di blocchi che vengono conservati e lo stato di blocco, i dettagli sui blocchi dell'intervallo di byte, le modalità sharelock, i blocchi di delega e i blocchi opportunistici e se i blocchi vengono aperti con handle durevoli o persistenti.

A proposito di questa attività

L'indirizzo IP del client non può essere visualizzato per i blocchi stabiliti tramite NFSv4 o NFSv4.1.

Per impostazione predefinita, il comando visualizza le informazioni relative a tutti i blocchi. È possibile utilizzare i parametri dei comandi per visualizzare informazioni sui blocchi di una specifica macchina virtuale di storage (SVM) o per filtrare l'output del comando in base ad altri criteri.

Il `vserver locks show` il comando visualizza informazioni su quattro tipi di blocchi:

- Blocchi byte-range, che bloccano solo una parte di un file.

- Blocchi di condivisione che bloccano i file aperti.
- Blocchi opportunistici, che controllano il caching lato client su SMB.
- Deleghe, che controllano il caching lato client su NFSv4.x.

Specificando i parametri opzionali, è possibile determinare informazioni importanti su ciascun tipo di blocco. Per ulteriori informazioni, vedere la pagina man per il comando.

Fase

1. Visualizzare le informazioni sui blocchi utilizzando `vserver locks show` comando.

Esempi

Nell'esempio riportato di seguito vengono visualizzate informazioni riepilogative per un blocco NFSv4 su un file con il percorso `/vol1/file1`. La modalità di accesso sharelock è write-deny_none e il blocco è stato concesso con delega di scrittura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

Nell'esempio riportato di seguito vengono visualizzate informazioni dettagliate sull'oplock e sullo sharlock relative al blocco SMB in un file con il percorso `/data2/data2_2/intro.pptx`. Un handle durevole viene concesso sul file con una modalità di accesso con blocco della condivisione write-deny_none a un client con un indirizzo IP 10.3.1.3. Un oplock di leasing viene concesso con un livello di oplock batch:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
```

```
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Blocchi di interruzione

Quando i blocchi di file impediscono l'accesso dei client ai file, è possibile visualizzare le informazioni sui blocchi attualmente in attesa e quindi interrompere blocchi specifici. Esempi di scenari in cui potrebbe essere necessario interrompere i blocchi includono il debug delle applicazioni.

A proposito di questa attività

Il `vserver locks break` il comando è disponibile solo a un livello di privilegio avanzato e superiore. La pagina man del comando contiene informazioni dettagliate.

Fasi

1. Per trovare le informazioni necessarie per interrompere un blocco, utilizzare `vserver locks show` comando.

   La pagina man del comando contiene informazioni dettagliate.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Eseguire una delle seguenti operazioni:

Se si desidera interrompere un blocco specificando…	Immettere il comando…
Il nome SVM, il nome del volume, il nome LIF e il percorso del file	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID blocco	`vserver locks break -lockid UUID`

4. Tornare al livello di privilegio admin: `set -privilege admin`

Monitorare l'attività delle PMI

Visualizzare le informazioni sulla sessione SMB

È possibile visualizzare informazioni sulle sessioni SMB stabilite, tra cui la connessione SMB, l'ID della sessione e l'indirizzo IP della workstation che utilizza la sessione. È possibile visualizzare informazioni sulla versione del protocollo SMB della sessione e sul livello di protezione continuamente disponibile, per identificare se la sessione supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare le informazioni relative a tutte le sessioni della SVM in forma di riepilogo. Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali:

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output relativo ai campi scelti.

  È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sulle sessioni SMB stabilite.
- È possibile utilizzare `-fields` o il `-instance` parametro da solo o in combinazione con altri parametri opzionali.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
Per tutte le sessioni su SVM in forma di riepilogo	`vserver cifs session show -vserver vserver_name`
Su un ID di connessione specificato	`vserver cifs session show -vserver vserver_name -connection-id integer`
Da un indirizzo IP della workstation specificato	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Su un indirizzo IP LIF specificato	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Su un nodo specificato	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Da un utente Windows specificato
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Con un meccanismo di autenticazione specificato
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Con una versione del protocollo specificata	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== La protezione a disponibilità continua e SMB Multichannel sono disponibili solo su SMB 3.0 e sessioni successive. Per visualizzarne lo stato in tutte le sessioni qualificanti, specificare questo parametro con il valore impostato su `SMB3` o versioni successive. ====

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
Con un livello specifico di protezione a disponibilità continua	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Se lo stato di disponibilità continua è `Partial`, questo significa che la sessione contiene almeno un file aperto a disponibilità continua, ma la sessione ha alcuni file che non sono aperti con una protezione continuamente disponibile. È possibile utilizzare `vserver cifs sessions file show` comando per determinare quali file della sessione stabilita non sono aperti con una protezione continuamente disponibile. ====
Con uno stato di sessione SMB Signing specificato	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Esempi

Il seguente comando visualizza le informazioni sulla sessione per le sessioni su SVM vs1 stabilite da una workstation con indirizzo IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

Il seguente comando visualizza informazioni dettagliate sulla sessione per le sessioni con protezione continuamente disponibile su SVM vs1. La connessione è stata effettuata utilizzando l’account di dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Il seguente comando visualizza le informazioni di sessione su una sessione che utilizza SMB 3.0 e SMB Multichannel su SVM vs1. Nell'esempio, l'utente si è connesso a questa condivisione da un client SMB 3.0 utilizzando l'indirizzo IP LIF; pertanto, il meccanismo di autenticazione è stato impostato su NTLMv2 per impostazione predefinita. La connessione deve essere effettuata utilizzando l'autenticazione Kerberos per connettersi con la protezione continuamente disponibile.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informazioni correlate

Visualizzazione delle informazioni sui file SMB aperti

Visualizzare le informazioni sui file SMB aperti

È possibile visualizzare informazioni sui file SMB aperti, tra cui la connessione SMB e l'ID sessione, il volume di hosting, il nome della condivisione e il percorso di condivisione. È possibile visualizzare informazioni sul livello di protezione continuamente disponibile di un file, utile per determinare se un file aperto si trova in uno stato che supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare informazioni sui file aperti in una sessione SMB stabilita. Le informazioni visualizzate sono utili quando è necessario determinare le informazioni della sessione SMB per determinati file all'interno di una sessione SMB.

Ad esempio, se si dispone di una sessione SMB in cui alcuni dei file aperti sono aperti con una protezione continuamente disponibile e alcuni non sono aperti con una protezione continuamente disponibile (il valore per `-continuously-available` campo in `vserver cifs session show` l'output del comando è `Partial`), è possibile determinare quali file non sono continuamente disponibili utilizzando questo comando.

È possibile visualizzare le informazioni relative a tutti i file aperti nelle sessioni SMB stabilite sulle macchine virtuali di storage (SVM) in forma riepilogativa utilizzando `vserver cifs session file show` senza

parametri opzionali.

Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Ciò può essere utile quando si desidera visualizzare informazioni solo per un piccolo sottoinsieme di file aperti.

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output nei campi scelti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sui file SMB aperti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
Sul modulo SVM in forma di riepilogo	`vserver cifs session file show -vserver vserver_name`
Su un nodo specificato	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Su un ID file specificato
`vserver cifs session file show -vserver vserver_name -file-id integer`	Su un ID connessione SMB specificato
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Su un ID sessione SMB specificato
`vserver cifs session file show -vserver vserver_name -session-id integer`	Sull'aggregato di hosting specificato
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Sul volume specificato
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Sulla condivisione SMB specificata

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	Sul percorso SMB specificato
`vserver cifs session file show -vserver vserver_name -path path`	Con il livello specificato di protezione a disponibilità continua
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Se lo stato di disponibilità continua è `No`, questo significa che questi file aperti non sono in grado di eseguire il ripristino senza interruzioni dal takeover e dal giveback. Inoltre, non possono essere ripristinati dal trasferimento generale di aggregati tra partner in una relazione ad alta disponibilità. ====
Con lo stato di riconnessione specificato	`vserver cifs session file show -vserver vserver_name -reconnected {No

Sono disponibili ulteriori parametri opzionali che è possibile utilizzare per perfezionare i risultati di output. Per ulteriori informazioni, consulta la pagina man.

Esempi

Nell'esempio seguente vengono visualizzate informazioni sui file aperti su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sui file SMB aperti con ID file 82 su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informazioni correlate

Visualizzazione delle informazioni sulla sessione SMB

Determinare quali oggetti e contatori statistici sono disponibili

Prima di ottenere informazioni su CIFS, SMB, audit e statistiche hash BranchCache e monitorare le performance, è necessario sapere quali oggetti e contatori sono disponibili per ottenere i dati.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera determinare…	Inserisci…
Quali oggetti sono disponibili	`statistics catalog object show`
Oggetti specifici disponibili	`statistics catalog object show object object_name`
Quali contatori sono disponibili	`statistics catalog counter show object object_name`

   Per ulteriori informazioni sugli oggetti e i contatori disponibili, consultare le pagine man.

3. Tornare al livello di privilegio admin: `set -privilege admin`

Esempi

Il seguente comando visualizza le descrizioni degli oggetti statistici selezionati relativi all'accesso CIFS e SMB nel cluster, come si vede al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Il seguente comando visualizza informazioni su alcuni contatori di `cifs` oggetto visto a livello di privilegi avanzati:

In questo esempio non vengono visualizzati tutti i contatori disponibili per `cifs` oggetto; l'output è troncato.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                      2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informazioni correlate

Visualizzazione delle statistiche

Visualizzare le statistiche

È possibile visualizzare varie statistiche, tra cui statistiche su CIFS e SMB, audit e hash di BranchCache, per monitorare le performance e diagnosticare i problemi.

Prima di iniziare

È necessario aver raccolto campioni di dati utilizzando `statistics start` e. `statistics stop` prima di poter visualizzare informazioni sugli oggetti.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le statistiche per…	Inserisci…
Tutte le versioni di SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x e SMB 3.0	`statistics show -object smb2`
Sottosistema CIFS del nodo	`statistics show -object nblade_cifs`
Audit multiprotocollo	`statistics show -object audit_ng`
Servizio hash BranchCache	`statistics show -object hashd`
DNS dinamico	`statistics show -object ddns_update`

   Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

3. Tornare al livello di privilegio admin: `set -privilege admin`

Informazioni correlate

Determinazione degli oggetti e dei contatori delle statistiche disponibili

Monitoraggio delle statistiche delle sessioni firmate SMB

Visualizzazione delle statistiche di BranchCache

Utilizzo delle statistiche per monitorare l'attività di riferimento automatico del nodo

"Configurazione SMB per Microsoft Hyper-V e SQL Server"

"Configurazione del monitoraggio delle performance"

Implementare servizi basati su client SMB

Utilizzare i file offline per consentire il caching dei file per l'utilizzo offline

Utilizzare i file offline per consentire il caching dei file per la panoramica dell'utilizzo offline

ONTAP supporta la funzione Microsoft Offline Files, o *caching lato client*, che consente di memorizzare i file nella cache dell'host locale per l'utilizzo offline. Gli utenti possono utilizzare la funzionalità offline Files per continuare a lavorare sui file anche quando sono disconnessi dalla rete.

È possibile specificare se i documenti utente e i programmi Windows vengono automaticamente memorizzati nella cache di una condivisione o se i file devono essere selezionati manualmente per il caching. Il caching manuale è attivato per impostazione predefinita per le nuove condivisioni. I file resi disponibili offline vengono sincronizzati sul disco locale del client Windows. La sincronizzazione si verifica quando viene ripristinata la connettività di rete a una specifica condivisione del sistema di storage.

Poiché i file e le cartelle offline mantengono le stesse autorizzazioni di accesso della versione dei file e delle cartelle salvati sul server CIFS, l'utente deve disporre di autorizzazioni sufficienti per i file e le cartelle salvati sul server CIFS per eseguire azioni sui file e sulle cartelle offline.

Quando l'utente e un altro utente della rete apportano modifiche allo stesso file, l'utente può salvare la versione locale del file nella rete, conservare l'altra versione o salvare entrambe. Se l'utente mantiene entrambe le versioni, un nuovo file con le modifiche dell'utente locale viene salvato localmente e il file memorizzato nella cache viene sovrascritto con le modifiche della versione del file salvato sul server CIFS.

È possibile configurare i file offline in base alla condivisione utilizzando le impostazioni di configurazione della condivisione. È possibile scegliere una delle quattro configurazioni di cartelle offline quando si creano o modificano le condivisioni:

- Nessun caching

  Disattiva il caching lato client per la condivisione. I file e le cartelle non vengono automaticamente memorizzati nella cache locale sui client e gli utenti non possono scegliere di memorizzare nella cache i file o le cartelle localmente.

- Caching manuale

  Consente la selezione manuale dei file da memorizzare nella cache della condivisione. Questa è l'impostazione predefinita. Per impostazione predefinita, nessun file o cartella viene memorizzato nella cache del client locale. Gli utenti possono scegliere i file e le cartelle da memorizzare nella cache locale per l'utilizzo offline.

- Caching automatico dei documenti

  Consente di memorizzare automaticamente i documenti utente nella cache della condivisione. Solo i file e le cartelle a cui si accede vengono memorizzati nella cache locale.

- Caching automatico dei programmi

  Consente ai programmi e ai documenti utente di essere automaticamente memorizzati nella cache della condivisione. Solo i file, le cartelle e i programmi a cui si accede vengono memorizzati nella cache locale. Inoltre, questa impostazione consente al client di eseguire file eseguibili memorizzati nella cache locale anche quando è connesso alla rete.

Per ulteriori informazioni sulla configurazione dei file offline su server e client Windows, consultare la Microsoft TechNet Library.

Informazioni correlate

Utilizzo di profili roaming per memorizzare i profili utente centralmente su un server CIFS associato a SVM

Utilizzo del reindirizzamento delle cartelle per memorizzare i dati su un server CIFS

Utilizzo di BranchCache per memorizzare nella cache SMB i contenuti vengono condivisi in una filiale

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti per l'utilizzo di file offline

Prima di poter utilizzare la funzionalità file offline di Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano tale funzionalità.

Requisiti di versione di ONTAP

Le release di ONTAP supportano i file offline.

Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta i file offline su tutte le versioni di SMB.

Requisiti del client Windows

Il client Windows deve supportare i file offline.

Per informazioni aggiornate sui client Windows che supportano la funzionalità file offline, vedere la matrice di interoperabilità.

"mysupport.netapp.com/matrix"

Linee guida per la distribuzione di file offline

Esistono alcune importanti linee guida da comprendere quando si distribuiscono file offline nelle condivisioni home directory che dispongono di `showsnapshot` proprietà di condivisione impostata nelle home directory.

Se il `showsnapshot` La proprietà Share viene impostata su una condivisione home directory con file offline configurati, i client Windows memorizzano nella cache tutte le copie Snapshot in `~snapshot` nella home directory dell'utente.

I client Windows memorizzano nella cache tutte le copie Snapshot nella home directory se si verifica una delle seguenti condizioni:

- L'utente rende la home directory disponibile offline dal client.

  Il contenuto di `~snapshot` la cartella nella home directory viene inclusa e resa disponibile offline.

- L'utente configura il reindirizzamento delle cartelle per reindirizzare una cartella come `My Documents` Alla

directory principale di una home directory che risiede nella condivisione del server CIFS.

Alcuni client Windows potrebbero rendere automaticamente disponibile la cartella reindirizzata offline. Se la cartella viene reindirizzata alla directory principale della home directory, il `~snapshot` la cartella è inclusa nel contenuto offline memorizzato nella cache.

> Implementazioni di file offline in cui `~snapshot` la cartella è inclusa nei file offline dovrebbe essere evitata. Le copie Snapshot in `~snapshot` La cartella contiene tutti i dati sul volume nel punto in cui ONTAP ha creato la copia Snapshot. Pertanto, è necessario creare una copia offline di `~snapshot` la cartella consuma un notevole storage locale sul client, consuma la larghezza di banda della rete durante la sincronizzazione dei file offline e aumenta il tempo necessario per la sincronizzazione dei file offline.

Configurare il supporto dei file offline sulle condivisioni SMB utilizzando la CLI

È possibile configurare il supporto dei file offline utilizzando l'interfaccia utente di ONTAP specificando una delle quattro impostazioni offline quando si creano condivisioni SMB o in qualsiasi momento modificando le condivisioni SMB esistenti. Il supporto manuale dei file offline è l'impostazione predefinita.

A proposito di questa attività

Quando si configura il supporto per i file offline, è possibile scegliere una delle seguenti quattro impostazioni per i file offline:

Impostazione	Descrizione
`none`	Non consente ai client Windows di memorizzare nella cache i file presenti in questa condivisione.
`manual`	Consente agli utenti sui client Windows di selezionare manualmente i file da memorizzare nella cache.
`documents`	Consente ai client Windows di memorizzare nella cache i documenti utente utilizzati dall'utente per l'accesso offline.
`programs`	Consente ai client Windows di memorizzare nella cache i programmi utilizzati dall'utente per l'accesso offline. I client possono utilizzare i file di programma memorizzati nella cache in modalità offline anche se la condivisione è disponibile.

È possibile scegliere una sola impostazione di file offline. Se si modifica un'impostazione dei file offline su una condivisione SMB esistente, la nuova impostazione dei file offline sostituisce l'impostazione originale. Le altre impostazioni di configurazione della condivisione SMB e le proprietà di condivisione esistenti non vengono rimosse o sostituite. Rimangono in vigore fino a quando non vengono esplicitamente rimossi o modificati.

Fasi

1. Eseguire l'azione appropriata:

Se si desidera configurare i file offline su…	Immettere il comando…
Una nuova condivisione SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Una condivisione SMB esistente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Verificare che la configurazione della condivisione SMB sia corretta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Esempio

Il seguente comando crea una condivisione SMB denominata “data1” con i file offline impostati su `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                     Share Comment: Offline files
                         Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                       Volume Name: -
                     Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Il seguente comando modifica una condivisione SMB esistente denominata “data1” modificando l’impostazione

dei file offline su `manual` e aggiungendo i valori per la maschera di creazione della modalità file e directory:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: 644
     Directory Mode Creation Mask: 777
                  Share Comment: Offline files
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                  Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informazioni correlate

Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente

Configurare il supporto dei file offline sulle condivisioni SMB utilizzando la MMC Gestione computer

Se si desidera consentire agli utenti di memorizzare i file nella cache locale per l'utilizzo offline, è possibile configurare il supporto dei file offline utilizzando la console MMC Gestione computer (Microsoft Management Console).

Fasi

1. Per aprire MMC sul server Windows, in Esplora risorse fare clic con il pulsante destro del mouse sull'icona del computer locale, quindi selezionare **Gestisci**.
2. Nel pannello di sinistra, selezionare **Gestione computer**.
3. Selezionare **azione** > **connessione a un altro computer**.

   Viene visualizzata la finestra di dialogo Select computer (Seleziona computer).

4. Digitare il nome del server CIFS o fare clic su **Browse** (Sfoglia) per individuare il server CIFS.

   Se il nome del server CIFS corrisponde al nome host della macchina virtuale di storage (SVM), digitare il

nome SVM. Se il nome del server CIFS è diverso dal nome host SVM, digitare il nome del server CIFS.

5. Fare clic su **OK**.
6. Nella struttura della console, fare clic su **System Tools** > **Shared Folders**.
7. Fare clic su **shares**.
8. Nel riquadro dei risultati, fare clic con il pulsante destro del mouse sulla condivisione.
9. Fare clic su **Proprietà**.

   Vengono visualizzate le proprietà della condivisione selezionata.

10. Nella scheda **Generale**, fare clic su **Impostazioni offline**.

    Viene visualizzata la finestra di dialogo Offline Settings (Impostazioni offline).

11. Configurare le opzioni di disponibilità offline in base alle esigenze.
12. Fare clic su **OK**.

Utilizzare i profili roaming per memorizzare i profili utente centralmente su un server SMB associato a SVM

Utilizza i profili di roaming per memorizzare i profili utente centralmente su un server SMB associato alla panoramica SVM

ONTAP supporta la memorizzazione dei profili di roaming Windows su un server CIFS associato alla macchina virtuale di storage (SVM). La configurazione dei profili di roaming degli utenti offre vantaggi all'utente, ad esempio la disponibilità automatica delle risorse, indipendentemente dalla posizione di accesso dell'utente. I profili roaming semplificano inoltre l'amministrazione e la gestione dei profili utente.

