



Gestione dello storage NAS

ONTAP 9

NetApp
April 24, 2024

Sommario

- Gestione dello storage NAS 1
 - Gestire i protocolli NAS con System Manager 1
 - Configurare NFS con la CLI 20
 - Gestisci NFS con la CLI 88
 - Gestire il trunking NFS 205
 - Gestire NFS su RDMA 215
 - Configurare SMB con la CLI 221
 - Gestire SMB con la CLI 264
 - Fornire l'accesso del client S3 ai dati NAS 618
 - Configurazione SMB per Microsoft Hyper-V e SQL Server 627

Gestione dello storage NAS

Gestire i protocolli NAS con System Manager

Panoramica sulla gestione NAS con System Manager

Gli argomenti di questa sezione mostrano come configurare e gestire gli ambienti NAS con Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione di sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), consultare i seguenti argomenti:

- ["Panoramica della configurazione di NFS"](#)
- ["Panoramica della configurazione SMB"](#)

System Manager supporta i flussi di lavoro per:

- Configurazione iniziale dei cluster che si intende utilizzare per i file service NAS.
- Provisioning di volumi aggiuntivo per esigenze di storage in continua evoluzione.
- Configurazione e manutenzione per strutture di sicurezza e autenticazione standard di settore.

Con System Manager, è possibile gestire i servizi NAS a livello di componente:

- Protocolli: NFS, SMB o entrambi (multiprotocollo NAS)
- Servizi di gestione dei nomi: DNS, LDAP e NIS
- Switch name service
- Sicurezza Kerberos
- Esportazioni e condivisioni
- Qtree
- Mappatura dei nomi di utenti e gruppi

Provisioning dello storage NFS per gli archivi dati VMware

Prima di utilizzare la console di storage virtuale per VMware vSphere (VSC) per eseguire il provisioning dei volumi NFS su un sistema di storage basato su ONTAP per gli host ESXi, abilitare NFS utilizzando Gestione di sistema per ONTAP 9.7 o versioni successive.

Dopo aver creato un ["Storage VM abilitato per NFS"](#) In System Manager, è possibile eseguire il provisioning dei volumi NFS e gestire i datastore utilizzando VSC.

A partire da VSC 7.0, VSC fa parte di ["Strumenti ONTAP per appliance virtuali VMware vSphere"](#), Che include VSC, vStorage API for Storage Awareness (VASA) Provider e Storage Replication Adapter (SRA) per le funzionalità di VMware vSphere.

Controllare ["Matrice di interoperabilità NetApp"](#) Per confermare la compatibilità tra le versioni correnti di ONTAP e VSC.

Per impostare l'accesso NFS per gli host ESXi agli archivi dati utilizzando System Manager Classic (per

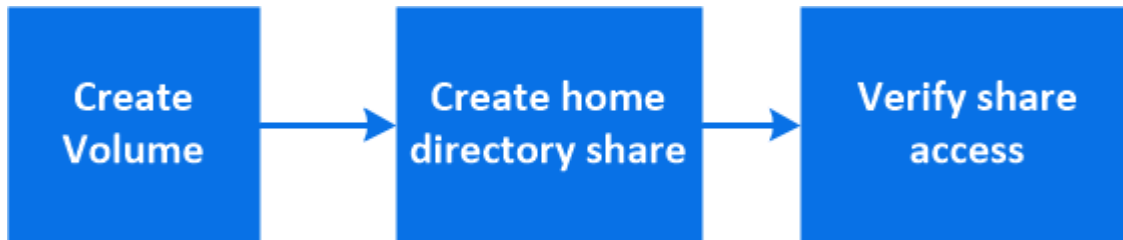
ONTAP 9.7 e versioni precedenti), vedere ["Panoramica della configurazione NFS per ESXi con VSC"](#)

Per ulteriori informazioni, vedere ["TR-4597: VMware vSphere per ONTAP"](#) E la documentazione per la release VSC.

Provisioning dello storage NAS per le home directory

Creare volumi per fornire storage per le home directory utilizzando il protocollo SMB.

Questa procedura crea nuovi volumi per le home directory su un ["VM di storage già in uso con SMB"](#). È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate.