I profili utente comuni presentano i seguenti vantaggi:

- Disponibilità automatica delle risorse

  Il profilo univoco di un utente è automaticamente disponibile quando l'utente accede a qualsiasi computer della rete che esegue Windows 8, Windows 7, Windows 2000 o Windows XP. Gli utenti non devono creare un profilo su ciascun computer in rete.

- Sostituzione semplificata del computer

  Poiché tutte le informazioni del profilo dell'utente vengono conservate separatamente sulla rete, è possibile scaricare facilmente il profilo dell'utente su un nuovo computer sostitutivo. Quando l'utente accede al nuovo computer per la prima volta, la copia del profilo dell'utente sul server viene copiata nel nuovo computer.

Informazioni correlate

Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline

Utilizzo del reindirizzamento delle cartelle per memorizzare i dati su un server CIFS

Requisiti per l'utilizzo dei profili di roaming

Prima di poter utilizzare i profili di roaming di Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano la funzionalità.

Requisiti di versione di ONTAP

ONTAP supporta i profili di roaming.

Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta i profili di roaming su tutte le versioni di SMB.

Requisiti del client Windows

Prima che un utente possa utilizzare i profili di roaming, il client Windows deve supportare la funzione.

Per informazioni aggiornate sui client Windows che supportano i profili di roaming, consultare la matrice di interoperabilità.

"Tool di matrice di interoperabilità NetApp"

Configurare i profili di roaming

Se si desidera rendere automaticamente disponibile il profilo di un utente quando quest'ultimo effettua l'accesso a un computer della rete, è possibile configurare i profili di roaming tramite lo snap-in MMC utenti e computer di Active Directory. Se si configurano profili comuni su Windows Server, è possibile utilizzare il Centro di amministrazione di Active Directory.

Fasi

1. Sul server Windows, aprire la MMC utenti e computer di Active Directory (o Active Directory Administration Center sui server Windows).
2. Individuare l'utente per cui si desidera configurare un profilo di roaming.
3. Fare clic con il pulsante destro del mouse sull'utente e fare clic su **Proprietà**.
4. Nella scheda **Profilo**, immettere il percorso del profilo per la condivisione in cui si desidera memorizzare il profilo di roaming dell'utente, seguito da `%username%`.

   Ad esempio, il percorso di un profilo potrebbe essere il seguente: `\\vs1.example.com\profiles\%username%`. La prima volta che un utente effettua l'accesso, `%username%` viene sostituito con il nome dell'utente.

   > Nel percorso `\\vs1.example.com\profiles\%username%`, `profiles` È il nome di condivisione di una condivisione su SVM (Storage Virtual Machine) vs1 con diritti di controllo completo per tutti.

5. Fare clic su **OK**.

Utilizzare il reindirizzamento delle cartelle per memorizzare i dati su un server SMB

Utilizzare il reindirizzamento delle cartelle per memorizzare i dati su una panoramica del server SMB

ONTAP supporta il reindirizzamento delle cartelle Microsoft, che consente agli utenti o agli amministratori di reindirizzare il percorso di una cartella locale a una posizione sul server CIFS. Sembra che le cartelle reindirizzate siano memorizzate sul client Windows locale, anche se i dati sono memorizzati in una condivisione SMB.

Il reindirizzamento delle cartelle è destinato principalmente alle organizzazioni che hanno già implementato le home directory e che desiderano mantenere la compatibilità con l'ambiente di home directory esistente.

- `Documents`, `Desktop`, e. `Start Menu` sono esempi di cartelle che è possibile reindirizzare.
- Gli utenti possono reindirizzare le cartelle dal client Windows.
- Gli amministratori possono configurare e gestire centralmente il reindirizzamento delle cartelle configurando gli oggetti Criteri di gruppo in Active Directory.
- Se gli amministratori hanno configurato i profili di roaming, il reindirizzamento delle cartelle consente agli amministratori di dividere i dati degli utenti dai dati del profilo.
- Gli amministratori possono utilizzare il reindirizzamento delle cartelle e i file offline insieme per reindirizzare lo storage dei dati per le cartelle locali al server CIFS, consentendo allo stesso tempo agli utenti di memorizzare il contenuto nella cache locale.

Informazioni correlate

Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline

Utilizzo di profili roaming per memorizzare i profili utente centralmente su un server CIFS associato a SVM

Requisiti per l'utilizzo del reindirizzamento delle cartelle

Prima di poter utilizzare il reindirizzamento delle cartelle Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano la funzionalità.

Requisiti di versione di ONTAP

ONTAP supporta il reindirizzamento delle cartelle Microsoft.

Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta il reindirizzamento delle cartelle Microsoft su tutte le versioni di SMB.

Requisiti del client Windows

Prima che un utente possa utilizzare il reindirizzamento delle cartelle di Microsoft, il client Windows deve supportare questa funzionalità.

Per informazioni aggiornate sui client Windows che supportano il reindirizzamento delle cartelle, consultare la matrice di interoperabilità.

"mysupport.netapp.com/matrix"

Configurare il reindirizzamento delle cartelle

È possibile configurare il reindirizzamento delle cartelle utilizzando la finestra Proprietà di Windows. Il vantaggio di utilizzare questo metodo consiste nel fatto che l'utente Windows può configurare il reindirizzamento delle cartelle senza l'assistenza dell'amministratore di SVM.

Fasi

1. In Esplora risorse, fare clic con il pulsante destro del mouse sulla cartella che si desidera reindirizzare a una condivisione di rete.
2. Fare clic su **Proprietà**.

   Vengono visualizzate le proprietà della condivisione selezionata.

3. Nella scheda **scelta rapida**, fare clic su **destinazione** e specificare il percorso di rete in cui si desidera reindirizzare la cartella selezionata.

   Ad esempio, se si desidera reindirizzare una cartella a `data` in una home directory mappata a. `Q:\`, specificare `Q:\data` come destinazione.

4. Fare clic su **OK**.

   Per ulteriori informazioni sulla configurazione delle cartelle offline, consultare la Microsoft TechNet Library.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Accedere alla directory ~snapshot dai client Windows utilizzando SMB 2.x.

Il metodo utilizzato per accedere a. `~snapshot` La directory dei client Windows che utilizzano SMB 2.x differisce dal metodo utilizzato per SMB 1.0. È necessario conoscere le modalità di accesso a `~snapshot` Directory quando si utilizzano connessioni SMB 2.x per accedere correttamente ai dati memorizzati nelle copie Snapshot.

L'amministratore di SVM controlla se gli utenti sui client Windows possono visualizzare e accedere a. `~snapshot` directory su una condivisione attivando o disattivando `showsnapshot` condividere la proprietà utilizzando i comandi delle famiglie di proprietà di condivisione di vserver cifs.

Quando il `showsnapshot` La proprietà Share è disattivata, un utente su un client Windows che utilizza SMB 2.x non può visualizzare `~snapshot` E non possono accedere alle copie Snapshot in `~snapshot` directory, anche quando si immette manualmente il percorso di `~snapshot` Directory o a copie Snapshot specifiche all'interno della directory.

Quando il `showsnapshot` La proprietà Share è attivata, un utente su un client Windows che utilizza SMB 2.x non può ancora visualizzare `~snapshot` directory nella directory principale della condivisione o all'interno di qualsiasi giunzione o directory sotto la directory principale della condivisione. Tuttavia, dopo la connessione a una condivisione, l'utente può accedere a nascosto `~snapshot` directory aggiungendo manualmente `\~snapshot` alla fine del percorso di condivisione. Il nascosto `~snapshot` la directory è accessibile da due punti di ingresso:

- Alla radice della condivisione

- In ogni punto di giunzione nello spazio di condivisione

Il nascosto `~snapshot` la directory non è accessibile dalle sottodirectory non di giunzione all'interno della condivisione.

Esempio

Con la configurazione illustrata nell'esempio seguente, un utente su un client Windows con una connessione SMB 2.x alla condivisione "eng" può accedere a. `~snapshot` directory aggiungendo manualmente `\~snapshot` al percorso di condivisione alla radice della condivisione e in ogni punto di giunzione del percorso. Il nascosto `~snapshot` la directory è accessibile dai tre percorsi seguenti:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Ripristinare file e cartelle utilizzando le versioni precedenti

Panoramica sul ripristino di file e cartelle utilizzando le versioni precedenti

La possibilità di utilizzare le versioni precedenti di Microsoft è applicabile ai file system che supportano le copie Snapshot in qualche forma e le hanno attivate. La tecnologia Snapshot è parte integrante di ONTAP. Gli utenti possono ripristinare file e cartelle dalle copie Snapshot dal client Windows utilizzando la funzionalità delle versioni precedenti di Microsoft.

La funzionalità delle versioni precedenti offre agli utenti un metodo per sfogliare le copie Snapshot o per ripristinare i dati da una copia Snapshot senza l'intervento di un amministratore dello storage. Le versioni precedenti non sono configurabili. È sempre attivato. Se l'amministratore dello storage ha reso disponibili copie Snapshot in una condivisione, l'utente può utilizzare le versioni precedenti per eseguire le seguenti attività:

- Recuperare i file cancellati accidentalmente.

- Ripristino della sovrascrittura accidentale di un file.
- Confronta le versioni del file mentre lavori.

I dati memorizzati nelle copie Snapshot sono di sola lettura. Gli utenti devono salvare una copia di un file in un'altra posizione per apportare eventuali modifiche al file. Le copie Snapshot vengono periodicamente eliminate; pertanto, gli utenti devono creare copie dei file contenuti nelle versioni precedenti se desiderano conservare una versione precedente di un file a tempo indeterminato.

Requisiti per l'utilizzo delle versioni precedenti di Microsoft

Prima di poter utilizzare le versioni precedenti con il server CIFS, è necessario conoscere le versioni di ONTAP e SMB e i client Windows che lo supportano. È inoltre necessario conoscere il requisito di impostazione della copia Snapshot.

Requisiti di versione di ONTAP

Supporta le versioni precedenti.

Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta le versioni precedenti su tutte le versioni di SMB.

Requisiti del client Windows

Prima che un utente possa utilizzare le versioni precedenti per accedere ai dati nelle copie Snapshot, il client Windows deve supportare questa funzione.

Per informazioni aggiornate sui client Windows che supportano le versioni precedenti, consultare la matrice di interoperabilità.

"Tool di matrice di interoperabilità NetApp"

Requisiti per le impostazioni di copia Snapshot

Per utilizzare le versioni precedenti per accedere ai dati nelle copie Snapshot, al volume contenente i dati deve essere associata una policy Snapshot attivata, i client devono poter accedere ai dati Snapshot e devono esistere copie Snapshot.

Utilizzare la scheda versioni precedenti per visualizzare e gestire i dati di copia Snapshot

Gli utenti sulle macchine client Windows possono utilizzare la scheda versioni precedenti della finestra Proprietà di Windows per ripristinare i dati memorizzati nelle copie Snapshot senza richiedere l'intervento dell'amministratore della macchina virtuale di storage (SVM).

A proposito di questa attività

È possibile utilizzare la scheda versioni precedenti solo per visualizzare e gestire i dati nelle copie Snapshot dei dati memorizzati sulla SVM se l'amministratore ha attivato le copie Snapshot sul volume contenente la condivisione e se l'amministratore configura la condivisione in modo che visualizzi le copie Snapshot.

Fasi

1. In Esplora risorse, visualizzare il contenuto dell'unità mappata dei dati memorizzati nel server CIFS.

2. Fare clic con il pulsante destro del mouse sul file o sulla cartella nell'unità di rete mappata di cui si desidera visualizzare o gestire le copie Snapshot.
3. Fare clic su **Proprietà**.

   Vengono visualizzate le proprietà del file o della cartella selezionata.

4. Fare clic sulla scheda **versioni precedenti**.

   Nella casella Folder Versions: (Versioni cartella) viene visualizzato un elenco di copie Snapshot disponibili del file o della cartella selezionata. Le copie Snapshot elencate sono identificate dal prefisso del nome della copia Snapshot e dall'indicatore data e ora di creazione.

5. Nella casella **versioni cartella:**, fare clic con il pulsante destro del mouse sulla copia del file o della cartella che si desidera gestire.
6. Eseguire l'azione appropriata:

Se si desidera…	Effettuare le seguenti operazioni…
Visualizzare i dati della copia Snapshot	Fare clic su **Apri**.
Creare una copia dei dati da tale copia Snapshot	Fare clic su **Copy** (Copia).

   I dati nelle copie Snapshot sono di sola lettura. Se si desidera apportare modifiche ai file e alle cartelle elencati nella scheda versioni precedenti, è necessario salvare una copia dei file e delle cartelle che si desidera modificare in una posizione scrivibile e apportare modifiche alle copie.

7. Una volta terminata la gestione dei dati Snapshot, chiudere la finestra di dialogo **Proprietà** facendo clic su **OK**.

   Per ulteriori informazioni sull'utilizzo della scheda versioni precedenti per visualizzare e gestire i dati Snapshot, consultare la Microsoft TechNet Library.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Determinare se le copie Snapshot sono disponibili per le versioni precedenti

È possibile visualizzare le copie Snapshot dalla scheda versioni precedenti solo se al volume contenente la condivisione viene applicato un criterio Snapshot attivato e se la configurazione del volume consente l'accesso alle copie Snapshot. Determinare la disponibilità delle copie Snapshot è utile quando si assiste un utente con l'accesso alle versioni precedenti.

Fasi

1. Determinare se nel volume in cui risiedono i dati di condivisione sono attivate le copie Snapshot automatiche e se i client hanno accesso alle directory Snapshot: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   L'output visualizza il criterio Snapshot associato al volume, se l'accesso alla directory Snapshot del client è

attivato e il numero di copie Snapshot disponibili.

2. Determinare se la policy Snapshot associata è attivata: `volume snapshot policy show -policy policy-name`
3. Elencare le copie Snapshot disponibili: `volume snapshot show -volume volume_name`

   Per ulteriori informazioni sulla configurazione e la gestione delle policy Snapshot e delle pianificazioni Snapshot, vedere "Protezione dei dati".

Esempio

Nell'esempio seguente vengono visualizzate informazioni sulle policy Snapshot associate al volume denominato "data1" che contiene i dati condivisi e le copie Snapshot disponibili su "data1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                    3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- -------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                            ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Informazioni correlate

Creazione di una configurazione Snapshot per consentire l'accesso alle versioni precedenti

"Protezione dei dati"

Creare una configurazione Snapshot per consentire l'accesso alle versioni precedenti

La funzionalità delle versioni precedenti è sempre disponibile, a condizione che l'accesso client alle copie Snapshot sia attivato e che esistano copie Snapshot. Se la configurazione della copia Snapshot non soddisfa questi requisiti, è possibile creare una configurazione della copia Snapshot.

Fasi

1. Se il volume contenente la condivisione a cui si desidera consentire l'accesso alle versioni precedenti non dispone di un criterio Snapshot associato, associare un criterio Snapshot al volume e attivarlo utilizzando `volume modify` comando.

   Per ulteriori informazioni sull'utilizzo di `volume modify` vedere le pagine man.

2. Abilitare l'accesso alle copie Snapshot utilizzando `volume modify` per impostare `-snap-dir` opzione a. `true`.

   Per ulteriori informazioni sull'utilizzo di `volume modify` vedere le pagine man.

3. Verificare che i criteri Snapshot siano attivati e che l'accesso alle directory Snapshot sia attivato utilizzando `volume show` e. `volume snapshot policy show` comandi.

   Per ulteriori informazioni sull'utilizzo di `volume show` e. `volume snapshot policy show` comandi, vedere le pagine man.

   Per ulteriori informazioni sulla configurazione e la gestione delle policy Snapshot e delle pianificazioni Snapshot, vedere "Protezione dei dati".

Informazioni correlate

"Protezione dei dati"

Linee guida per il ripristino di directory che contengono giunzioni

Esistono alcune linee guida da tenere presenti quando si utilizzano versioni precedenti per ripristinare le cartelle che contengono punti di giunzione.

Quando si utilizzano le versioni precedenti per ripristinare le cartelle con cartelle figlio che sono punti di giunzione, il ripristino potrebbe non riuscire con un `Access Denied` errore.

È possibile determinare se la cartella che si sta tentando di ripristinare contiene una giunzione utilizzando `vol show` con il `-parent` opzione. È inoltre possibile utilizzare `vserver security trace` comandi per creare log dettagliati sui problemi di accesso a file e cartelle.

Informazioni correlate

Creazione e gestione di volumi di dati negli spazi dei nomi NAS

Implementare servizi basati su server SMB

Gestire le home directory

In che modo ONTAP abilita le home directory dinamiche

Le home directory di ONTAP consentono di configurare una condivisione SMB che viene mappata a diverse directory in base all'utente che si connette ad essa e a una serie di variabili. Invece di creare condivisioni separate per ciascun utente, è possibile configurare una condivisione con alcuni parametri della home directory per definire la relazione di un utente tra un punto di ingresso (la condivisione) e la home directory (una

directory sulla SVM).

Un utente che ha effettuato l'accesso come utente ospite non dispone di una home directory e non può accedere alle home directory di altri utenti. Esistono quattro variabili che determinano il modo in cui un utente viene mappato a una directory:

- **Nome condivisione**

  Si tratta del nome della condivisione creata a cui l'utente si connette. È necessario impostare la proprietà home directory per questa condivisione.

  Il nome della condivisione può utilizzare i seguenti nomi dinamici:

  - `%w` (Il nome utente Windows dell'utente)
  - `%d` (Il nome di dominio Windows dell'utente)
  - `%u` (Il nome utente UNIX mappato dell'utente) per rendere unico il nome di condivisione in tutte le home directory, il nome di condivisione deve contenere/`%w` o il `%u` variabile. Il nome della condivisione può contenere entrambi `%d` e a./`%w` variabile (ad esempio, `%d`/`%w`), oppure il nome della condivisione può contenere una porzione statica e una porzione variabile (ad esempio, home_/`%w`).

- **Percorso di condivisione**

  Si tratta del percorso relativo, definito dalla condivisione e quindi associato a uno dei nomi di condivisione, che viene aggiunto a ciascun percorso di ricerca per generare l'intero percorso della home directory dell'utente dalla directory principale della SVM. Può essere statico (ad esempio, `home`), dinamico (ad esempio, `%w`), o una combinazione dei due (ad esempio, `eng/%w`).

- **Percorsi di ricerca**

  Questo è l'insieme di percorsi assoluti dalla directory principale di SVM che si specifica che dirige la ricerca di home directory in ONTAP. È possibile specificare uno o più percorsi di ricerca utilizzando `vserver cifs home-directory search-path add` comando. Se si specificano più percorsi di ricerca, ONTAP li prova nell'ordine specificato fino a trovare un percorso valido.

- **Directory**

  Questa è la home directory dell'utente creata per l'utente. Il nome della directory è generalmente il nome dell'utente. È necessario creare la home directory in una delle directory definite dai percorsi di ricerca.

Ad esempio, considerare la seguente configurazione:

- Utente: John Smith
- Dominio utente: acme
- Nome utente: Jsmith
- Nome SVM: vs1
- Nome di condivisione della home directory n. 1: home_ `%w` - percorso di condivisione: `%w`
- Nome condivisione home directory n. 2: `%w` - percorso di condivisione: `%d/%w`
- Percorso di ricerca n. 1: `/vol0home/home`
- Percorso di ricerca n. 2: `/vol1home/home`

- Percorso di ricerca n. 3: `/vol2home/home`
- Home directory: `/vol1home/home/jsmith`

Scenario 1: L'utente si connette a. `\\vs1\home_jsmith`. Corrisponde al primo nome di condivisione della home directory e genera il relativo percorso `jsmith`. ONTAP ricerca ora una directory denominata `jsmith` selezionando ciascun percorso di ricerca nell'ordine indicato:

- `/vol0home/home/jsmith` non esiste; passaggio al percorso di ricerca n. 2.
- `/vol1home/home/jsmith` esiste; pertanto, il percorso di ricerca n. 3 non è selezionato; l'utente è ora connesso alla propria home directory.

Scenario 2: L'utente si connette a. `\\vs1\jsmith`. Corrisponde al secondo nome di condivisione della home directory e genera il relativo percorso `acme/jsmith`. ONTAP ricerca ora una directory denominata `acme/jsmith` selezionando ciascun percorso di ricerca nell'ordine indicato:

- `/vol0home/home/acme/jsmith` non esiste; passaggio al percorso di ricerca n. 2.
- `/vol1home/home/acme/jsmith` non esiste; passaggio al percorso di ricerca n. 3.
- `/vol2home/home/acme/jsmith` non esiste; la home directory non esiste; pertanto, la connessione non riesce.

Condivisioni home directory

Aggiungere una condivisione della home directory

Se si desidera utilizzare la funzione home directory SMB, è necessario aggiungere almeno una condivisione con la proprietà home directory inclusa nelle proprietà di condivisione.

A proposito di questa attività

È possibile creare una condivisione home directory al momento della creazione della condivisione utilizzando `vserver cifs share create` in alternativa, è possibile modificare una condivisione esistente in una condivisione della home directory in qualsiasi momento utilizzando `vserver cifs share modify` comando.

Per creare una condivisione della home directory, è necessario includere `homedirectory` valore in `-share -properties` quando si crea o si modifica una condivisione. È possibile specificare il nome della condivisione e il percorso di condivisione utilizzando variabili espanse dinamicamente quando gli utenti si connettono alle proprie home directory. Le variabili disponibili che è possibile utilizzare nel percorso sono `%w`, `%d`, e. `%u`, Corrispondenti rispettivamente al nome utente, al dominio e al nome utente UNIX mappato di Windows.

Fasi

1. Aggiungere una condivisione home directory:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.

   `-share-name` *`share-name`* specifica il nome di condivisione della home directory.

Oltre a contenere una delle variabili richieste, se il nome della condivisione contiene una delle stringhe letterali `%w`, `%u`, o. `%d`, È necessario precedere la stringa letterale con un carattere % (percentuale) per impedire a ONTAP di trattare la stringa letterale come una variabile (ad esempio, `%%w`).

- Il nome della condivisione deve contenere `%w` o il `%u` variabile.
- Il nome della condivisione può contenere anche `%d` variabile (ad esempio, `%d/%w`) o una parte statica nel nome della condivisione (ad esempio, home1_/`%w`).
- Se la condivisione viene utilizzata dagli amministratori per connettersi alle home directory di altri utenti o per consentire agli utenti di connettersi alle home directory di altri utenti, il modello dinamico di nome della condivisione deve essere preceduto da una tilde (~).

  Il `vserver cifs home-directory modify` viene utilizzato per abilitare questo accesso impostando `-is-home-dirs-access-for-admin-enabled` opzione a. `true`) o impostando l'opzione avanzata `-is-home-dirs-access-for-public-enabled` a. `true`.

`-path path` specifica il percorso relativo alla home directory.

`-share-properties homedirectory[,…]` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

1. Verificare che la condivisione della home directory sia stata aggiunta correttamente utilizzando `vserver cifs share show` comando.

Esempio

Il seguente comando crea una condivisione della home directory denominata `%w`. Il `oplocks`, `browsable`, e. `changenotify` oltre all'impostazione di, vengono impostate le proprietà di condivisione `homedirectory` condividere la proprietà.

> Questo esempio non visualizza l'output per tutte le condivisioni sulla SVM. L'output viene troncato.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Informazioni correlate

Aggiunta di un percorso di ricerca della home directory

Requisiti e linee guida per l'utilizzo dei riferimenti automatici ai nodi

Gestione dell'accessibilità alle home directory degli utenti

Le condivisioni della home directory richiedono nomi utente univoci

Fare attenzione a assegnare nomi utente univoci quando si creano condivisioni home directory utilizzando `%w` (Nome utente Windows) o. `%u` (Nome utente UNIX) variabili per generare condivisioni in modo dinamico. Il nome della condivisione viene associato al nome utente.

Quando il nome di una condivisione statica e il nome di un utente sono identici, possono verificarsi due problemi:

- Quando l'utente elenca le condivisioni su un cluster utilizzando `net view` vengono visualizzate due condivisioni con lo stesso nome utente.
- Quando l'utente si connette a tale nome di condivisione, l'utente è sempre connesso alla condivisione statica e non può accedere alla condivisione della home directory con lo stesso nome.

Ad esempio, esiste una condivisione denominata "Administrator" e si dispone di un nome utente Windows "Administrator". Se si crea una condivisione home directory e ci si connette a tale condivisione, si viene connessi alla condivisione statica "Administrator" e non alla condivisione home directory "Administrator".

Per risolvere il problema relativo ai nomi di condivisione duplicati, procedere come segue:

- Ridenominazione della condivisione statica in modo che non sia più in conflitto con la condivisione della home directory dell'utente.
- Assegnare all'utente un nuovo nome utente in modo che non sia più in conflitto con il nome di condivisione statico.
- Creazione di una condivisione della home directory CIFS con un nome statico come "home" invece di utilizzare `%w` per evitare conflitti con i nomi di condivisione.

Cosa accade ai nomi di condivisione della home directory statica dopo l'aggiornamento

I nomi di condivisione della home directory devono contenere `%w` o il `%u` variabile dinamica. Dopo l'aggiornamento a una versione di ONTAP con il nuovo requisito, dovresti essere consapevole di ciò che accade ai nomi di condivisione della home directory statica esistenti.

Se la configurazione della home directory contiene nomi di condivisione statici e si esegue l'aggiornamento a ONTAP, i nomi di condivisione della home directory statica non vengono modificati e sono ancora validi. Tuttavia, non è possibile creare nuove condivisioni della home directory che non contengono `%w` oppure `%u` variabile.

La richiesta di includere una di queste variabili nel nome di condivisione della home directory dell'utente garantisce che ogni nome di condivisione sia univoco nella configurazione della home directory. Se lo si desidera, è possibile modificare i nomi di condivisione della home directory statica in nomi che contengono `%w` oppure `%u` variabile.

Aggiungere un percorso di ricerca della home directory

Se si desidera utilizzare le home directory SMB di ONTAP, è necessario aggiungere almeno un percorso di ricerca della home directory.

A proposito di questa attività

È possibile aggiungere un percorso di ricerca della home directory utilizzando `vserver cifs home-directory search-path add` comando.

Il `vserver cifs home-directory search-path add` il comando verifica il percorso specificato in `-path` durante l'esecuzione del comando. Se il percorso specificato non esiste, il comando genera un messaggio che richiede se si desidera continuare. Scegli tu `y` oppure `n`. Se si sceglie `y` Per continuare, ONTAP crea il percorso di ricerca. Tuttavia, è necessario creare la struttura di directory prima di poter utilizzare il percorso di ricerca nella configurazione della home directory. Se si sceglie di non continuare, il comando non riesce; il percorso di ricerca non viene creato. È quindi possibile creare la struttura della directory dei percorsi ed eseguire di nuovo il `vserver cifs home-directory search-path add` comando.

Fasi

1. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.

Esempio

Nell'esempio seguente viene aggiunto il percorso `/home1` Alla configurazione della home directory su SVM vs1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Nell'esempio seguente viene tentato di aggiungere il percorso `/home2` Alla configurazione della home directory su SVM vs1. Il percorso non esiste. La scelta è fatta per non continuare.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informazioni correlate

Aggiunta di una condivisione della home directory

Creare una configurazione della home directory utilizzando le variabili %w e %d.

È possibile creare una configurazione della home directory utilizzando `%w` e. `%d` variabili. Gli utenti possono quindi connettersi alla propria home share utilizzando condivisioni

create dinamicamente.

Fasi

1. Creare un qtree per contenere le home directory dell'utente: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verificare che il qtree utilizzi lo stile di protezione corretto: `volume qtree show`
3. Se qtree non utilizza lo stile di protezione desiderato, modificare lo stile di protezione utilizzando `volume qtree security` comando.
4. Aggiunta di una condivisione home directory: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.

   `-share-name %w` specifica il nome di condivisione della home directory. ONTAP crea dinamicamente il nome di condivisione quando ogni utente si connette alla propria home directory. Il nome della condivisione avrà il formato *Windows_User_NAME*.

   `-path %d/%w` specifica il percorso relativo alla home directory. Il percorso relativo viene creato dinamicamente quando ciascun utente si connette alla propria home directory e avrà la forma *domain/Windows_user_name*.

   `-share-properties homedirectory[,…]+` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

5. Verificare che la condivisione abbia la configurazione desiderata utilizzando `vserver cifs share show` comando.
6. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Specifica la SVM abilitata per CIFS su cui aggiungere il percorso di ricerca.

   `-path` *`path`* specifica il percorso assoluto della directory per il percorso di ricerca.

7. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.
8. Per gli utenti con una home directory, creare una directory corrispondente nel qtree o nel volume designato per contenere home directory.

   Ad esempio, se è stato creato un qtree con il percorso di `/vol/vol1/users` e il nome utente di cui si desidera creare la directory è mydomain.user1, si crea una directory con il seguente percorso: `/vol/vol1/users/mydomain/user1`.

   Se è stato creato un volume denominato "home1" montato in `/home1`, creare una directory con il seguente percorso: `/home1/mydomain/user1`.

9. Verificare che un utente possa connettersi correttamente alla home share mappando un disco o connettendosi utilizzando il percorso UNC.

Ad esempio, se l'utente mydomain/user1 desidera connettersi alla directory creata nella fase 8 che si trova su SVM vs1, l'utente 1 si connette utilizzando il percorso UNC `\\vs1\user1`.

Esempio

I comandi dell'esempio seguente creano una configurazione della home directory con le seguenti impostazioni:

- Il nome della condivisione è %w.
- Il percorso relativo della home directory è %d/%W.
- Il percorso di ricerca utilizzato per contenere le home directory, `/home1`, È un volume configurato con lo stile di protezione NTFS.
- La configurazione viene creata su SVM vs1.

È possibile utilizzare questo tipo di configurazione della home directory quando gli utenti accedono alle home directory dagli host Windows. È possibile utilizzare questo tipo di configurazione anche quando gli utenti accedono alle proprie home directory da host Windows e UNIX e l'amministratore del file system utilizza utenti e gruppi basati su Windows per controllare l'accesso al file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Informazioni correlate

Configurazione delle home directory utilizzando la variabile %u

Configurazioni aggiuntive della home directory

Visualizzazione delle informazioni sul percorso home directory di un utente SMB

Configurare le home directory utilizzando la variabile %u

È possibile creare una configurazione della home directory in cui designare il nome della condivisione utilizzando `%w` variabile ma si utilizza `%u` variabile per indicare il percorso relativo alla condivisione della home directory. Gli utenti possono quindi connettersi alla propria home share utilizzando condivisioni create dinamicamente utilizzando il proprio nome utente Windows senza conoscere il nome o il percorso effettivo della home directory.

Fasi

1. Creare un qtree per contenere le home directory dell'utente: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verificare che il qtree utilizzi lo stile di protezione corretto: `volume qtree show`
3. Se qtree non utilizza lo stile di protezione desiderato, modificare lo stile di protezione utilizzando `volume qtree security` comando.
4. Aggiunta di una condivisione home directory: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.

   `-share-name %w` specifica il nome di condivisione della home directory. Il nome della condivisione viene creato in modo dinamico quando ciascun utente si connette alla propria home directory e ha la forma *Windows_User_NAME*.

   > È inoltre possibile utilizzare `%u` variabile per `-share-name` opzione. In questo modo viene creato un percorso di condivisione relativo che utilizza il nome utente UNIX mappato.

   `-path %u` specifica il percorso relativo alla home directory. Il percorso relativo viene creato in modo dinamico quando ciascun utente si connette alla propria home directory ed è del tipo *mapped_UNIX_user_name*.

   > Il valore di questa opzione può contenere anche elementi statici. Ad esempio, `eng/%u`.

   `-share-properties homedirectory\[,...\]` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

5. Verificare che la condivisione abbia la configurazione desiderata utilizzando `vserver cifs share show` comando.
6. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Specifica la SVM abilitata per CIFS su cui aggiungere il percorso di ricerca.

   `-path path` specifica il percorso assoluto della directory per il percorso di ricerca.

7. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.
8. Se l'utente UNIX non esiste, creare l'utente UNIX utilizzando `vserver services unix-user create` comando.

   > Il nome utente UNIX a cui si esegue il mapping del nome utente Windows deve esistere prima di eseguire il mapping dell'utente.

9. Creare una mappatura dei nomi per l'utente Windows e l'utente UNIX utilizzando il seguente comando: `vserver name-mapping create -vserver vserver_name -direction win-unix`

```
-priority integer -pattern windows_user_name -replacement unix_user_name
```

> Se esistono già mappature dei nomi che associano gli utenti Windows agli utenti UNIX, non è necessario eseguire la procedura di mappatura.

Il nome utente di Windows viene associato al nome utente UNIX corrispondente. Quando l'utente Windows si connette alla propria home directory share, si connette a una home directory creata dinamicamente con un nome di condivisione che corrisponde al proprio nome utente Windows senza essere consapevole che il nome della directory corrisponde al nome utente UNIX.

10. Per gli utenti con una home directory, creare una directory corrispondente nel qtree o nel volume designato per contenere home directory.

    Ad esempio, se è stato creato un qtree con il percorso di `/vol/vol1/users` E il nome utente UNIX mappato dell'utente la cui directory si desidera creare è "unixuser1", si crea una directory con il seguente percorso: `/vol/vol1/users/unixuser1`.

    Se è stato creato un volume denominato "home1" montato in `/home1`, creare una directory con il seguente percorso: `/home1/unixuser1`.

11. Verificare che un utente possa connettersi correttamente alla home share mappando un disco o connettendosi utilizzando il percorso UNC.

    Ad esempio, se l'utente mydomain/user1 esegue il mapping all'utente UNIX unixuser1 e desidera connettersi alla directory creata nella fase 10 che si trova su SVM vs1, l'utente 1 si connette utilizzando il percorso UNC `\\vs1\user1`.

Esempio

I comandi dell'esempio seguente creano una configurazione della home directory con le seguenti impostazioni:

- Il nome della condivisione è %w.
- Il percorso relativo della home directory è %u.
- Il percorso di ricerca utilizzato per contenere le home directory, `/home1`, È un volume configurato con lo stile di sicurezza UNIX.
- La configurazione viene creata su SVM vs1.

È possibile utilizzare questo tipo di configurazione della home directory quando gli utenti accedono alle proprie home directory da host Windows o Windows e da host UNIX e l'amministratore del file system utilizza utenti e gruppi basati su UNIX per controllare l'accesso al file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Informazioni correlate

Creazione di una configurazione della home directory utilizzando le variabili %w e %d.

Configurazioni aggiuntive della home directory

Visualizzazione delle informazioni sul percorso home directory di un utente SMB

Configurazioni aggiuntive della home directory

È possibile creare ulteriori configurazioni della home directory utilizzando `%w`, `%d`, e. `%u` variables, che consente di personalizzare la configurazione della home directory in base alle proprie esigenze.

È possibile creare una serie di configurazioni della home directory utilizzando una combinazione di variabili e stringhe statiche nei nomi di condivisione e nei percorsi di ricerca. La seguente tabella fornisce alcuni esempi che illustrano come creare diverse configurazioni della home directory:

Percorsi creati quando `/vol1/user` contiene home directory…	**Comando di condivisione…**
Per creare un percorso di condivisione `\\vs1\~win_username` che indica all'utente `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Per creare un percorso di condivisione `\\vs1\win_username` che indica all'utente `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Per creare un percorso di condivisione `\\vs1\win_username` che indica all'utente `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Per creare un percorso di condivisione `\\vs1\unix_username` che indica all'utente `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Comandi per la gestione dei percorsi di ricerca

Esistono comandi ONTAP specifici per la gestione dei percorsi di ricerca per le configurazioni della home directory SMB. Ad esempio, sono disponibili comandi per aggiungere, rimuovere e visualizzare informazioni sui percorsi di ricerca. È inoltre disponibile un comando per modificare l'ordine dei percorsi di ricerca.

Se si desidera…	**Utilizzare questo comando…**
Aggiungere un percorso di ricerca	`vserver cifs home-directory search-path add`
Visualizzare i percorsi di ricerca	`vserver cifs home-directory search-path show`

Se si desidera…	Utilizzare questo comando…
Modificare l'ordine dei percorsi di ricerca	`vserver cifs home-directory search-path reorder`
Rimuovere un percorso di ricerca	`vserver cifs home-directory search-path remove`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Visualizza informazioni sul percorso home directory di un utente SMB

È possibile visualizzare il percorso home directory di un utente SMB sulla macchina virtuale di storage (SVM), che può essere utilizzato se sono stati configurati più percorsi home directory CIFS e si desidera vedere quale percorso contiene la home directory dell'utente.