È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per SMB.
 - a. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi fare clic su **Add** (Aggiungi).
 - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo SMB. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.
- È possibile fare clic su **altre opzioni** per personalizzare la configurazione del volume e abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. [[fase 2,fase 2 nel flusso di lavoro]] fare clic su **Storage > Shares**, fare clic su **Add** e selezionare **Home Directory**.
3. Su un client Windows, effettuare le seguenti operazioni per verificare che la condivisione sia accessibile.
 - a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:
`_SMB_Server_Name__Share_Name__`

Se il nome della condivisione è stato creato con variabili (%w, %d o %u), verificare l'accesso con un nome risolto.
 - b. Sul disco appena creato, creare un file di prova, quindi eliminare il file.

Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom**, **Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a [\[step2\]](#) per completare il provisioning delle home directory.

Provisioning dello storage NAS per i server Linux utilizzando NFS

Creare volumi per fornire storage ai server Linux utilizzando il protocollo NFS con Gestione di sistema di ONTAP (9.7 e versioni successive).

Questa procedura crea nuovi volumi su un ["VM di storage esistente abilitata per NFS"](#). È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il

sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Per ulteriori informazioni sulla gamma di funzionalità del protocollo NFS ONTAP, consultare ["Panoramica di riferimento di NFS"](#).

Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per NFS.
 - a. Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
 - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo NFS. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.



Il criterio di esportazione predefinito garantisce l'accesso completo a tutti gli utenti.

- È possibile fare clic su **altre opzioni** per personalizzare la configurazione del volume e abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. su un client Linux, procedere come segue per verificare l'accesso.
 - a. Creare e montare il volume utilizzando l'interfaccia di rete della VM di storage.
 - b. Sul volume appena montato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile ["limitare l'accesso del client con i criteri di esportazione del volume"](#) E impostare la proprietà e le autorizzazioni UNIX desiderate sul volume montato.

Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume

FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a [\[step2-complete-prov\]](#) Per completare il provisioning per i server Linux utilizzando NFS.

Altri modi per farlo in ONTAP

Per eseguire questa attività con...	Fare riferimento a...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	"Panoramica della configurazione di NFS"
Interfaccia a riga di comando (CLI) di ONTAP	"Panoramica della configurazione di NFS con la CLI"

Gestire l'accesso utilizzando policy di esportazione

Abilitare l'accesso del client Linux ai server NFS utilizzando i criteri di esportazione.

Questa procedura crea o modifica i criteri di esportazione per un ["VM di storage esistente abilitata per NFS"](#).

Fasi

1. In System Manager, fare clic su **Storage > Volumes**.
2. Fare clic su un volume abilitato NFS e fare clic su **More** (Altro).
3. Fare clic su **Edit Export Policy** (Modifica policy di esportazione), quindi su **Select an existing policy** (Seleziona policy esistente) o **Add a new policy** (Aggiungi nuova policy).

Provisioning dello storage NAS per i server Windows utilizzando SMB

Creare volumi per fornire storage ai server Windows utilizzando il protocollo SMB utilizzando Gestione di sistema, disponibile con ONTAP 9.7 e versioni successive.

Questa procedura crea nuovi volumi su un ["VM di storage già in uso con SMB"](#) e crea una condivisione per la directory root (/) del volume. È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate. Dopo la configurazione SMB iniziale, è possibile creare condivisioni aggiuntive e modificarne le proprietà.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Per ulteriori informazioni sulla gamma di funzionalità del protocollo SMB ONTAP, consultare ["Panoramica di riferimento SMB"](#).

Prima di iniziare

- A partire da ONTAP 9.13.1, puoi attivare l'analisi della capacità e il monitoraggio delle attività per impostazione predefinita sui nuovi volumi. In System Manager, è possibile gestire le impostazioni predefinite a livello di cluster o storage VM. Per ulteriori informazioni, vedere [Abilita analisi del file system](#).

Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per SMB.

- a. Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
- b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo SMB. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si seleziona **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.
- È possibile selezionare **altre opzioni** per personalizzare la configurazione del volume in modo da abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. passa a un client Windows per verificare che la condivisione sia accessibile.

- a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:

_SMB_Server_Name__Share_Name_

- b. Sul disco appena creato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile limitare l'accesso client con l'ACL di condivisione e impostare le proprietà di sicurezza desiderate sull'unità mappata. Vedere ["Creare una condivisione SMB"](#) per ulteriori informazioni.