Fase

1. Visualizzare il percorso della home directory utilizzando `vserver cifs home-directory show-user` comando.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                  Home Dir Path
   -----------  --------------------  -----------------------
   vs1          user1                 /home/user1
   ```

Informazioni correlate

Gestione dell'accessibilità alle home directory degli utenti

Gestire l'accessibilità alle home directory degli utenti

Per impostazione predefinita, l'accesso alla home directory di un utente è consentito solo a quell'utente. Per le condivisioni in cui il nome dinamico della condivisione è preceduto da una tilde (~), è possibile attivare o disattivare l'accesso alle home directory degli utenti da parte degli amministratori di Windows o di qualsiasi altro utente (accesso pubblico).

Prima di iniziare

Le condivisioni home directory sulla macchina virtuale di storage (SVM) devono essere configurate con nomi di condivisione dinamici preceduti da una tilde (~). I seguenti casi illustrano i requisiti di naming delle condivisioni:

Nome di condivisione della home directory	Esempio di comando per connettersi alla condivisione
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`

Nome di condivisione della home directory	Esempio di comando per connettersi alla condivisione
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Fase

1. Eseguire l'azione appropriata:

Se si desidera attivare o disattivare l'accesso alle home directory degli utenti per…	Immettere quanto segue…
Amministratori di Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}`L'impostazione predefinita è `true.
Qualsiasi utente (accesso pubblico)	a. Impostare il livello di privilegio su Advanced: `set -privilege advanced` b. Abilitare o disabilitare l'accesso: `vserver cifs home-directory modify -vserver *vserver_name* -is-home-dirs-access-for-public-enabled {true

L'esempio seguente consente l'accesso pubblico alle home directory degli utenti:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informazioni correlate

Visualizzazione delle informazioni sul percorso home directory di un utente SMB

Configurare l'accesso del client SMB ai collegamenti simbolici UNIX

In che modo ONTAP consente di fornire l'accesso del client SMB ai collegamenti simbolici UNIX

Un collegamento simbolico è un file creato in un ambiente UNIX che contiene un riferimento a un altro file o directory. Se un client accede a un collegamento simbolico, il client viene reindirizzato al file o alla directory di destinazione a cui si riferisce il collegamento simbolico. ONTAP supporta collegamenti simbolici relativi e assoluti, inclusi i widelink (collegamenti assoluti con destinazioni esterne al file system locale).

ONTAP offre ai client SMB la possibilità di seguire i collegamenti simbolici UNIX configurati sulla SVM. Questa funzione è opzionale ed è possibile configurarla in base alle condivisioni, utilizzando `-symlink-properties` opzione di `vserver cifs share create` con una delle seguenti impostazioni:

- Abilitato con accesso in lettura/scrittura
- Abilitato con accesso di sola lettura
- Disattivato nascondendo i collegamenti simbolici dai client SMB
- Disattivato senza accesso ai collegamenti simbolici dai client SMB

Se si abilitano i collegamenti simbolici su una condivisione, i collegamenti simbolici relativi funzionano senza ulteriori configurazioni.

Se si abilitano i collegamenti simbolici su una condivisione, i collegamenti simbolici assoluti non funzionano immediatamente. È necessario innanzitutto creare un mapping tra il percorso UNIX del collegamento simbolico e il percorso SMB di destinazione. Quando si creano mappature di collegamento simboliche assolute, è possibile specificare se si tratta di un collegamento locale o di un *widelink*; i widelink possono essere collegamenti a file system su altri dispositivi di storage o collegamenti a file system ospitati in SVM separate sullo stesso sistema ONTAP. Quando si crea un widelink, deve includere le informazioni che il client deve seguire; ovvero, si crea un punto di analisi per il client per rilevare il punto di giunzione della directory. Se si crea un collegamento simbolico assoluto a un file o a una directory all'esterno della condivisione locale ma si imposta la località su locale, ONTAP non consente l'accesso alla destinazione.

> Se un client tenta di eliminare un collegamento simbolico locale (assoluto o relativo), viene cancellato solo il collegamento simbolico, non il file o la directory di destinazione. Tuttavia, se un client tenta di eliminare un widelink, potrebbe eliminare il file o la directory di destinazione effettiva a cui si riferisce il widelink. ONTAP non ha il controllo su questo dato che il client può aprire esplicitamente il file o la directory di destinazione all'esterno della SVM ed eliminarlo.

- **Reparse point e servizi file system ONTAP**

  Un *punto di analisi* è un oggetto del file system NTFS che può essere facoltativamente memorizzato sui volumi insieme a un file. I reparse point offrono ai client SMB la possibilità di ricevere servizi di file system avanzati o estesi quando si lavora con volumi di stile NTFS. I punti di analisi sono costituiti da tag standard che identificano il tipo di punto di analisi e il contenuto del punto di analisi che può essere recuperato dai client SMB per un'ulteriore elaborazione da parte del client. Dei tipi di oggetti disponibili per la funzionalità estesa del file system, ONTAP implementa il supporto per i collegamenti simbolici NTFS e i punti di giunzione della directory utilizzando tag di punto di analisi. I client SMB che non sono in grado di comprendere il contenuto di un punto di analisi lo ignorano semplicemente e non forniscono il servizio di file system esteso che il punto di analisi potrebbe abilitare.

- **Directory Junction point e supporto ONTAP per link simbolici**

  I punti di giunzione della directory sono posizioni all'interno di una struttura di directory del file system che possono fare riferimento a posizioni alternative in cui sono memorizzati i file, su un percorso diverso (collegamenti simbolici) o su un dispositivo di storage separato (widelink). I server SMB di ONTAP espongono i punti di giunzione della directory ai client Windows come punti di analisi, consentendo ai client in grado di ottenere contenuti dei punti di analisi da ONTAP quando viene attraversato un punto di giunzione della directory. In questo modo, possono navigare e connettersi a diversi percorsi o dispositivi di storage come se fossero parte dello stesso file system.

- **Abilitazione del supporto widelink utilizzando le opzioni di reparse point**

  Il `-is-use-junctions-as-reparse-points-enabled` L'opzione è attivata per impostazione predefinita in ONTAP 9. Non tutti i client SMB supportano i widelink, pertanto l'opzione per abilitare le informazioni è configurabile in base alla versione per protocollo, consentendo agli amministratori di ospitare client SMB supportati e non supportati. In ONTAP 9.2 e versioni successive, è necessario attivare l'opzione `-widelink-as-reparse-point-versions` Per ogni protocollo client che accede alla

condivisione utilizzando i widelink, l'impostazione predefinita è SMB1. Nelle versioni precedenti, sono stati segnalati solo i widelink a cui si accedeva utilizzando SMB1 predefinito e i sistemi che utilizzavano SMB2 o SMB3 non erano in grado di accedere ai widelink.

Per ulteriori informazioni, consultare la documentazione di Microsoft NTFS.

"Documentazione Microsoft: Analisi dei punti"

Limiti durante la configurazione dei collegamenti simbolici UNIX per l'accesso SMB

È necessario conoscere alcuni limiti durante la configurazione dei collegamenti simbolici UNIX per l'accesso SMB.

Limite	Descrizione
45	Lunghezza massima del nome del server CIFS che è possibile specificare quando si utilizza un FQDN per il nome del server CIFS. In alternativa, è possibile specificare il nome del server CIFS come nome NetBIOS, che può contenere al massimo 15 caratteri.
80	Lunghezza massima del nome di condivisione.
256	Lunghezza massima del percorso UNIX che è possibile specificare quando si crea un collegamento simbolico o si modifica il percorso UNIX di un collegamento simbolico esistente.il percorso UNIX deve iniziare con un "/" (slash) and end with a "/". Le barre iniziali e finali vengono conteggiate come parte del limite di 256 caratteri.
256	Lunghezza massima del percorso CIFS che è possibile specificare quando si crea un collegamento simbolico o si modifica il percorso CIFS di un collegamento simbolico esistente. Il percorso CIFS deve iniziare con un "/" (slash) and end with a "/". Le barre iniziali e finali vengono conteggiate come parte del limite di 256 caratteri.

Informazioni correlate

Creazione di mappature di collegamento simboliche per le condivisioni SMB

Controlla gli annunci DFS automatici in ONTAP con un'opzione del server CIFS

Un'opzione del server CIFS controlla il modo in cui le funzionalità DFS vengono pubblicizzate ai client SMB durante la connessione alle condivisioni. Poiché ONTAP utilizza i riferimenti DFS quando i client accedono a collegamenti simbolici su SMB, è

necessario essere consapevoli dell'impatto della disattivazione o dell'attivazione di questa opzione.

Un'opzione del server CIFS determina se i server CIFS annunciano automaticamente se sono compatibili con DFS per i client SMB. Per impostazione predefinita, questa opzione è attivata e il server CIFS comunica sempre che è compatibile con DFS per i client SMB (anche quando ci si connette a condivisioni in cui l'accesso ai collegamenti simbolici è disattivato). Se si desidera che il server CIFS annunci che è compatibile con DFS solo quando si connettono a condivisioni in cui è attivato l'accesso ai collegamenti simbolici, è possibile disattivare questa opzione.

Tenere presente cosa accade quando questa opzione è disattivata:

- Le configurazioni di condivisione per i collegamenti simbolici sono invariate.
- Se il parametro share è impostato in modo da consentire l'accesso simbolico al collegamento (accesso in lettura/scrittura o accesso in sola lettura), il server CIFS comunica le funzionalità DFS ai client che si connettono a tale condivisione.

  Le connessioni client e l'accesso ai collegamenti simbolici continuano senza interruzioni.

- Se il parametro share è impostato in modo da non consentire l'accesso tramite collegamento simbolico (disattivando l'accesso o se il valore del parametro share è nullo), il server CIFS non segnala le funzionalità DFS ai client che si connettono a tale condivisione.

  Poiché i client hanno memorizzato nella cache le informazioni che il server CIFS è compatibile con DFS e non pubblicizzano più, i client connessi alle condivisioni in cui l'accesso al collegamento simbolico è disattivato potrebbero non essere in grado di accedere a queste condivisioni dopo la disattivazione dell'opzione del server CIFS. Una volta disattivata l'opzione, potrebbe essere necessario riavviare i client connessi a queste condivisioni, eliminando così le informazioni memorizzate nella cache.

Queste modifiche non si applicano alle connessioni SMB 1.0.

Configurare il supporto dei collegamenti simbolici UNIX sulle condivisioni SMB

È possibile configurare il supporto del collegamento simbolico UNIX sulle condivisioni SMB specificando un'impostazione simbolica di proprietà-condivisione del collegamento quando si creano condivisioni SMB o in qualsiasi momento modificando le condivisioni SMB esistenti. Il supporto dei collegamenti simbolici UNIX è attivato per impostazione predefinita. È inoltre possibile disattivare il supporto dei collegamenti simbolici UNIX su una condivisione.

A proposito di questa attività

Quando si configura il supporto del collegamento simbolico UNIX per le condivisioni SMB, è possibile scegliere una delle seguenti impostazioni:

Impostazione	Descrizione
`enable` (OBSOLETO*)	Specifica che i collegamenti simbolici sono abilitati per l'accesso in lettura/scrittura.

Impostazione	Descrizione
`read_only` (OBSOLETO*)	Specifica che i collegamenti simbolici sono abilitati per l'accesso in sola lettura. Questa impostazione non si applica ai widelink. L'accesso a Widelink è sempre in lettura/scrittura.
`hide` (OBSOLETO*)	Specifica che ai client SMB viene impedito di visualizzare i collegamenti simbolici.
`no-strict-security`	Specifica che i client seguono collegamenti simbolici al di fuori dei limiti di condivisione.
`symlinks`	Specifica che i collegamenti simbolici sono attivati localmente per l'accesso in lettura/scrittura. Gli annunci DFS non vengono generati anche se l'opzione CIFS `is-advertise-dfs-enabled` è impostato su `true`. Questa è l'impostazione predefinita.
`symlinks-and-widelinks`	Specifica che sia i collegamenti simbolici locali che i collegamenti widelink per l'accesso in lettura/scrittura. Gli annunci DFS vengono generati sia per symlink locale che per wildelink anche se l'opzione CIFS `is-advertise-dfs-enabled` è impostato su `false`.
`disable`	Specifica che i collegamenti simbolici e i collegamenti widelink sono disattivati. Gli annunci DFS non vengono generati anche se l'opzione CIFS `is-advertise-dfs-enabled` è impostato su `true`.
`""` (nullo, non impostato)	Disattiva i collegamenti simbolici sulla condivisione.
– (non impostato)	Disattiva i collegamenti simbolici sulla condivisione.

*I parametri *enable*, *hide* e *Read-only* sono deprecati e possono essere rimossi in una release futura di ONTAP.

Fasi

1. Configurare o disattivare il supporto dei collegamenti simbolici:

Se è…	Inserisci…
Una nuova condivisione SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only

Se è…	Inserisci…
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Una condivisione SMB esistente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Verificare che la configurazione della condivisione SMB sia corretta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Esempio

Il seguente comando crea una condivisione SMB denominata “data1” con la configurazione del collegamento simbolico UNIX impostata su `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informazioni correlate

Creazione di mappature di collegamento simboliche per le condivisioni SMB

Creare mappature di collegamento simboliche per le condivisioni SMB

È possibile creare mappature di collegamenti simbolici UNIX per le condivisioni SMB. È possibile creare un collegamento simbolico relativo, che si riferisce al file o alla cartella relativa alla cartella principale, oppure creare un collegamento simbolico assoluto, che si riferisce al file o alla cartella utilizzando un percorso assoluto.

A proposito di questa attività

I Widelink non sono accessibili dai client Mac OS X se si utilizza SMB 2.x. Quando un utente tenta di connettersi a una condivisione utilizzando i collegamenti wireless da un client Mac OS X, il tentativo non riesce. Tuttavia, è possibile utilizzare i widelink con i client Mac OS X se si utilizza SMB 1.

Fasi

1. Per creare mappature di collegamento simboliche per le condivisioni SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Specifica il nome della SVM (Storage Virtual Machine).

   `-unix-path path` Specifica il percorso UNIX. Il percorso UNIX deve iniziare con una barra (`/`) e deve terminare con una barra (`/`).

   `-share-name share_name` Specifica il nome della condivisione SMB da mappare.

   `-cifs-path path` Specifica il percorso CIFS. Il percorso CIFS deve iniziare con una barra (`/`) e deve terminare con una barra (`/`).

   `-cifs-server server_name` Specifica il nome del server CIFS. Il nome del server CIFS può essere specificato come nome DNS (ad esempio, mynetwork.cifs.server.com), indirizzo IP o nome NetBIOS. Il nome NetBIOS può essere determinato utilizzando `vserver cifs show` comando. Se questo parametro opzionale non viene specificato, il valore predefinito è il nome NetBIOS del server CIFS locale.

   `-locality local|free|widelink}` specifica se creare un link locale, un link libero o un link simbolico esteso. Un collegamento simbolico locale viene mappato alla condivisione SMB locale. Un collegamento simbolico gratuito può essere mappato in qualsiasi punto del server SMB locale. Un link simbolico esteso si collega a qualsiasi condivisione SMB sulla rete. Se non si specifica questo parametro opzionale, il valore predefinito è `local`.

   `-home-directory true false}` specifica se la condivisione di destinazione è una home directory. Anche se questo parametro è facoltativo, è necessario impostarlo su `true` quando la condivisione di destinazione è configurata come home directory. L'impostazione predefinita è `false`.

Esempio

Il seguente comando crea un mapping di collegamento simbolico sulla SVM denominata vs1. Ha il percorso UNIX `/src/`, Il nome di condivisione SMB "SOURCE", il percorso CIFS `/mycompany/source/`, E l'indirizzo IP del server CIFS 123.123.123.123, ed è un wirdelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informazioni correlate

Configurazione del supporto del collegamento simbolico UNIX sulle condivisioni SMB

Comandi per la gestione delle mappature di collegamenti simbolici

Sono disponibili comandi ONTAP specifici per la gestione delle mappature dei collegamenti simbolici.

Se si desidera…	Utilizzare questo comando…
Creare una mappatura simbolica del collegamento	`vserver cifs symlink create`
Visualizza informazioni sulle mappature dei collegamenti simbolici	`vserver cifs symlink show`
Modificare un mapping di collegamento simbolico	`vserver cifs symlink modify`
Eliminare un mapping di collegamento simbolico	`vserver cifs symlink delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Utilizza BranchCache per memorizzare nella cache i contenuti di condivisione SMB in una filiale

Utilizza BranchCache per memorizzare nella cache i contenuti di condivisione SMB in una panoramica delle filiali

BranchCache è stato sviluppato da Microsoft per consentire il caching dei contenuti sui computer locali dei client che richiedono. L'implementazione ONTAP di BranchCache può ridurre l'utilizzo della WAN (Wide-Area Network) e fornire tempi di risposta dell'accesso migliorati quando gli utenti di una filiale accedono ai contenuti memorizzati su macchine virtuali storage (SVM) utilizzando le PMI.

Se si configura BranchCache, i client Windows BranchCache recuperano prima il contenuto dalla SVM e poi lo memorizzano nella cache su un computer all'interno della filiale. Se un altro client abilitato a BranchCache nella filiale richiede lo stesso contenuto, la SVM prima autentica e autorizza l'utente richiedente. La SVM determina quindi se il contenuto memorizzato nella cache è ancora aggiornato e, in tal caso, invia i metadati del client relativi al contenuto memorizzato nella cache. Il client utilizza quindi i metadati per recuperare il contenuto direttamente dalla cache basata su locale.

Informazioni correlate

Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline

Requisiti e linee guida

Supporto della versione di BranchCache

È necessario conoscere le versioni di BranchCache supportate da ONTAP.

ONTAP supporta BranchCache 1 e BranchCache 2:

- Quando configuri BranchCache sul server SMB per la macchina virtuale di storage (SVM), puoi abilitare BranchCache 1, BranchCache 2 o tutte le versioni.

  Per impostazione predefinita, tutte le versioni sono attivate.

- Se si attiva solo BranchCache 2, i computer client Windows della sede remota devono supportare BranchCache 2.

  Solo i client SMB 3.0 o versioni successive supportano BranchCache 2.

Per ulteriori informazioni sulle versioni di BranchCache, consulta la Microsoft TechNet Library.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti di supporto del protocollo di rete

È necessario conoscere i requisiti del protocollo di rete per l'implementazione di ONTAP BranchCache.

È possibile implementare la funzionalità BranchCache di ONTAP su reti IPv4 e IPv6 utilizzando SMB 2.1 o versioni successive.

Tutti i server CIFS e i computer delle filiali che partecipano all'implementazione di BranchCache devono avere il protocollo SMB 2.1 o successivo abilitato. SMB 2.1 dispone di estensioni di protocollo che consentono a un client di partecipare a un ambiente BranchCache. Questa è la versione minima del protocollo SMB che offre il supporto BranchCache. SMB 2.1 supporta la versione BranchCache versione 1.

Se si desidera utilizzare BranchCache versione 2, SMB 3.0 è la versione minima supportata. Tutti i server CIFS e i computer delle filiali che partecipano a un'implementazione di BranchCache 2 devono avere SMB 3.0 o versioni successive abilitate.

Se si dispone di uffici remoti in cui alcuni client supportano solo SMB 2.1 e alcuni client supportano SMB 3.0, è possibile implementare una configurazione BranchCache sul server CIFS che fornisce il supporto del caching su BranchCache 1 e BranchCache 2.

> Anche se la funzionalità Microsoft BranchCache supporta l'utilizzo dei protocolli HTTP/HTTPS e SMB come protocolli di accesso ai file, ONTAP BranchCache supporta solo l'utilizzo di SMB.

Requisiti di versione per gli host ONTAP e Windows

Gli host Windows di ONTAP e delle filiali devono soddisfare determinati requisiti di versione prima di poter configurare BranchCache.

Prima di configurare BranchCache, è necessario assicurarsi che la versione di ONTAP sul cluster e i client

delle filiali partecipanti supportino SMB 2.1 o versioni successive e la funzionalità BranchCache. Se si configura la modalità cache in hosting, è necessario anche assicurarsi di utilizzare un host supportato per il server della cache.

BranchCache 1 è supportato dalle seguenti versioni di ONTAP e dagli host Windows:

- Server di contenuti: SVM (Storage Virtual Machine) con ONTAP
- Server cache: Windows Server 2008 R2 o Windows Server 2012 o versione successiva
- Peer o client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 o Windows Server 2012 o versione successiva

BranchCache 2 è supportato dalle seguenti versioni di ONTAP e dagli host Windows:

- Server di contenuti: SVM con ONTAP
- Server cache: Windows Server 2012 o versione successiva
- Peer o client: Windows 8 o Windows Server 2012 o versione successiva

Motivi per cui ONTAP invalida gli hash di BranchCache

Comprendere i motivi per cui ONTAP invalida gli hash può essere utile durante la pianificazione della configurazione di BranchCache. Può aiutarti a decidere quale modalità operativa configurare e a scegliere quali condivisioni abilitare BranchCache.

ONTAP deve gestire gli hash BranchCache per garantire la validità degli hash. Se un hash non è valido, ONTAP invalida l'hash e calcola un nuovo hash alla successiva richiesta del contenuto, presupponendo che BranchCache sia ancora abilitato.

ONTAP invalida gli hash per i seguenti motivi:

- La chiave del server viene modificata.

  Se la chiave del server viene modificata, ONTAP invalida tutti gli hash nell'archivio hash.

- Un hash viene svuotato dalla cache perché è stata raggiunta la dimensione massima dell'archivio hash BranchCache.

  Si tratta di un parametro sintonizzabile che può essere modificato per soddisfare i requisiti di business.

- Un file viene modificato tramite accesso SMB o NFS.
- Un file per il quale sono stati calcolati gli hash viene ripristinato utilizzando `snap restore` comando.
- Un volume che contiene condivisioni SMB abilitate a BranchCache viene ripristinato utilizzando `snap restore` comando.

Linee guida per la scelta della posizione dell'archivio hash

Quando configuri BranchCache, scegli dove memorizzare gli hash e le dimensioni dell'archivio hash. La comprensione delle linee guida per la scelta della posizione e delle dimensioni dell'archivio hash può aiutarti a pianificare la configurazione di BranchCache su una SVM abilitata per CIFS.

- È necessario individuare l'archivio hash su un volume in cui sono consentiti gli aggiornamenti atime.

Il tempo di accesso a un file hash viene utilizzato per conservare i file ad accesso frequente nell'archivio hash. Se gli aggiornamenti aTime sono disattivati, viene utilizzata l'ora di creazione. È preferibile utilizzare atime per tenere traccia dei file utilizzati di frequente.

- Non è possibile memorizzare gli hash su file system di sola lettura, ad esempio destinazioni SnapMirror e volumi SnapLock.
- Se viene raggiunta la dimensione massima dell'archivio hash, gli hash più vecchi vengono eliminati per fare spazio ai nuovi hash.

  È possibile aumentare le dimensioni massime dell'archivio hash per ridurre la quantità di hash scaricati dalla cache.

- Se il volume su cui si memorizzano gli hash non è disponibile o è pieno, o se si verifica un problema di comunicazione all'interno del cluster in cui il servizio BranchCache non riesce a recuperare le informazioni sugli hash, i servizi BranchCache non sono disponibili.

  Il volume potrebbe non essere disponibile perché non è in linea o perché l'amministratore dello storage ha specificato una nuova posizione per l'archivio hash.

  Questo non causa problemi di accesso al file. Se l'accesso all'archivio hash viene impedito, ONTAP restituisce un errore definito da Microsoft al client, che fa in modo che il client richieda il file utilizzando la normale richiesta di lettura SMB.

Informazioni correlate

Configurare BranchCache sul server SMB

Modificare la configurazione di BranchCache

Consigli su BranchCache

Prima di configurare BranchCache, è necessario tenere a mente alcuni consigli quando si decide quali condivisioni SMB si desidera attivare il caching BranchCache.

Quando decidi quale modalità operativa utilizzare e su quali condivisioni SMB abilitare BranchCache, devi tenere a mente i seguenti consigli:

- I vantaggi di BranchCache si riducono quando i dati da memorizzare nella cache in remoto cambiano frequentemente.
- I servizi BranchCache sono vantaggiosi per le condivisioni contenenti contenuto di file che viene riutilizzato da più client della sede remota o da contenuto di file a cui un singolo utente remoto accede ripetutamente.
- Considerare l'attivazione del caching per contenuti di sola lettura, come i dati nelle copie Snapshot e nelle destinazioni SnapMirror.

Configurare BranchCache

Panoramica sulla configurazione di BranchCache

Configuri BranchCache sul tuo server SMB utilizzando i comandi ONTAP. Per implementare BranchCache, è necessario configurare anche i client e, facoltativamente, i server di cache ospitati nelle filiali in cui si desidera memorizzare il contenuto nella cache.

Se configuri BranchCache per abilitare il caching su base share-by-share, devi attivare BranchCache sulle

condivisioni SMB per le quali desideri fornire servizi di caching BranchCache.

Requisiti per la configurazione di BranchCache

Una volta soddisfatti alcuni prerequisiti, puoi impostare BranchCache.

Prima di configurare BranchCache sul server CIFS per SVM, è necessario soddisfare i seguenti requisiti:

- ONTAP deve essere installato su tutti i nodi del cluster.
- È necessario disporre della licenza CIFS ed è necessario configurare un server SMB. 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.
- È necessario configurare la connettività di rete IPv4 o IPv6.
- Per BranchCache 1, è necessario attivare SMB 2.1 o versione successiva.
- Per BranchCache 2, SMB 3.0 deve essere attivato e i client Windows remoti devono supportare BranchCache 2.

Configurare BranchCache sul server SMB

Puoi configurare BranchCache per fornire i servizi BranchCache in base alle condivisioni. In alternativa, puoi configurare BranchCache per attivare automaticamente il caching su tutte le condivisioni SMB.

A proposito di questa attività

È possibile configurare BranchCache sulle SVM.

- È possibile creare una configurazione BranchCache all-share se si desidera offrire servizi di caching per tutti i contenuti contenuti all'interno di tutte le condivisioni SMB sul server CIFS.
- È possibile creare una configurazione BranchCache per condivisione se si desidera offrire servizi di caching per il contenuto contenuto all'interno di condivisioni SMB selezionate sul server CIFS.

Durante la configurazione di BranchCache, è necessario specificare i seguenti parametri:

Parametri richiesti	Descrizione
Nome SVM	BranchCache viene configurato per SVM. Specificare su quale SVM CIFS-Enabled si desidera configurare il servizio BranchCache.

Parametri richiesti	Descrizione
Percorso all'archivio hash	Gli hash BranchCache vengono memorizzati in file regolari sul volume SVM. È necessario specificare il percorso di una directory esistente in cui si desidera che ONTAP memorizzi i dati hash.il percorso hash BranchCache deve essere leggibile-scrivibile. I percorsi di sola lettura, come le directory Snapshot, non sono consentiti. È possibile memorizzare i dati hash in un volume che contiene altri dati oppure creare un volume separato per memorizzare i dati hash. Se SVM è un'origine di disaster recovery SVM, il percorso hash non può trovarsi sul volume root. Questo perché il volume root non viene replicato nella destinazione del disaster recovery. Il percorso hash può contenere spazi vuoti e qualsiasi carattere di nome file valido.

È possibile specificare i seguenti parametri:

Parametri opzionali	Descrizione
Versioni supportate	ONTAP supporta BranchCache 1 e 2. È possibile attivare la versione 1, la versione 2 o entrambe le versioni. L'impostazione predefinita prevede l'attivazione di entrambe le versioni.
Dimensione massima dell'archivio hash	È possibile specificare la dimensione da utilizzare per l'archivio dati hash. Se i dati hash superano questo valore, ONTAP elimina gli hash più vecchi per fare spazio agli hash più recenti. La dimensione predefinita per l'archivio hash è 1 GB. Le prestazioni di BranchCache sono più efficienti se gli hash non vengono scartati in modo eccessivamente aggressivo. Se si determina che gli hash vengono eliminati frequentemente perché l'archivio hash è pieno, è possibile aumentare le dimensioni dell'archivio hash modificando la configurazione di BranchCache.

Parametri opzionali	Descrizione
Chiave server	È possibile specificare una chiave server utilizzata dal servizio BranchCache per impedire ai client di rappresentare il server BranchCache. Se non si specifica una chiave server, ne viene generata una in modo casuale quando si crea la configurazione BranchCache. È possibile impostare la chiave del server su un valore specifico in modo che, se più server forniscono dati BranchCache per gli stessi file, i client possano utilizzare gli hash da qualsiasi server utilizzando la stessa chiave del server. Se la chiave del server contiene spazi, racchiudere la chiave del server tra virgolette.
Modalità operativa	Per impostazione predefinita, BranchCache viene attivato in base alle condivisioni. • Per creare una configurazione BranchCache in cui abilitare BranchCache in base alle condivisioni, non è possibile specificare questo parametro facoltativo oppure è possibile specificarlo `per-share`. • Per attivare automaticamente BranchCache su tutte le condivisioni, è necessario impostare la modalità operativa su `all-shares`.

Fasi

1. Abilitazione di SMB 2.1 e 3.0 in base alle esigenze:
   a. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
   b. Controllare le impostazioni SMB SVM configurate per determinare se tutte le versioni richieste di SMB sono abilitate: `vserver cifs options show -vserver vserver_name`
   c. Se necessario, abilitare SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      Il comando abilita sia SMB 2.0 che SMB 2.1.

   d. Se necessario, abilitare SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. Tornare al livello di privilegio admin: `set -privilege admin`
2. Configura BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   Il percorso di storage hash specificato deve esistere e risiedere in un volume gestito da SVM. Il percorso deve trovarsi anche su un volume in lettura/scrittura. Il comando non riesce se il percorso è di sola lettura o non esiste.

Se si desidera utilizzare la stessa chiave server per ulteriori configurazioni SVM BranchCache, registrare il valore immesso per la chiave server. La chiave server non viene visualizzata quando si visualizzano informazioni sulla configurazione di BranchCache.

3. Verificare che la configurazione di BranchCache sia corretta: `vserver cifs branchcache show -vserver vserver_name`

Esempi

I seguenti comandi verificano che SMB 2.1 e 3.0 siano attivati e configurano BranchCache per abilitare automaticamente il caching su tutte le condivisioni SMB su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

I seguenti comandi verificano che SMB 2.1 e 3.0 siano attivati, configurano BranchCache per abilitare il caching per condivisione su SVM vs1 e verificano la configurazione di BranchCache:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informazioni correlate

Requisiti e linee guida: Supporto della versione di BranchCache

Dove trovare informazioni sulla configurazione di BranchCache presso la sede remota

Crea una condivisione SMB abilitata per BranchCache

Abilitare BranchCache su una condivisione SMB esistente

Modificare la configurazione di BranchCache

Panoramica sulla disattivazione di BranchCache sulle condivisioni SMB

Eliminare la configurazione BranchCache sulle SVM

Dove trovare informazioni sulla configurazione di BranchCache presso la sede remota

Dopo aver configurato BranchCache sul server SMB, è necessario installare e configurare BranchCache sui computer client e, facoltativamente, sui server di caching della sede remota. Microsoft fornisce istruzioni per la configurazione di BranchCache presso la sede remota.

Le istruzioni per la configurazione dei client delle filiali e, facoltativamente, dei server di caching per l'utilizzo di BranchCache sono disponibili sul sito Web Microsoft BranchCache.

"Documenti Microsoft BranchCache: Novità"

Configurare le condivisioni SMB abilitate per BranchCache

Panoramica sulla configurazione delle condivisioni SMB abilitate a BranchCache

Dopo aver configurato BranchCache sul server SMB e nella filiale, è possibile attivare BranchCache sulle condivisioni SMB che contengono contenuti che si desidera consentire ai client delle filiali di memorizzare nella cache.

Il caching BranchCache può essere attivato su tutte le condivisioni SMB sul server SMB o su base share-by-share.

- Se abiliti BranchCache su base share-by-share, puoi abilitare BranchCache durante la creazione della condivisione o modificando le condivisioni esistenti.

  Se abiliti il caching su una condivisione SMB esistente, ONTAP inizia a calcolare gli hash e a inviare metadati ai client che richiedono contenuti non appena abiliti BranchCache su quella condivisione.

- Tutti i client che dispongono di una connessione SMB esistente a una condivisione non ricevono il supporto BranchCache se BranchCache viene successivamente abilitato su tale condivisione.

  ONTAP annuncia il supporto di BranchCache per una condivisione al momento della configurazione della sessione SMB. I client che hanno già stabilito sessioni quando BranchCache è abilitato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.

> Se BranchCache su una condivisione SMB viene successivamente disattivato, ONTAP interrompe l'invio dei metadati al client richiedente. Un client che necessita di dati lo recupera direttamente dal server di contenuti (server SMB).

Crea una condivisione SMB abilitata per BranchCache

È possibile attivare BranchCache su una condivisione SMB quando si crea la condivisione impostando `branchcache` condividere la proprietà.

A proposito di questa attività

- Se BranchCache è attivato nella condivisione SMB, la condivisione deve avere la configurazione dei file offline impostata sul caching manuale.

  Questa è l'impostazione predefinita quando si crea una condivisione.

- È inoltre possibile specificare ulteriori parametri di condivisione opzionali quando si crea la condivisione abilitata per BranchCache.
- È possibile impostare `branchcache` Proprietà su una condivisione anche se BranchCache non è configurato e abilitato sulla macchina virtuale di storage (SVM).

  Tuttavia, se si desidera che la condivisione offra contenuti memorizzati nella cache, è necessario configurare e attivare BranchCache sulla SVM.

- Poiché non esistono proprietà di condivisione predefinite applicate alla condivisione quando si utilizza `-share-properties` è necessario specificare tutte le altre proprietà di condivisione che si desidera applicare alla condivisione oltre a `branchcache` condividere la proprietà utilizzando un elenco delimitato da virgole.
- Per ulteriori informazioni, vedere la pagina man di `vserver cifs share create` comando.

Fase

1. Creare una condivisione SMB abilitata per BranchCache:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Verificare che la proprietà di condivisione BranchCache sia impostata sulla condivisione SMB utilizzando `vserver cifs share show` comando.

Esempio

Il seguente comando crea una condivisione SMB abilitata a BranchCache denominata “data” con un percorso di `/data` Su SVM vs1. Per impostazione predefinita, l’impostazione file offline è impostata su `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informazioni correlate

Disattivazione di BranchCache in una singola condivisione SMB

Abilitare BranchCache su una condivisione SMB esistente

È possibile attivare BranchCache su una condivisione SMB esistente aggiungendo `branchcache` condividere la proprietà con l’elenco esistente di proprietà di condivisione.

A proposito di questa attività

- Se BranchCache è attivato nella condivisione SMB, la condivisione deve avere la configurazione dei file offline impostata sul caching manuale.

  Se l'impostazione dei file offline della condivisione esistente non è impostata sul caching manuale, è necessario configurarla modificando la condivisione.

- È possibile impostare `branchcache` Proprietà su una condivisione anche se BranchCache non è configurato e abilitato sulla macchina virtuale di storage (SVM).

  Tuttavia, se si desidera che la condivisione offra contenuti memorizzati nella cache, è necessario configurare e attivare BranchCache sulla SVM.

- Quando si aggiunge `branchcache` la proprietà di condivisione nella condivisione, le impostazioni di condivisione esistenti e le proprietà di condivisione vengono conservate.

  La proprietà di condivisione BranchCache viene aggiunta all'elenco esistente di proprietà di condivisione. Per ulteriori informazioni sull'utilizzo di `vserver cifs share properties add` vedere le pagine man.

Fasi

1. Se necessario, configurare l'impostazione di condivisione file offline per il caching manuale:
   a. Determinare l'impostazione di condivisione dei file offline utilizzando `vserver cifs share show` comando.
   b. Se l'impostazione di condivisione file offline non è impostata su manuale, modificarla nel valore richiesto: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Abilitare BranchCache su una condivisione SMB esistente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verificare che la proprietà di condivisione BranchCache sia impostata sulla condivisione SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Esempio

Il seguente comando abilita BranchCache su una condivisione SMB esistente denominata "data2" con un percorso di `/data2` Su SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               showsnapshot
                               changenotify
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informazioni correlate

Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente

Disattivazione di BranchCache in una singola condivisione SMB

Gestire e monitorare la configurazione di BranchCache

Modificare le configurazioni di BranchCache

È possibile modificare la configurazione del servizio BranchCache sulle SVM, tra cui la modifica del percorso della directory dell'archivio hash, la dimensione massima della directory dell'archivio hash, la modalità operativa e le versioni di BranchCache supportate. È inoltre possibile aumentare le dimensioni del volume che contiene l'archivio hash.

Fasi

1. Eseguire l'azione appropriata:

Se si desidera…	Immettere quanto segue…
Modificare le dimensioni della directory dell'archivio hash	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Aumentare le dimensioni del volume che contiene l'archivio hash	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Se il volume contenente l'archivio hash si riempie, potrebbe essere possibile aumentare le dimensioni del volume. È possibile specificare la nuova dimensione del volume come numero seguito da una designazione dell'unità. Scopri di più "Gestione dei volumi FlexVol"	Modificare il percorso della directory dell'archivio hash

Se si desidera…	Immettere quanto segue…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Se SVM è un'origine di disaster recovery SVM, il percorso hash non può trovarsi sul volume root. Questo perché il volume root non viene replicato nella destinazione del disaster recovery. Il percorso hash di BranchCache può contenere spazi vuoti e qualsiasi carattere valido per il nome del file. Se si modifica il percorso hash, `-flush-hashes` È un parametro obbligatorio che specifica se si desidera che ONTAP svuota gli hash dalla posizione dell'archivio hash originale. È possibile impostare i seguenti valori per `-flush-hashes` parametro: **Se si specifica `true`, ONTAP elimina gli hash nella posizione originale e crea nuovi hash nella nuova posizione man mano che le nuove richieste vengono effettuate dai client abilitati a BranchCache.** Se si specifica `false`, gli hash non vengono spazzati via. + In questo caso, è possibile scegliere di riutilizzare gli hash esistenti in un secondo momento modificando il percorso dell'archivio hash nella posizione originale.
Modificare la modalità operativa	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Quando si modifica la modalità operativa, tenere presente quanto segue: **ONTAP annuncia il supporto di BranchCache per una condivisione quando viene impostata la sessione SMB.** I client che hanno già stabilito sessioni quando BranchCache è abilitato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.
Modificare il supporto della versione di BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Verificare le modifiche alla configurazione utilizzando `vserver cifs branchcache show` comando.

Visualizza informazioni sulle configurazioni di BranchCache

È possibile visualizzare informazioni sulle configurazioni di BranchCache sulle macchine virtuali di storage (SVM), che possono essere utilizzate per verificare una configurazione

o per determinare le impostazioni correnti prima di modificare una configurazione.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare…	Immettere questo comando…
Informazioni riepilogative sulle configurazioni di BranchCache su tutte le SVM	`vserver cifs branchcache show`
Informazioni dettagliate sulla configurazione di una SVM specifica	`vserver cifs branchcache show -vserver` *`vserver_name`*

Esempio

Nell'esempio seguente vengono visualizzate informazioni sulla configurazione di BranchCache su SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                  Vserver: vs1
            Supported BranchCache Versions: enable_all
                        Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Modificare la chiave del server BranchCache

È possibile modificare la chiave del server BranchCache modificando la configurazione BranchCache sulla macchina virtuale di storage (SVM) e specificando una chiave server diversa.

A proposito di questa attività

È possibile impostare la chiave del server su un valore specifico in modo che, se più server forniscono dati BranchCache per gli stessi file, i client possano utilizzare gli hash da qualsiasi server utilizzando la stessa chiave del server.

Quando si modifica la chiave del server, è necessario svuotare anche la cache hash. Dopo aver eseguito il flushing degli hash, ONTAP crea nuovi hash man mano che i client abilitati a BranchCache inoltrano nuove richieste.

Fasi

1. Modificare la chiave del server utilizzando il seguente comando: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   Quando si configura una nuova chiave server, è necessario specificare anche `-flush-hashes` e impostare il valore su `true`.

2. Verificare che la configurazione di BranchCache sia corretta utilizzando `vserver cifs branchcache`

`show` comando.

Esempio

Nell'esempio seguente viene impostata una nuova chiave server che contiene spazi e svuota la cache hash su SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informazioni correlate

Motivi per cui ONTAP invalida gli hash di BranchCache

Pre-calcolare gli hash BranchCache su percorsi specifici

È possibile configurare il servizio BranchCache per pre-calcolare gli hash per un singolo file, per una directory o per tutti i file di una struttura di directory. Questo può essere utile se si desidera calcolare gli hash sui dati in una condivisione abilitata per BranchCache durante le ore non di punta.

A proposito di questa attività

Se si desidera raccogliere un campione di dati prima di visualizzare le statistiche hash, è necessario utilizzare `statistics start` e opzionale `statistics stop` comandi.

- È necessario specificare la SVM (Storage Virtual Machine) e il percorso su cui si desidera pre-calcolare gli hash.
- È inoltre necessario specificare se si desidera che gli hash vengano calcolati in modo ricorsivo.
- Se si desidera che gli hash vengano calcolati in modo ricorrente, il servizio BranchCache attraversa l'intero albero di directory nel percorso specificato e calcola gli hash per ciascun oggetto idoneo.

Fasi

1. Pre-calcolare gli hash come desiderato:

Se si desidera pre-calcolare gli hash su…	Immettere il comando…
Un singolo file o directory	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`

Se si desidera pre-calcolare gli hash su…	Immettere il comando…
In modo ricorrente su tutti i file di una struttura di directory	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verificare che gli hash vengano calcolati utilizzando `statistics` comando:
   a. Visualizzare le statistiche per `hashd` Oggetto sull'istanza SVM desiderata: `statistics show -object hashd -instance vserver_name`
   b. Verificare che il numero di hash creati aumenti ripetendo il comando.

Esempi

Nell'esempio seguente vengono creati gli hash sul percorso `/data` E su tutti i file e sottodirectory contenuti su SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Informazioni correlate

"Configurazione del monitoraggio delle performance"

Scarica gli hash dall'archivio hash BranchCache di SVM

È possibile scaricare tutti gli hash memorizzati nella cache dall'archivio hash BranchCache sulla macchina virtuale di storage (SVM). Ciò può essere utile se hai modificato la configurazione BranchCache della filiale. Ad esempio, se di recente è stata riconfigurata la modalità di caching dalla modalità di caching distribuito alla modalità di caching in hosting, si consiglia di svuotare l'archivio hash.

A proposito di questa attività

Dopo aver eseguito il flushing degli hash, ONTAP crea nuovi hash man mano che i client abilitati a BranchCache inoltrano nuove richieste.

Fase

1. Eliminare gli hash dall'archivio hash di BranchCache: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Visualizzare le statistiche di BranchCache

È possibile visualizzare le statistiche di BranchCache, tra l'altro, per identificare le prestazioni del caching, determinare se la configurazione fornisce contenuti memorizzati nella cache ai client e determinare se i file hash sono stati eliminati per fare spazio a dati hash più recenti.

A proposito di questa attività

Il `hashd` Oggetto Statistic contiene contatori che forniscono informazioni statistiche sugli hash BranchCache. Il `cifs` Oggetto Statistic contiene contatori che forniscono informazioni statistiche sull'attività correlata a BranchCache. È possibile raccogliere e visualizzare informazioni su questi oggetti a livello di privilegi avanzati.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`

   ```
   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
   ```

2. Visualizzare i contatori relativi a BranchCache utilizzando `statistics catalog counter show` comando.

   Per ulteriori informazioni sui contatori delle statistiche, vedere la pagina man di questo comando.

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
   ```

```
    Counter                     Description
    ---------------------------
---------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
---------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
```

```
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
    ....Output truncated....
```