Aggiungere o modificare le condivisioni

È possibile aggiungere ulteriori condivisioni dopo la configurazione SMB iniziale. Le condivisioni vengono create con i valori predefiniti e le proprietà selezionate. Questi possono essere modificati in un secondo momento.

Durante la configurazione di una condivisione, è possibile impostare le seguenti proprietà di condivisione:


- Autorizzazioni di accesso
- Condividere le proprietà
 - Abilita la disponibilità continua per le condivisioni che contengono dati Hyper-V e SQL Server su SMB (a partire da ONTAP 9.10.1). Vedere anche:
 - ["Requisiti di condivisione continuamente disponibili per Hyper-V su SMB"](#)
 - ["Requisiti di condivisione continuamente disponibili per SQL Server su SMB"](#)
 - Crittografare i dati con SMB 3.0 mentre si accede a questa condivisione.

Dopo la configurazione iniziale, è anche possibile modificare queste proprietà:

- Link simbolici
 - Attiva o disattiva i link simbolici e i widelink
- Condividere le proprietà
 - Consentire ai client di accedere alla directory Snapshot Copies.
 - Abilitare gli oplock, consentendo ai client di bloccare i file e memorizzare nella cache il contenuto localmente (impostazione predefinita).
 - Abilitare l'enumerazione basata sull'accesso (ABE) per visualizzare le risorse condivise in base alle autorizzazioni di accesso dell'utente.

Procedure

Per aggiungere una nuova condivisione in un volume abilitato per SMB, fare clic su **Storage > Shares**, fare clic su **Add** e selezionare **Share**.

Per modificare una condivisione esistente, fare clic su **Storage > Shares**, quindi fare clic su  E selezionare **Modifica**.

Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di QoS personalizzato o disattivare la QoS, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

Questa opzione non è disponibile se in precedenza è stato selezionato *posizionamento manuale in Performance Service Level. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita. **Autorizzazione di accesso per i protocolli per i quali è**

configurato il volume. *Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa. *Fare clic su *Save (Salva) per creare il volume e aggiungerlo alla VM del cluster e dello storage.

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a. [\[step2-compl-prov-win\]](#) Per completare il provisioning per i server Windows utilizzando SMB.

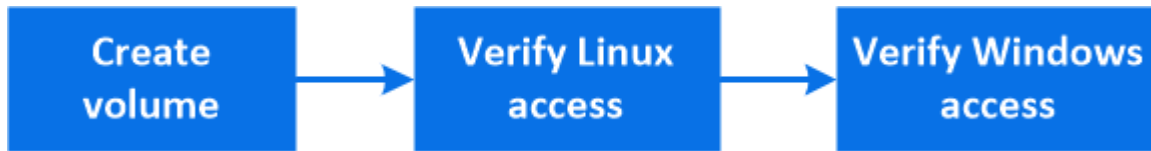
Altri modi per farlo in ONTAP

Per eseguire questa attività con...	Fare riferimento a...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	"Panoramica della configurazione SMB"
L'interfaccia della riga di comando di ONTAP	"Panoramica della configurazione SMB con la CLI"

Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB

Creare volumi per fornire storage ai client utilizzando il protocollo NFS o SMB.

Questa procedura crea nuovi volumi su un ["VM di storage esistente abilitata per protocolli NFS e SMB"](#).



Il protocollo NFS è generalmente utilizzato in ambienti Linux. Di norma il protocollo SMB viene utilizzato in ambienti Windows. Tuttavia, sia NFS che SMB possono essere utilizzati con Linux o Windows.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per NFS e SMB.

- Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
- Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con i protocolli NFS e SMB. Se è disponibile una sola VM di storage configurata con i protocolli NFS e SMB, il campo **Storage VM** non viene visualizzato.

- Fare clic su **altre opzioni** e selezionare **Esporta tramite NFS**.

L'impostazione predefinita garantisce l'accesso completo a tutti gli utenti. È possibile aggiungere altre regole restrittive al criterio di esportazione in un secondo momento.

- Selezionare **Condividi tramite SMB/CIFS**.