3. Raccogliere le statistiche relative a BranchCache utilizzando `statistics start` e. `statistics stop` comandi.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. Visualizzare le statistiche BranchCache raccolte utilizzando `statistics show` comando.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. Tornare al livello di privilegio admin: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Informazioni correlate

Visualizzazione delle statistiche

"Configurazione del monitoraggio delle performance"

Supporto per gli oggetti Criteri di gruppo BranchCache

BranchCache di ONTAP fornisce il supporto per gli oggetti Criteri di gruppo BranchCache, che consentono la gestione centralizzata di alcuni parametri di

configurazione BranchCache. Per BranchCache vengono utilizzati due GPO, la pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache e il supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache.

- **Pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache**

  La pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde a. `-operating-mode` parametro. Quando si verificano gli aggiornamenti dei GPO, questo valore viene applicato agli oggetti SVM (Storage Virtual Machine) contenuti nell'unità organizzativa (OU) a cui si applicano i criteri di gruppo.

- **Supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache**

  Il supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde a. `-versions` parametro. Quando si verificano gli aggiornamenti dei GPO, questo valore viene applicato agli oggetti SVM contenuti nell'unità organizzativa a cui si applicano i criteri di gruppo.

Informazioni correlate

Applicazione di oggetti Criteri di gruppo ai server CIFS

Visualizza informazioni sugli oggetti Criteri di gruppo BranchCache

È possibile visualizzare informazioni sulla configurazione dell'oggetto Criteri di gruppo (GPO) del server CIFS per determinare se gli oggetti Criteri di gruppo BranchCache sono definiti per il dominio a cui appartiene il server CIFS e, in caso affermativo, quali sono le impostazioni consentite. È inoltre possibile determinare se le impostazioni dell'oggetto Criteri di gruppo BranchCache sono applicate al server CIFS.

A proposito di questa attività

Anche se un'impostazione GPO è definita all'interno del dominio a cui appartiene il server CIFS, non viene necessariamente applicata all'unità organizzativa (OU) contenente la SVM (Storage Virtual Machine) abilitata per CIFS. Le impostazioni dell'oggetto Criteri di gruppo applicato sono il sottoinsieme di tutti gli oggetti Criteri di gruppo definiti che vengono applicati alla SVM abilitata per CIFS. Le impostazioni BranchCache applicate tramite gli oggetti GPO sovrascrivono le impostazioni applicate tramite l'interfaccia CLI.

Fasi

1. Visualizzare l'impostazione dell'oggetto Criteri di gruppo BranchCache definita per il dominio Active Directory utilizzando `vserver cifs group-policy show-defined` comando.

> In questo esempio non vengono visualizzati tutti i campi di output disponibili per il comando. L'output viene troncato.

```
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
  [...]

    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
  [...]
```

2. Visualizzare l'impostazione dell'oggetto Criteri di gruppo BranchCache applicata al server CIFS utilizzando `vserver cifs group-policy show-applied` comando. ``

> In questo esempio non vengono visualizzati tutti i campi di output disponibili per il comando. L'output viene troncato.

```
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: version1
  [...]

    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: version1
 [...]
```

Informazioni correlate

Attivazione o disattivazione del supporto GPO su un server CIFS

Disattiva BranchCache sulle condivisioni SMB

Panoramica sulla disattivazione di BranchCache sulle condivisioni SMB

Se non si desidera fornire servizi di caching BranchCache su determinate condivisioni SMB, ma si desidera fornire servizi di caching su tali condivisioni in un secondo momento, è possibile disattivare BranchCache in base alla condivisione. Se BranchCache è configurato per offrire il caching su tutte le condivisioni, ma si desidera disattivare temporaneamente tutti i servizi di caching, è possibile modificare la configurazione di BranchCache per interrompere il caching automatico su tutte le condivisioni.

Se BranchCache su una condivisione SMB viene successivamente disattivato dopo la prima attivazione, ONTAP interrompe l'invio dei metadati al client richiedente. Un client che necessita di dati lo recupera

direttamente dal server di contenuti (server CIFS sulla macchina virtuale di storage (SVM)).

Informazioni correlate

Configurazione delle condivisioni SMB abilitate per BranchCache

Disattiva BranchCache su una singola condivisione SMB

Se non si desidera offrire servizi di caching su determinate condivisioni che in precedenza offrivano contenuti memorizzati nella cache, è possibile disattivare BranchCache su una condivisione SMB esistente.

Fase

1. Immettere il seguente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   La proprietà di condivisione BranchCache viene rimossa. Le altre proprietà di condivisione applicate rimangono attive.

Esempio

Il seguente comando disattiva BranchCache in una condivisione SMB esistente denominata “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Arrestare il caching automatico su tutte le condivisioni SMB

Se la configurazione di BranchCache abilita automaticamente il caching su tutte le condivisioni SMB su ciascuna macchina virtuale di storage (SVM), puoi modificare la configurazione di BranchCache per interrompere automaticamente il caching del contenuto per tutte le condivisioni SMB.

A proposito di questa attività

Per interrompere il caching automatico su tutte le condivisioni SMB, si cambia la modalità operativa BranchCache in caching per-share.

Fasi

1. Configurare BranchCache per interrompere il caching automatico su tutte le condivisioni SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verificare che la configurazione di BranchCache sia corretta: `vserver cifs branchcache show -vserver vserver_name`

Esempio

Il seguente comando modifica la configurazione di BranchCache su storage virtual machine (SVM, precedentemente noto come Vserver) vs1 per interrompere il caching automatico su tutte le condivisioni SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Disattivare o attivare BranchCache sulla SVM

Cosa accade quando si disattiva o si riattiva BranchCache sul server CIFS

Se in precedenza è stato configurato BranchCache ma non si desidera che i client delle filiali utilizzino il contenuto memorizzato nella cache, è possibile disattivare il caching sul server CIFS. Devi essere consapevole di ciò che accade quando disattivi BranchCache.

Quando disattivi BranchCache, ONTAP non calcola più gli hash o invia i metadati al client richiedente. Tuttavia, non si verifica alcuna interruzione nell'accesso ai file. In seguito, quando i client abilitati a BranchCache richiedono informazioni sui metadati per il contenuto a cui desiderano accedere, ONTAP risponde con un errore definito da Microsoft, che fa in modo che il client invii una seconda richiesta, richiedendo il contenuto effettivo. In risposta alla richiesta di contenuto, il server CIFS invia il contenuto effettivo memorizzato sulla macchina virtuale di storage (SVM).

Una volta disattivato BranchCache sul server CIFS, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache. Per accedere ai dati sulle nuove connessioni SMB, i client eseguono le normali richieste SMB in lettura.

Puoi riabilitare BranchCache sul server CIFS in qualsiasi momento.

- Poiché l'archivio hash non viene cancellato quando disattivi BranchCache, ONTAP può utilizzare gli hash memorizzati quando risponde alle richieste hash dopo la riabilitazione di BranchCache, a condizione che l'hash richiesto sia ancora valido.
- Tutti i client che hanno effettuato connessioni SMB alle condivisioni abilitate a BranchCache durante il periodo in cui BranchCache è stato disattivato non ottengono il supporto BranchCache se BranchCache viene successivamente riabilitato.

  Questo perché ONTAP pubblicizza il supporto di BranchCache per una condivisione al momento della configurazione della sessione SMB. I client che hanno stabilito sessioni per le condivisioni abilitate a BranchCache mentre BranchCache è stato disattivato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.

> Se non si desidera salvare l'archivio hash dopo la disattivazione di BranchCache su un server CIFS, è possibile eliminarlo manualmente. Se riabiliti BranchCache, devi assicurarti che la directory dell'archivio hash esista. Una volta riabilitato BranchCache, le condivisioni abilitate a BranchCache pubblicizzano le funzionalità di BranchCache. ONTAP crea nuovi hash man mano che le nuove richieste vengono effettuate dai client abilitati a BranchCache.

Disattiva o attiva BranchCache

È possibile disattivare BranchCache sulla macchina virtuale di storage (SVM) modificando la modalità operativa BranchCache su `disabled`. Puoi abilitare BranchCache in qualsiasi momento modificando la modalità operativa per offrire servizi BranchCache per share o automaticamente per tutte le condivisioni.

Fasi

1. Eseguire il comando appropriato:

Se si desidera…	Quindi, immettere quanto segue…
Disattiva BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Attiva BranchCache per share	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Abilitare BranchCache per tutte le condivisioni	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Verificare che la modalità operativa BranchCache sia configurata con l'impostazione desiderata: `vserver cifs branchcache show -vserver vserver_name`

Esempio

Nell'esempio seguente viene disattivata BranchCache su SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Eliminare la configurazione BranchCache sulle SVM

Cosa succede quando elimini la configurazione BranchCache

Se in precedenza è stato configurato BranchCache ma non si desidera che la macchina virtuale di storage (SVM) continui a fornire contenuto memorizzato nella cache, è possibile eliminare la configurazione BranchCache sul server CIFS. È necessario essere consapevoli di cosa accade quando si elimina la configurazione.

Quando si elimina la configurazione, ONTAP rimuove dal cluster le informazioni di configurazione relative a tale SVM e interrompe il servizio BranchCache. È possibile scegliere se ONTAP deve eliminare l'archivio hash sulla SVM.

L'eliminazione della configurazione BranchCache non interrompe l'accesso dei client abilitati a BranchCache. Successivamente, quando i client abilitati a BranchCache richiedono informazioni sui metadati sulle connessioni SMB esistenti per il contenuto già memorizzato nella cache, ONTAP risponde con un errore definito da Microsoft, che fa in modo che il client invii una seconda richiesta, richiedendo il contenuto effettivo. In risposta alla richiesta di contenuto, il server CIFS invia il contenuto effettivo memorizzato nella SVM

Una volta eliminata la configurazione di BranchCache, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache. Per accedere a contenuti che non sono stati precedentemente memorizzati nella cache utilizzando nuove connessioni SMB, i client eseguono normali richieste SMB in lettura.

Eliminare la configurazione BranchCache

Il comando utilizzato per eliminare il servizio BranchCache sulla macchina virtuale di storage (SVM) varia a seconda che si desideri eliminare o mantenere gli hash esistenti.

Fase

1. Eseguire il comando appropriato:

Se si desidera…	Quindi, immettere quanto segue…
Eliminare la configurazione BranchCache ed eliminare gli hash esistenti	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Eliminare la configurazione BranchCache ma mantenere gli hash esistenti	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Esempio

Nell'esempio riportato di seguito viene eliminata la configurazione BranchCache su SVM vs1 e vengono eliminati tutti gli hash esistenti:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Cosa succede a BranchCache quando si esegue il ripristino

È importante comprendere cosa accade quando si ripristina ONTAP a una release che non supporta BranchCache.

- Quando si torna a una versione di ONTAP che non supporta BranchCache, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache ai client abilitati a BranchCache; pertanto, i client non richiedono informazioni hash.

  Richiedono invece il contenuto effettivo utilizzando le normali richieste di lettura SMB. In risposta alla richiesta di contenuto, il server SMB invia il contenuto effettivo memorizzato sulla macchina virtuale di storage (SVM).

- Quando un nodo che ospita un archivio hash viene ripristinato a una release che non supporta BranchCache, l'amministratore dello storage deve ripristinare manualmente la configurazione BranchCache utilizzando un comando stampato durante il revert.

  Questo comando elimina la configurazione e gli hash di BranchCache.

  Una volta completato il ripristino, l'amministratore dello storage può eliminare manualmente la directory che conteneva l'archivio hash, se lo si desidera.

Informazioni correlate

Eliminazione della configurazione BranchCache sulle SVM

Migliorare le performance di copia remota di Microsoft

Migliora la panoramica delle performance della copia remota di Microsoft

Microsoft Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento diretto dei dati all'interno o tra dispositivi di storage compatibili senza

trasferire i dati attraverso il computer host.

ONTAP supporta ODX per i protocolli SMB e SAN. L'origine può essere un server CIFS o un LUN e la destinazione può essere un server CIFS o un LUN.

Nei trasferimenti di file non ODX, i dati vengono letti dall'origine e trasferiti attraverso la rete al computer client. Il computer client trasferisce i dati di nuovo sulla rete alla destinazione. In sintesi, il computer client legge i dati dall'origine e li scrive nella destinazione. Con i trasferimenti di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione.

Poiché le copie ODX offloaded vengono eseguite direttamente tra lo storage di origine e di destinazione, le performance sono notevolmente migliorate. I benefici delle performance ottenuti includono tempi di copia più rapidi tra origine e destinazione, utilizzo ridotto delle risorse (CPU, memoria) sul client e utilizzo ridotto della larghezza di banda i/o di rete.

Per gli ambienti SMB, questa funzionalità è disponibile solo quando sia il client che il server di storage supportano SMB 3.0 e la funzionalità ODX. Per gli ambienti SAN, questa funzionalità è disponibile solo quando sia il client che il server di storage supportano la funzionalità ODX. I computer client che supportano ODX e che hanno ODX abilitato automaticamente e in modo trasparente utilizzano il trasferimento di file offload durante lo spostamento o la copia dei file. ODX viene utilizzato indipendentemente dal fatto che si trascinino i file tramite Esplora risorse o si utilizzino comandi di copia dei file dalla riga di comando o che un'applicazione client avvii richieste di copia dei file.

Informazioni correlate

Migliorare i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con Auto Location

"Configurazione SMB per Microsoft Hyper-V e SQL Server"

Come funziona ODX

L'offload delle copie di ODX utilizza un meccanismo basato su token per la lettura e la scrittura dei dati all'interno o tra server CIFS abilitati per ODX. Invece di instradare i dati attraverso l'host, il server CIFS invia al client un piccolo token, che rappresenta i dati. Il client ODX presenta tale token al server di destinazione, che può quindi trasferire i dati rappresentati da tale token dall'origine alla destinazione.

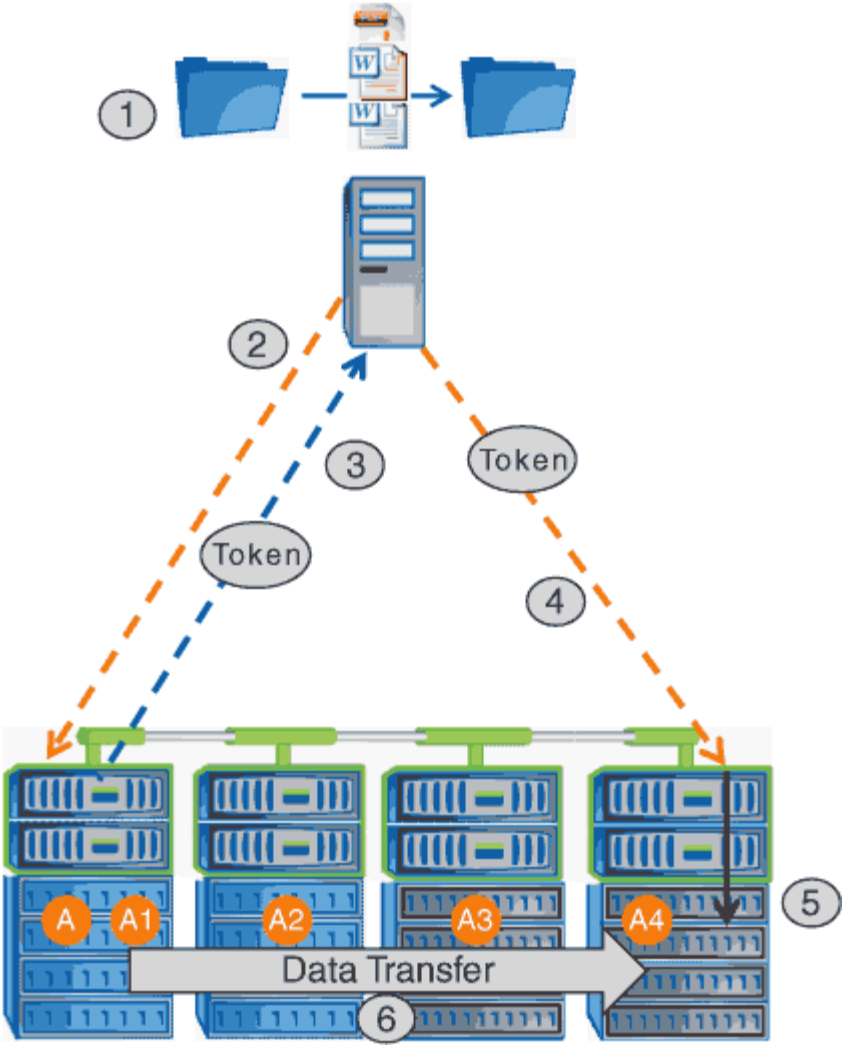
Quando un client ODX rileva che il server CIFS è compatibile con ODX, apre il file di origine e richiede un token dal server CIFS. Dopo aver aperto il file di destinazione, il client utilizza il token per indicare al server di copiare i dati direttamente dall'origine alla destinazione.

> L'origine e la destinazione possono trovarsi sulla stessa SVM (Storage Virtual Machine) o su SVM diverse, a seconda dell'ambito dell'operazione di copia.

Il token funge da rappresentazione point-in-time dei dati. Ad esempio, quando si copiano i dati tra posizioni di storage, un token che rappresenta un segmento di dati viene restituito al client richiedente, che il client copia nella destinazione, eliminando così la necessità di copiare i dati sottostanti attraverso il client.

ONTAP supporta token che rappresentano 8 MB di dati. Le copie ODX superiori a 8 MB vengono eseguite utilizzando più token, ciascuno dei quali rappresenta 8 MB di dati.

La seguente figura illustra i passaggi relativi a un'operazione di copia ODX:



1. Un utente copia o sposta un file utilizzando Esplora risorse, un'interfaccia della riga di comando o come parte di una migrazione di macchine virtuali, oppure un'applicazione avvia copie o spostamenti di file.
2. Il client compatibile con ODX traduce automaticamente questa richiesta di trasferimento in una richiesta ODX.

   La richiesta ODX inviata al server CIFS contiene una richiesta per un token.

3. Se ODX è attivato sul server CIFS e la connessione avviene tramite SMB 3.0, il server CIFS genera un token, che rappresenta una rappresentazione logica dei dati sull'origine.
4. Il client riceve un token che rappresenta i dati e li invia con la richiesta di scrittura al server CIFS di destinazione.

   Si tratta degli unici dati copiati in rete dall'origine al client e quindi dal client alla destinazione.

5. Il token viene consegnato al sottosistema di storage.
6. La SVM esegue internamente la copia o lo spostamento.

   Se il file che viene copiato o spostato è più grande di 8 MB, sono necessari più token per eseguire la copia. I passi da 2 a 6 vengono eseguiti in base alle necessità per completare la copia.

> Se si verifica un errore con la copia ODX scaricata, l'operazione di copia o spostamento torna alle letture e scritture tradizionali per l'operazione di copia o spostamento. Allo stesso modo, se il server CIFS di destinazione non supporta ODX o ODX è disattivato, l'operazione di copia o spostamento ritorna alle operazioni di lettura e scrittura tradizionali per l'operazione di copia o spostamento.