La condivisione viene creata con un ACL (Access Control List) predefinito impostato su "controllo completo" per il gruppo **Everyone**. È possibile aggiungere restrizioni all'ACL in un secondo momento.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.

In alternativa, è possibile continuare ad abilitare eventuali servizi aggiuntivi richiesti, come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. su un client Linux, verificare che l'esportazione sia accessibile.

- Creare e montare il volume utilizzando l'interfaccia di rete della VM di storage.
- Sul volume appena montato, creare un file di test, scriverne del testo ed eliminare il file.

3. Su un client Windows, effettuare le seguenti operazioni per verificare che la condivisione sia accessibile.

a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:

_SMB_Server_Name__Share_Name_

b. Sul disco appena creato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile "[Limitare l'accesso del client con i criteri di esportazione del volume e limitare l'accesso del client con l'ACL di condivisione](#)" e impostare la proprietà e le autorizzazioni desiderate sul volume esportato e condiviso.

Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.

Dopo aver salvato il volume, tornare a. [\[step2-compl-prov-nfs-smb\]](#) Per completare il provisioning multiprotocollo per server Windows e Linux.

Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Guarda questo contenuto...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	"Panoramica della configurazione multiprotocollo SMB e NFS"
L'interfaccia della riga di comando di ONTAP	"Panoramica della configurazione SMB con la CLI" +"Panoramica della configurazione di NFS con la CLI" +"Quali sono gli stili di sicurezza e i loro effetti" +"Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo"

Accesso client sicuro con Kerberos

Abilitare Kerberos per proteggere l'accesso allo storage per i client NAS.

Questa procedura consente di configurare Kerberos su una VM di storage esistente abilitata per ["NFS"](#) oppure ["PMI"](#).

Prima di iniziare, è necessario aver configurato DNS, NTP e ["LDAP"](#) sul sistema storage.



Fasi

1. Nella riga di comando di ONTAP, impostare le autorizzazioni UNIX per il volume root della VM di storage.
 - a. Visualizzare le autorizzazioni pertinenti sul volume root della VM di storage: `volume show -volume root_vol_name-fields user,group,unix-permissions`

Il volume root della VM di storage deve avere la seguente configurazione:

Nome...	Impostazione in corso...
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	755

- a. Se questi valori non vengono visualizzati, utilizzare `volume modify` per aggiornarli.
2. Impostare le autorizzazioni utente per il volume root della VM di storage.
 - a. Visualizzare gli utenti UNIX locali: `vserver services name-service unix-user show -vserver vserver_name`

Per la macchina virtuale di storage devono essere configurati i seguenti utenti UNIX:

Nome utente	ID utente	ID gruppo primario
nfs	500	0
root	0	0

+

Nota: l'utente NFS non è richiesto se esiste una mappatura nome Kerberos-UNIX per l'SPN dell'utente client NFS; vedere il passaggio 5.

- a. Se questi valori non vengono visualizzati, utilizzare `vserver services name-service unix-user modify` per aggiornarli.

3. Impostare le autorizzazioni di gruppo per il volume root della VM di storage.

- a. Visualizzare i gruppi UNIX locali: `vserver services name-service unix-group show -vserver vserver_name`

La macchina virtuale di storage deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0

- a. Se questi valori non vengono visualizzati, utilizzare `vserver services name-service unix-group modify` per aggiornarli.

4. Passare a System Manager per configurare Kerberos

5. In System Manager, fare clic su **Storage > Storage VM** e selezionare la VM di storage.

6. Fare clic su **Impostazioni**.

7. Fare clic su ➔ In Kerberos.

8. Fare clic su **Add** (Aggiungi) sotto Kerberos Realm (Area autenticazione Kerberos) e completare le seguenti sezioni:

- Aggiungi area di autenticazione Kerberos

Inserire i dettagli di configurazione in base al vendor KDC.

- Aggiungi interfaccia di rete a Realm

Fare clic su **Aggiungi** e selezionare un'interfaccia di rete.

9. Se lo si desidera, aggiungere i mapping dai nomi principali Kerberos ai nomi utente locali.

- a. Fare clic su **Storage > Storage VM** (Storage VM) e selezionare la VM di storage.
- b. Fare clic su **Impostazioni**, quindi su ➔ Sotto **mappatura nome**.
- c. In **Kerberos to UNIX**, aggiungere modelli e sostituzioni utilizzando espressioni regolari.