Requisiti per l'utilizzo di ODX

Prima di poter utilizzare ODX per gli offload delle copie con la vostra macchina virtuale di storage (SVM), dovete essere consapevoli di alcuni requisiti.

Requisiti di versione di ONTAP

Le release di ONTAP supportano ODX per gli offload delle copie.

Requisiti di versione SMB

- ONTAP supporta ODX con SMB 3.0 e versioni successive.
- SMB 3.0 deve essere abilitato sul server CIFS prima di poter abilitare ODX:
  - L'abilitazione di ODX abilita anche SMB 3.0, se non è già abilitato.
  - La disattivazione di SMB 3.0 disattiva anche ODX.

Requisiti di server e client Windows

Prima di poter utilizzare ODX per gli offload delle copie, il client Windows deve supportare questa funzionalità.

Il "Matrice di interoperabilità NetApp"Contiene le informazioni più recenti sui client Windows supportati.

Requisiti di volume

- I volumi di origine devono essere di almeno 1.25 GB.
- Se si utilizzano volumi compressi, il tipo di compressione deve essere adattivo e sono supportate solo le dimensioni del gruppo di compressione 8K.

  Il tipo di compressione secondario non è supportato.

Linee guida per l'utilizzo di ODX

Prima di poter utilizzare ODX per l'offload delle copie, è necessario conoscere le linee guida. Ad esempio, è necessario sapere quali tipi di volumi è possibile utilizzare ODX e comprendere le considerazioni relative a ODX all'interno del cluster e tra cluster.

Linee guida sui volumi

- Non è possibile utilizzare ODX per l'offload delle copie con le seguenti configurazioni di volume:
  - Le dimensioni del volume di origine sono inferiori a 1.25 GB

    Per utilizzare ODX, le dimensioni del volume devono essere pari o superiori a 1.25 GB.

  - Volumi di sola lettura

ODX non viene utilizzato per file e cartelle residenti in mirror di condivisione del carico o in volumi di destinazione SnapMirror o SnapVault.

  - Se il volume di origine non viene deduplicato

- Le copie ODX sono supportate solo per le copie all'interno del cluster.

  Non è possibile utilizzare ODX per copiare file o cartelle in un volume in un altro cluster.

Altre linee guida

- Negli ambienti SMB, per utilizzare ODX per l'offload delle copie, i file devono essere di 256 kb o superiore.

  I file più piccoli vengono trasferiti utilizzando un'operazione di copia tradizionale.

- L'offload delle copie di ODX utilizza la deduplica come parte del processo di copia.

  Se non si desidera che la deduplica avvenga sui volumi SVM durante la copia o lo spostamento dei dati, è necessario disattivare l'offload delle copie ODX su tale SVM.

- L'applicazione che esegue il trasferimento dei dati deve essere scritta per supportare ODX.

  Le operazioni applicative che supportano ODX includono:

  - Operazioni di gestione di Hyper-V, come la creazione e la conversione di dischi rigidi virtuali (VHD), la gestione di copie Snapshot e la copia di file tra macchine virtuali
  - Operazioni di Esplora risorse
  - Comandi di copia di Windows PowerShell
  - Comandi di copia del prompt dei comandi di Windows

    Robocopy al prompt dei comandi di Windows supporta ODX.

    > Le applicazioni devono essere in esecuzione su server o client Windows che supportano ODX.

  + Per ulteriori informazioni sulle applicazioni ODX supportate su server e client Windows, consultare la Microsoft TechNet Library.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Casi di utilizzo per ODX

È necessario conoscere i casi di utilizzo per l'utilizzo di ODX su SVM in modo da poter determinare in quali circostanze ODX offre vantaggi in termini di performance.

I server e i client Windows che supportano ODX utilizzano l'offload delle copie come metodo predefinito per copiare i dati tra server remoti. Se il server o il client Windows non supporta ODX o l'offload delle copie ODX non riesce in qualsiasi momento, l'operazione di copia o spostamento ritorna alle tradizionali operazioni di lettura e scrittura per l'operazione di copia o spostamento.

I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti ODX:

- Intra-volume

  I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Intervolume, stesso nodo, stessa SVM

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

- Tra cluster

  Le LUN di origine e di destinazione si trovano su volumi diversi che si trovano su nodi diversi tra cluster. Questo è supportato solo per SAN e non funziona per CIFS.

Esistono alcuni casi di utilizzo speciali aggiuntivi:

- Con l'implementazione di ONTAP ODX, è possibile utilizzare ODX per copiare i file tra le condivisioni SMB e le unità virtuali FC o iSCSI collegate.

  È possibile utilizzare Esplora risorse, la CLI di Windows o PowerShell, Hyper-V o altre applicazioni che supportano ODX per copiare o spostare i file senza problemi utilizzando l'offload delle copie ODX tra le condivisioni SMB e le LUN connesse, a condizione che le condivisioni SMB e le LUN si trovino sullo stesso cluster.

- Hyper-V offre alcuni casi di utilizzo aggiuntivi per l'offload delle copie ODX:

  - È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

    Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

  - Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
  - L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.

> Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

Attivare o disattivare ODX

È possibile attivare o disattivare ODX su macchine virtuali storage (SVM). L'impostazione predefinita prevede l'attivazione del supporto per l'offload delle copie ODX se è attivato anche SMB 3.0.

Prima di iniziare

SMB 3.0 deve essere attivato.

A proposito di questa attività

Se si disattiva SMB 3.0, ONTAP disattiva anche SMB ODX. Se si riattiva SMB 3.0, è necessario riabilitare manualmente SMB ODX.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che l'offload delle copie ODX sia…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Disattivato	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Tornare al livello di privilegio admin: `set -privilege admin`

Esempio

Il seguente esempio consente l'offload delle copie ODX su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informazioni correlate

Opzioni server SMB disponibili

Migliora i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con Auto Location

Migliora i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con panoramica della posizione automatica

Auto Location utilizza i riferimenti automatici ai nodi SMB per aumentare le performance dei client SMB sulle macchine virtuali di storage (SVM). I riferimenti automatici ai nodi reindirizzano automaticamente il client richiedente a una LIF sul nodo SVM che ospita il volume in cui risiedono i dati, il che può portare a tempi di risposta del client migliorati.

Quando un client SMB si connette a una condivisione SMB ospitata sulla SVM, potrebbe connettersi utilizzando una LIF che si trova su un nodo che non possiede i dati richiesti. Il nodo a cui è connesso il client accede ai dati di proprietà di un altro nodo utilizzando la rete del cluster. Se la connessione SMB utilizza un LIF situato sul nodo contenente i dati richiesti, il client può ottenere tempi di risposta più rapidi:

- ONTAP fornisce questa funzionalità utilizzando i riferimenti DFS Microsoft per informare i client SMB che un file o una cartella richiesta nello spazio dei nomi è ospitato altrove.

  Un nodo fa un riferimento quando determina che esiste una LIF SVM sul nodo contenente i dati.

- I riferimenti automatici dei nodi sono supportati per gli indirizzi IP LIF IPv4 e IPv6.
- I riferimenti vengono effettuati in base alla posizione della directory principale della condivisione attraverso la quale il client è connesso.
- Il riferimento si verifica durante la negoziazione SMB.

  Il riferimento viene fatto prima che venga stabilita la connessione. Dopo che ONTAP fa riferimento al nodo di destinazione, la connessione viene stabilita e il client accede ai dati attraverso il percorso LIF indicato da quel punto in poi. In questo modo, i client possono accedere più rapidamente ai dati ed evitare ulteriori comunicazioni del cluster.

> Se una condivisione si estende su più punti di giunzione e alcune delle giunzioni si riferiscono a volumi contenuti su altri nodi, i dati all'interno della condivisione vengono distribuiti su più nodi. Poiché ONTAP fornisce riferimenti locali alla directory principale della condivisione, ONTAP deve utilizzare la rete del cluster per recuperare i dati contenuti in questi volumi non locali. Con questo tipo di architettura dello spazio dei nomi, i riferimenti automatici ai nodi potrebbero non fornire benefici significativi in termini di performance.

Se il nodo che ospita i dati non dispone di una LIF disponibile, ONTAP stabilisce la connessione utilizzando la LIF scelta dal client. Dopo l'apertura di un file da parte di un client SMB, il file continua ad accedere attraverso la stessa connessione a cui si fa riferimento.

Se, per qualsiasi motivo, il server CIFS non è in grado di fare riferimento, il servizio SMB non viene disgresso. La connessione SMB viene stabilita come se i riferimenti automatici al nodo non fossero abilitati.

Informazioni correlate

Miglioramento delle performance di copia remota di Microsoft

Requisiti e linee guida per l'utilizzo dei riferimenti automatici ai nodi

Prima di poter utilizzare i riferimenti automatici ai nodi SMB, noti anche come *autolocation*, è necessario conoscere alcuni requisiti, incluse le versioni di ONTAP che supportano la funzione. È inoltre necessario conoscere le versioni del protocollo SMB supportate e alcune altre linee guida speciali.

Versione di ONTAP e requisiti di licenza

- Tutti i nodi del cluster devono eseguire una versione di ONTAP che supporti i riferimenti automatici dei nodi.
- Per utilizzare l'autolocation, i Widelink devono essere abilitati su una condivisione SMB.
- CIFS deve essere concesso in licenza e un server SMB deve esistere sulle SVM. 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 i riferimenti automatici dei nodi su tutte le versioni di SMB.

Requisiti del client SMB

Tutti i client Microsoft supportati da ONTAP supportano i riferimenti automatici dei nodi SMB.

La matrice di interoperabilità contiene le informazioni più recenti sui client Windows supportati da ONTAP.

"Tool di matrice di interoperabilità NetApp"

Requisiti Data LIF

Se si desidera utilizzare una LIF di dati come potenziale riferimento per i client SMB, è necessario creare LIF di dati con NFS e CIFS abilitati.

I riferimenti automatici dei nodi possono non funzionare se il nodo di destinazione contiene LIF di dati che sono abilitati solo per il protocollo NFS o abilitati solo per il protocollo SMB.

Se questo requisito non viene soddisfatto, l'accesso ai dati non viene compromesso. Il client SMB esegue la mappatura della condivisione utilizzando la LIF originale utilizzata dal client per connettersi alla SVM.

Requisiti di autenticazione NTLM quando si effettua una connessione SMB di riferimento

L'autenticazione NTLM deve essere consentita nel dominio contenente il server CIFS e nei domini contenenti client che desiderano utilizzare i riferimenti automatici ai nodi.

Quando si fa un riferimento, il server SMB fa riferimento a un indirizzo IP per il client Windows. Poiché l'autenticazione NTLM viene utilizzata quando si effettua una connessione utilizzando un indirizzo IP, l'autenticazione Kerberos non viene eseguita per le connessioni di riferimento.

Questo accade perché il client Windows non può creare il nome principale del servizio utilizzato da Kerberos (che è del formato `service/NetBIOS name` e. `service/FQDN`), il che significa che il client non può richiedere un ticket Kerberos al servizio.

Linee guida per l'utilizzo dei riferimenti automatici ai nodi con la funzione home directory

Quando le condivisioni sono configurate con la proprietà di condivisione della home directory attivata, possono essere configurati uno o più percorsi di ricerca della home directory per una configurazione della home directory. I percorsi di ricerca possono puntare ai volumi contenuti in ciascun nodo contenente volumi SVM. I client ricevono un riferimento e, se è disponibile un LIF di dati locale attivo, si connettono attraverso un LIF di riferimento locale alla home directory dell'utente domestico.

Esistono linee guida quando i client SMB 1.0 accedono alle home directory dinamiche con i riferimenti automatici dei nodi abilitati. Questo perché i client SMB 1.0 richiedono il riferimento automatico al nodo prima dell'autenticazione, ovvero prima che il server SMB abbia il nome dell'utente. Tuttavia, l'accesso alla home directory SMB funziona correttamente per i client SMB 1.0 se le seguenti affermazioni sono vere:

- Le home directory SMB sono configurate in modo da utilizzare nomi semplici, come "%w" (nome utente Windows) o "%u" (nome utente UNIX mappato) e non nomi di stile dominio, come "`%d%w `" (nome-dominio nome-utente).
- Quando si creano condivisioni della home directory, i nomi delle condivisioni della home directory CIFS vengono configurati con variabili ("%w" o "%u") e non con nomi statici, ad esempio "HOME".

Per i client SMB 2.x e SMB 3.0, non esistono linee guida speciali per l'accesso alle home directory mediante riferimenti automatici ai nodi.

Linee guida per la disattivazione dei riferimenti automatici dei nodi sui server CIFS con connessioni referenziate esistenti

Se si disattivano i riferimenti automatici ai nodi dopo l'attivazione dell'opzione, i client attualmente connessi a una LIF referenziata mantengono la connessione referenziata. Poiché ONTAP utilizza i riferimenti DFS come meccanismo per i riferimenti automatici ai nodi SMB, i client possono anche riconnettersi al file LIF indicato dopo aver disattivato l'opzione fino al timeout del riferimento DFS memorizzato nella cache del client per la connessione a cui si fa riferimento. Ciò vale anche nel caso di un ripristino di una versione di ONTAP che non supporta i riferimenti automatici ai nodi. I client continuano a utilizzare i riferimenti fino a quando il riferimento DFS non passa in timeout dalla cache del client.

L'autolocation utilizza i riferimenti automatici ai nodi SMB per aumentare le performance dei client SMB facendo riferimento ai client alla LIF sul nodo proprietario del volume di dati di una SVM. Quando un client SMB si connette a una condivisione SMB ospitata su una SVM, potrebbe connettersi utilizzando una LIF su un nodo che non possiede i dati richiesti e utilizza una rete di interconnessione cluster per recuperare i dati. Se la connessione SMB utilizza un LIF situato sul nodo contenente i dati richiesti, il client può ottenere tempi di risposta più rapidi.

ONTAP fornisce questa funzionalità utilizzando i riferimenti del file system distribuito Microsoft (DFS) per informare i client SMB che un file o una cartella richiesti nello spazio dei nomi è ospitato altrove. Un nodo fa un riferimento quando determina la presenza di una LIF SVM sul nodo contenente i dati. I riferimenti vengono effettuati in base alla posizione della directory principale della condivisione attraverso la quale il client è connesso.

Il riferimento si verifica durante la negoziazione SMB. Il riferimento viene fatto prima che venga stabilita la connessione. Dopo che ONTAP fa riferimento al nodo di destinazione, la connessione viene stabilita e il client accede ai dati attraverso il percorso LIF indicato da quel punto in poi. In questo modo, i client possono accedere più rapidamente ai dati ed evitare ulteriori comunicazioni del cluster.

Linee guida per l'utilizzo dei riferimenti automatici dei nodi con client Mac OS

I client Mac OS X non supportano i riferimenti automatici ai nodi SMB, anche se Mac OS supporta il file system distribuito (DFS) di Microsoft. I client Windows effettuano una richiesta di riferimento DFS prima di connettersi a una condivisione SMB. ONTAP fornisce un riferimento a una LIF di dati trovata sullo stesso nodo che ospita i dati richiesti, il che porta a tempi di risposta del client migliorati. Anche se Mac OS supporta DFS, i client Mac OS non si comportano esattamente come i client Windows in quest'area.

Informazioni correlate

In che modo ONTAP abilita le home directory dinamiche

"Gestione della rete"

"Tool di matrice di interoperabilità NetApp"

Supporto per i riferimenti automatici ai nodi SMB

Prima di attivare i riferimenti automatici ai nodi SMB, è necessario tenere presente che alcune funzionalità di ONTAP non supportano i riferimenti.

- I seguenti tipi di volumi non supportano i riferimenti automatici ai nodi SMB:
  - Membri di sola lettura di un mirror di condivisione del carico
  - Volume di destinazione di un mirror per la protezione dei dati
- I riferimenti ai nodi non si spostano insieme a uno spostamento LIF.

  Se un client utilizza una connessione di riferimento su una connessione SMB 2.x o SMB 3.0 e una LIF dati si sposta senza interruzioni, il client continua a utilizzare la stessa connessione di riferimento, anche se la LIF non è più locale rispetto ai dati.

- I riferimenti ai nodi non si spostano insieme a uno spostamento del volume.

  Se un client utilizza una connessione di riferimento su qualsiasi connessione SMB e si verifica uno spostamento del volume, il client continua a utilizzare la stessa connessione di riferimento, anche se il volume non si trova più sullo stesso nodo del LIF dei dati.

Attiva o disattiva i riferimenti automatici ai nodi SMB

È possibile abilitare i riferimenti automatici ai nodi SMB per aumentare le performance di accesso al client SMB. È possibile disattivare i riferimenti automatici dei nodi se non si desidera che ONTAP faccia riferimento ai client SMB.

Prima di iniziare

Un server CIFS deve essere configurato e in esecuzione sulla macchina virtuale di storage (SVM).

A proposito di questa attività

Per impostazione predefinita, la funzionalità SMB automatic node referrals (riferimenti automatici al nodo SMB) è disattivata. È possibile attivare o disattivare questa funzionalità su ogni SVM in base alle esigenze.

Questa opzione è disponibile al livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Attivare o disattivare i riferimenti automatici ai nodi SMB secondo necessità:

Se si desidera che i riferimenti automatici ai nodi SMB siano…	Immettere il seguente comando…
Attivato	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Disattivato	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   L'impostazione dell'opzione ha effetto per le nuove sessioni SMB. I client con connessione esistente possono utilizzare il riferimento al nodo solo quando scade il timeout della cache esistente.

3. Passare al livello di privilegio admin: `set -privilege admin`

Informazioni correlate

Opzioni server SMB disponibili

Utilizza le statistiche per monitorare l'attività di riferimento automatico del nodo

Per determinare il numero di connessioni SMB a cui si fa riferimento, è possibile monitorare l'attività di riferimento automatico del nodo utilizzando `statistics` comando. Monitorando i riferimenti è possibile determinare in che misura i riferimenti automatici individuano le connessioni sui nodi che ospitano le condivisioni e se è necessario ridistribuire i file LIF dei dati per fornire un migliore accesso locale alle condivisioni sul server CIFS.

A proposito di questa attività

Il `cifs` Object fornisce diversi contatori a livello di privilegio avanzato che sono utili per il monitoraggio dei riferimenti automatici ai nodi SMB:

- `node_referral_issued`

  Numero di client che hanno ricevuto un riferimento al nodo della directory principale di condivisione dopo che il client si è connesso utilizzando una LIF ospitata da un nodo diverso dal nodo della directory principale di condivisione.

- `node_referral_local`

  Numero di client connessi utilizzando una LIF ospitata dallo stesso nodo che ospita la directory principale di condivisione. L'accesso locale offre generalmente performance ottimali.

- `node_referral_not_possible`

  Numero di client che non hanno ricevuto un riferimento al nodo che ospita la directory principale di condivisione dopo la connessione utilizzando una LIF ospitata da un nodo diverso dal nodo della directory principale di condivisione. Questo perché non è stato trovato un LIF di dati attivo per il nodo della directory principale di condivisione.

- `node_referral_remote`

  Numero di client connessi utilizzando una LIF ospitata da un nodo diverso dal nodo che ospita la directory principale di condivisione. L'accesso remoto potrebbe causare un peggioramento delle performance.

È possibile monitorare le statistiche di riferimento dei nodi automatici sulla macchina virtuale di storage (SVM) raccogliendo e visualizzando i dati per un periodo di tempo specifico (un esempio). 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 delle performance.

> Per valutare e utilizzare le informazioni raccolte da `statistics` è necessario conoscere la distribuzione dei client nei propri ambienti.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Visualizzare le statistiche di riferimento dei nodi automatici utilizzando `statistics` comando.

   Questo esempio visualizza le statistiche di riferimento dei nodi automatici raccogliendo e visualizzando i dati per un periodo di tempo campionato:

   a. Avviare la raccolta: `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. Attendere il tempo di raccolta desiderato.

   c. Interrompere la raccolta: `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   d. Visualizzare le statistiche di riferimento dei nodi automatici: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                     Value
    ---------------------------- ---------------------------
    node_name                                                 node1
    node_referral_issued                                          0
    node_referral_local                                           1
    node_referral_not_possible                                    2
    node_referral_remote                                          2
    ...

    node_name                                                 node2
    node_referral_issued                                          2
    node_referral_local                                           1
    node_referral_not_possible                                    0
    node_referral_remote                                          2
    ...
```

L'output visualizza i contatori di tutti i nodi che partecipano a SVM vs1. Per maggiore chiarezza, nell'esempio vengono forniti solo i campi di output relativi alle statistiche di riferimento dei nodi automatici.

3. Tornare al livello di privilegio admin: `set -privilege admin`

Informazioni correlate

Visualizzazione delle statistiche

"Configurazione del monitoraggio delle performance"

Monitorare le informazioni di riferimento del nodo automatico SMB lato client utilizzando un client Windows

Per determinare quali riferimenti vengono fatti dal punto di vista del client, è possibile utilizzare Windows `dfsutil.exe` utility.

Il kit Remote Server Administration Tools (RSAT) disponibile con Windows 7 e i client successivi contiene `dfsutil.exe` utility. Utilizzando questa utility, è possibile visualizzare informazioni sul contenuto della cache di riferimento e le informazioni relative a ciascun riferimento attualmente utilizzato dal client. È inoltre possibile utilizzare l'utility per cancellare la cache di riferimento del client. Per ulteriori informazioni, consultare la Microsoft TechNet Library.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Sicurezza delle cartelle sulle condivisioni con enumerazione basata sull'accesso

Fornire la sicurezza delle cartelle sulle condivisioni con una panoramica dell'enumerazione basata sull'accesso

Quando l'enumerazione basata sull'accesso (ABE) è attivata su una condivisione SMB, gli utenti che non dispongono dell'autorizzazione per accedere a una cartella o a un file contenuto nella condivisione (tramite restrizioni di autorizzazione individuali o di gruppo) non vedono la risorsa condivisa visualizzata nel proprio ambiente, anche se la condivisione stessa rimane visibile.

Le proprietà di condivisione convenzionali consentono di specificare quali utenti (individualmente o in gruppi) dispongono dell'autorizzazione per visualizzare o modificare file o cartelle contenuti nella condivisione. Tuttavia, non consentono di controllare se le cartelle o i file all'interno della condivisione sono visibili agli utenti che non dispongono dell'autorizzazione per accedervi. Ciò potrebbe causare problemi se i nomi di queste cartelle o file all'interno della condivisione descrivono informazioni riservate, come i nomi dei clienti o dei prodotti in fase di sviluppo.

L'enumerazione basata sull'accesso (ABE) estende le proprietà di condivisione per includere l'enumerazione di file e cartelle all'interno della condivisione. ABE consente quindi di filtrare la visualizzazione di file e cartelle all'interno della condivisione in base ai diritti di accesso dell'utente. In altre termini, la condivisione stessa sarebbe visibile a tutti gli utenti, ma i file e le cartelle all'interno della condivisione potrebbero essere visualizzati o nascosti agli utenti designati. Oltre a proteggere le informazioni sensibili sul luogo di lavoro, ABE consente di semplificare la visualizzazione di grandi strutture di directory a beneficio degli utenti che non hanno bisogno di accedere all'intera gamma di contenuti. Ad esempio, la condivisione stessa sarebbe visibile a tutti gli utenti, ma i file e le cartelle all'interno della condivisione potrebbero essere visualizzati o nascosti.

Scopri di più "Impatto delle performance quando si utilizza l'enumerazione SMB/CIFS Access Based Enumeration".

Abilitare o disabilitare l'enumerazione basata sull'accesso sulle condivisioni SMB

È possibile attivare o disattivare l'enumerazione basata sull'accesso (ABE) sulle condivisioni SMB per consentire o impedire agli utenti di visualizzare le risorse condivise a cui non dispongono dell'autorizzazione di accesso.

A proposito di questa attività

Per impostazione predefinita, ABE è disattivato.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Abilitare ABE su una nuova condivisione	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Quando si crea una condivisione SMB, è possibile specificare ulteriori impostazioni di condivisione opzionali e proprietà di condivisione aggiuntive. Per ulteriori informazioni, vedere la pagina man di `vserver cifs share create` comando.
Abilitare ABE su una condivisione esistente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Le proprietà di condivisione esistenti vengono conservate. La proprietà di condivisione ABE viene aggiunta all'elenco esistente di proprietà di condivisione.
Disattiva ABE su una condivisione esistente	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Le altre proprietà di condivisione vengono conservate. Solo la proprietà di condivisione ABE viene rimossa dall'elenco delle proprietà di condivisione.

2. Verificare che la configurazione della condivisione sia corretta utilizzando `vserver cifs share show` comando.

Esempi

Nell'esempio seguente viene creata una condivisione SMB ABE denominata "sales" con un percorso di `/sales` Su SVM vs1. La condivisione viene creata con `access-based-enumeration` come proprietà condivisa:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Nell'esempio riportato di seguito viene aggiunto il `access-based-enumeration` Condividere la proprietà su una condivisione SMB denominata "data2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ----------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informazioni correlate

Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente

Abilitare o disabilitare l'enumerazione basata sull'accesso da un client Windows

È possibile attivare o disattivare l'enumerazione basata sull'accesso (ABE) sulle condivisioni SMB da un client Windows, che consente di configurare questa impostazione di condivisione senza la necessità di connettersi al server CIFS.

> Il `abecmd` L'utility non è disponibile nelle nuove versioni dei client Windows Server e Windows. È stato rilasciato come parte di Windows Server 2008. Il supporto per Windows Server 2008 è terminato il 14 gennaio 2020.

Fasi

1. Da un client Windows che supporta ABE, immettere il seguente comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Per ulteriori informazioni su `abecmd` Consultare la documentazione del client Windows.

Dipendenze di nomi di file e directory NFS e SMB

Panoramica delle dipendenze di nomi di file e directory NFS e SMB

Le convenzioni di denominazione di file e directory dipendono dai` sistemi operativi dei client di rete e dai protocolli di condivisione file, oltre alle impostazioni della lingua del cluster e dei client ONTAP.

Il sistema operativo e i protocolli di condivisione file determinano quanto segue:

- Caratteri che possono essere utilizzati da un nome file
- Distinzione tra maiuscole e minuscole per un nome file

ONTAP supporta caratteri multi-byte nei nomi di file, directory e qtree, a seconda della versione di ONTAP.

Caratteri che possono essere utilizzati da un nome di file o di directory

Se si accede a un file o a una directory da client con sistemi operativi diversi, utilizzare caratteri validi in entrambi i sistemi operativi.

Ad esempio, se si utilizza UNIX per creare un file o una directory, non utilizzare i due punti (:) nel nome perché i due punti non sono consentiti nei nomi di file o directory MS-DOS. Poiché le restrizioni sui caratteri validi variano da un sistema operativo all'altro, consultare la documentazione del sistema operativo client per ulteriori informazioni sui caratteri non consentiti.

Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo

I nomi di file e directory sono sensibili al maiuscolo/minuscolo per i client NFS e non al maiuscolo/minuscolo ma conservano il maiuscolo/minuscolo per i client SMB. È necessario comprendere le implicazioni di un ambiente multiprotocollo e le azioni da intraprendere quando si specifica il percorso durante la creazione di condivisioni SMB e quando si accede ai dati all'interno delle condivisioni.

Se un client SMB crea una directory denominata `testdir`, Sia i client SMB che NFS visualizzano il nome del file come `testdir`. Tuttavia, se un utente SMB tenta in seguito di creare un nome di directory `TESTDIR`, Il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea una directory denominata `TESTDIR`I client , NFS e SMB visualizzano il nome della directory in modo diverso, come segue:

- Sui client NFS, ad esempio, vengono visualizzati entrambi i nomi di directory così come sono stati creati `testdir` e. `TESTDIR`, perché i nomi delle directory sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere le due directory. Una directory ha il nome del file di base. Alle directory aggiuntive viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `testdir` e. `TESTDI~1`.
  - ONTAP crea il `TESTDI~1` nome della directory per differenziare le due directory.

    In questo caso, è necessario utilizzare il nome 8.3 quando si specifica un percorso di condivisione durante la creazione o la modifica di una condivisione su una macchina virtuale di storage (SVM).

Analogamente per i file, se viene creato un client SMB `test.txt`, Sia i client SMB che NFS visualizzano il nome del file come `text.txt`. Tuttavia, se un utente SMB tenta di creare in un secondo momento `Test.txt`, Il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea un file denominato `Test.txt`I client , NFS e SMB visualizzano il nome del file in modo diverso, come segue:

- Sui client NFS, vengono visualizzati entrambi i nomi dei file così come sono stati creati, `test.txt` e. `Test.txt`, perché i nomi dei file sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere i due file. Un file ha il nome del file di base. Ai file aggiuntivi viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `test.txt` e. `TEST~1.TXT`.
  - ONTAP crea il `TEST~1.TXT` nome del file per differenziare i due file.

> Se è stata attivata o modificata la mappatura dei caratteri utilizzando i comandi di mappatura dei caratteri CIFS di Vserver, una ricerca di Windows normalmente non sensibile al maiuscolo/minuscolo diventa sensibile al maiuscolo/minuscolo.

Come ONTAP crea i nomi di file e directory

ONTAP crea e mantiene due nomi per i file o le directory in qualsiasi directory che ha accesso da un client SMB: Il nome lungo originale e un nome in formato 8.3.

Per i nomi di file o directory che superano il nome di otto caratteri o il limite di estensione di tre caratteri (per i file), ONTAP genera un nome in formato 8.3 come segue:

- Il nome del file o della directory originale viene troncato a sei caratteri, se il nome supera i sei caratteri.
- Aggiunge una tilde (~) e un numero, da uno a cinque, ai nomi di file o directory che non sono più univoci dopo essere stati troncati.

  Se esaurisce i numeri perché ci sono più di cinque nomi simili, crea un nome unico che non ha alcuna relazione con il nome originale.

- Nel caso dei file, l'estensione del nome del file viene troncata a tre caratteri.

Ad esempio, se un client NFS crea un file denominato `specifications.html`, Il nome del file di formato 8.3 creato da ONTAP è `specif~1.htm`. Se questo nome esiste già, ONTAP utilizza un numero diverso alla fine del nome del file. Ad esempio, se un client NFS crea un altro file denominato `specifications_new.html`, il formato 8.3 di `specifications_new.html` è `specif~2.htm`.

Come ONTAP gestisce i nomi di file, directory e qtree multi-byte

A partire da ONTAP 9.5, il supporto per i nomi codificati UTF-8 a 4 byte consente la creazione e la visualizzazione di nomi di file, directory e albero che includono caratteri aggiuntivi Unicode al di fuori del piano multilingua di base (BMP). Nelle versioni precedenti, questi caratteri supplementari non erano visualizzati correttamente negli ambienti multiprotocollo.

Per abilitare il supporto per i nomi codificati UTF-8 a 4 byte, è disponibile un nuovo codice lingua *utf8mb4* per `vserver` e. `volume` famiglie di comandi.

È necessario creare un nuovo volume in uno dei seguenti modi:

- Impostazione del volume `-language` opzione esplicitamente: `volume create -language utf8mb4 {…}`
- Ereditare il volume `-language` Opzione da una SVM creata con o modificata per l'opzione: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9,6 e versioni precedenti, non è possibile modificare i volumi esistenti per il supporto di utf8mb4; è necessario creare un nuovo volume pronto per utf8mb4 e quindi migrare i dati utilizzando strumenti di copia basati su client.

  È possibile aggiornare le SVM per il supporto di utf8mb4, ma i volumi esistenti conservano i codici lingua originali.

  Se si utilizza ONTAP 9.7P1 o versione successiva, è possibile modificare i volumi esistenti per utf8mb4 con una richiesta di supporto. Per ulteriori informazioni, vedere "È possibile modificare la lingua del volume dopo la creazione in ONTAP?".

- A partire da ONTAP 9,8, è possibile utilizzare `[-language <Language code>]` Parametro per modificare la lingua del volume da *.UTF-8 a utf8mb4. Per modificare la lingua di un volume, contattare "Supporto NetApp".

  > I nomi LUN con caratteri UTF-8 a 4 byte non sono attualmente supportati.

- I dati dei caratteri Unicode sono generalmente rappresentati nelle applicazioni di file system Windows che utilizzano il formato di trasformazione Unicode a 16 bit (UTF-16) e nei file system NFS che utilizzano il formato di trasformazione Unicode a 8 bit (UTF-8).

  Nelle release precedenti a ONTAP 9.5, i nomi, inclusi i caratteri supplementari UTF-16 creati dai client Windows, venivano visualizzati correttamente su altri client Windows ma non sono stati tradotti correttamente in UTF-8 per i client NFS. Analogamente, i nomi con caratteri supplementari UTF-8 creati dai client NFS non sono stati tradotti correttamente in UTF-16 per i client Windows.

- Quando si creano nomi di file su sistemi con ONTAP 9.4 o versioni precedenti che contengono caratteri supplementari validi o non validi, ONTAP rifiuta il nome del file e restituisce un errore di nome del file non valido.

  Per evitare questo problema, utilizzare solo caratteri BMP nei nomi dei file ed evitare di utilizzare caratteri supplementari oppure eseguire l'aggiornamento a ONTAP 9.5 o versioni successive.

A partire da ONTAP 9, i caratteri Unicode sono consentiti nei nomi qtree.

- È possibile utilizzare il `volume qtree` Command Family o System Manager per impostare o modificare i nomi di qtree.
- I nomi qtree possono includere caratteri multi-byte in formato Unicode, ad esempio caratteri giapponesi e cinesi.
- Nelle versioni precedenti a ONTAP 9.5, erano supportati solo i caratteri BMP (ovvero quelli che potevano essere rappresentati in 3 byte).

> Nelle release precedenti a ONTAP 9.5, il percorso di giunzione del volume padre del qtree può contenere nomi di qtree e directory con caratteri Unicode. Il `volume show` Il comando visualizza correttamente questi nomi quando il volume d'origine dispone di un'impostazione della lingua UTF-8. Tuttavia, se la lingua del volume padre non è una delle impostazioni della lingua UTF-8, alcune parti del percorso di giunzione vengono visualizzate utilizzando un nome alternativo NFS numerico.

- Nella versione 9.5 e successive, i caratteri a 4 byte sono supportati nei nomi qtree, a condizione che il qtree si trovi in un volume abilitato per utf8mb4.

Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi

I client NFS possono creare nomi di file che contengono caratteri non validi per i client SMB e alcune applicazioni Windows. È possibile configurare la mappatura dei caratteri per la conversione dei nomi file sui volumi per consentire ai client SMB di accedere ai file con nomi NFS che altrimenti non sarebbero validi.

A proposito di questa attività

Quando i client SMB accedono ai file creati dai client NFS, ONTAP esamina il nome del file. Se il nome non è un nome file SMB valido (ad esempio, se ha un carattere ":" incorporato), ONTAP restituisce il nome file 8.3 che viene mantenuto per ciascun file. Tuttavia, questo causa problemi per le applicazioni che codificano informazioni importanti in nomi di file lunghi.

Pertanto, se si condivide un file tra client su sistemi operativi diversi, è necessario utilizzare caratteri nei nomi dei file validi in entrambi i sistemi operativi.

Tuttavia, se si dispone di client NFS che creano nomi file contenenti caratteri non validi per i client SMB, è possibile definire una mappa che converte i caratteri NFS non validi in caratteri Unicode accettati sia da SMB che da alcune applicazioni Windows. Ad esempio, questa funzionalità supporta le applicazioni CATIA MCAD e Mathematica e altre applicazioni che richiedono questo requisito.

È possibile configurare la mappatura dei caratteri volume per volume.

Quando si configura la mappatura dei caratteri su un volume, è necessario tenere presente quanto segue:

- La mappatura dei caratteri non viene applicata tra i punti di giunzione.

  È necessario configurare esplicitamente la mappatura dei caratteri per ciascun volume di giunzione.

- È necessario assicurarsi che i caratteri Unicode utilizzati per rappresentare caratteri non validi o non validi siano caratteri che normalmente non vengono visualizzati nei nomi dei file; in caso contrario, si verificano mappature indesiderate.

  Ad esempio, se si tenta di mappare i due punti (:) a un trattino (-) ma il trattino (-) è stato utilizzato

correttamente nel nome del file, un client Windows che tenta di accedere a un file denominato “a-b” avrebbe la sua richiesta mappata al nome NFS “a:b” (non il risultato desiderato).

- Dopo aver applicato la mappatura dei caratteri, se la mappatura contiene ancora un carattere Windows non valido, ONTAP torna ai nomi file di Windows 8.3.
- Nelle notifiche FPolicy, nei registri di controllo NAS e nei messaggi di traccia di sicurezza, vengono visualizzati i nomi dei file mappati.
- Quando viene creata una relazione SnapMirror di tipo DP, la mappatura dei caratteri del volume di origine non viene replicata sul volume DP di destinazione.
- Distinzione tra maiuscole e minuscole: Poiché i nomi Windows mappati diventano nomi NFS, la ricerca dei nomi segue la semantica NFS. Ciò include il fatto che le ricerche NFS sono sensibili al maiuscolo/minuscolo. Ciò significa che le applicazioni che accedono alle condivisioni mappate non devono fare affidamento sul comportamento di Windows senza distinzione tra maiuscole e minuscole. Tuttavia, il nome 8.3 è disponibile, senza distinzione tra maiuscole e minuscole.
- Mappature parziali o non valide: Dopo aver mappato un nome da restituire ai client che eseguono l’enumerazione della directory ("dir"), il nome Unicode risultante viene controllato per la validità di Windows. Se il nome contiene ancora caratteri non validi o se non è valido per Windows (ad esempio, termina con "." o vuoto) viene restituito il nome 8.3 invece del nome non valido.

Fase

1. Configurare la mappatura dei caratteri:

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …`

Il mapping è costituito da un elenco di coppie di caratteri origine-destinazione separate da “:”. I caratteri sono caratteri Unicode immessi utilizzando cifre esadecimali. Ad esempio: 3C:E03C.

Il primo valore di ciascuno `mapping_text` La coppia separata dai due punti è il valore esadecimale del carattere NFS che si desidera convertire, mentre il secondo valore è il valore Unicode utilizzato da SMB. Le coppie di mappatura devono essere univoche (deve esistere una mappatura uno a uno).

- Mappatura di origine

La tabella seguente mostra il set di caratteri Unicode consentito per il mapping di origine:

+

Carattere Unicode	Carattere stampato	Descrizione
0x01-0x19	Non applicabile	Caratteri di controllo non stampabili
0x5C		Barra rovesciata
0x3A	:	Due punti
0x2A	*	Asterisco
0x3F	?	Punto interrogativo

Carattere Unicode	Carattere stampato	Descrizione
0x22	"	Virgoletta
0x3C	<	Inferiore a.
0x3E	>	Maggiore di
0x7C		
Linea verticale	0xB1	±

- Mappatura di destinazione

  È possibile specificare i caratteri di destinazione nella “Private Use Area” di Unicode nel seguente intervallo: U+E0000…U+F8FF.

Esempio

Il seguente comando crea un mapping di caratteri per un volume denominato “data” su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Informazioni correlate

Creazione e gestione di volumi di dati negli spazi dei nomi NAS

Comandi per la gestione delle mappature dei caratteri per la conversione dei nomi file SMB

È possibile gestire la mappatura dei caratteri creando, modificando, visualizzando o eliminando le mappature dei caratteri dei file utilizzate per la conversione dei nomi dei file SMB sui volumi FlexVol.

Se si desidera…	Utilizzare questo comando…
Creare nuove mappature dei caratteri del file	`vserver cifs character-mapping create`
Visualizza le informazioni sulle mappature dei caratteri del file	`vserver cifs character-mapping show`

Se si desidera…	Utilizzare questo comando…
Modificare le mappature dei caratteri del file esistente	`vserver cifs character-mapping modify`
Eliminare le mappature dei caratteri del file	`vserver cifs character-mapping delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Informazioni correlate

Configurazione della mappatura dei caratteri per la conversione dei nomi file SMB sui volumi