Fornire l'accesso client con i servizi di nome

Abilitare ONTAP per cercare informazioni su host, utenti, gruppi o netgroup utilizzando LDAP o NIS per autenticare i client NAS.

Questa procedura crea o modifica le configurazioni LDAP o NIS su una VM di storage esistente abilitata per "NFS" oppure "PMI".

Per le configurazioni LDAP, è necessario disporre dei dettagli di configurazione LDAP richiesti nell'ambiente e utilizzare uno schema LDAP ONTAP predefinito.

Fasi

1. Configurare il servizio richiesto: Fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, fare clic su **Impostazioni**, quindi fare clic su  Per LDAP o NIS.
3. Includi eventuali modifiche nel nome switch servizi: Fare clic su  Sotto Name Services Switch.

Gestire directory e file

Espandere la visualizzazione del volume di System Manager per visualizzare ed eliminare directory e file.

A partire da ONTAP 9.9.1, le directory vengono eliminate con la funzionalità di eliminazione rapida delle directory a bassa latenza.

Per ulteriori informazioni sulla visualizzazione dei file system in ONTAP 9.9.1 e versioni successive, vedere ["Panoramica di file System Analytics"](#).

Fase

1. Selezionare **Storage > Volumes** (Storage > volumi). Espandere un volume per visualizzarne il contenuto.

Gestione di utenti e gruppi specifici dell'host con System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per gestire utenti e gruppi specifici di un host UNIX o Windows.

È possibile eseguire le seguenti procedure:

Windows	UNIX
<ul style="list-style-type: none">• Visualizzare utenti e gruppi Windows• [add-edit-delete-Windows]• [manage-windows-users]	<ul style="list-style-type: none">• Visualizzare utenti e gruppi UNIX• [add-edit-delete-UNIX]• [manage-unix-users]



Visualizzare utenti e gruppi Windows

In System Manager, è possibile visualizzare un elenco di utenti e gruppi Windows.

Fasi

1. In System Manager, fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, quindi selezionare la scheda **Impostazioni**.
3. Scorrere fino all'area **host Users and Groups** (utenti e gruppi host).

La sezione **Windows** visualizza un riepilogo del numero di utenti in ciascun gruppo associato alla VM di storage selezionata.

4. Fare clic su  Nella sezione **Windows**.
5. Fare clic sulla scheda **gruppi**, quindi su  accanto al nome di un gruppo per visualizzare i dettagli relativi a tale gruppo.
6. Per visualizzare gli utenti di un gruppo, selezionare il gruppo, quindi fare clic sulla scheda **utenti**.

Aggiungere, modificare o eliminare un gruppo Windows

In System Manager, è possibile gestire i gruppi Windows aggiungendoli, modificandoli o eliminandoli.

Fasi

1. In Gestione sistema, visualizzare l'elenco dei gruppi Windows. Fare riferimento a [Visualizzare utenti e gruppi Windows](#).
2. Nella scheda **gruppi**, è possibile gestire i gruppi con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un gruppo	<ol style="list-style-type: none">1. Fare clic su + Add.2. Inserire le informazioni del gruppo.3. Specificare i privilegi.4. Specificare i membri del gruppo (aggiungere utenti locali, utenti di dominio o gruppi di dominio).
Modificare un gruppo	<ol style="list-style-type: none">1. Accanto al nome del gruppo, fare clic su :, Quindi fare clic su Edit (Modifica).2. Modificare le informazioni del gruppo.
Eliminare un gruppo	<ol style="list-style-type: none">1. Selezionare la casella accanto al gruppo o ai gruppi che si desidera eliminare.2. Fare clic su Delete. <p>Nota: è anche possibile eliminare un singolo gruppo facendo clic su : Accanto al nome del gruppo, quindi fare clic su Delete (Elimina).</p>






Gestire gli utenti Windows

In System Manager, è possibile gestire gli utenti Windows aggiungendoli, modificandoli, eliminandoli, abilitandoli o disattivandoli. È inoltre possibile modificare la password di un utente Windows.

Fasi

1. In System Manager, visualizzare l'elenco degli utenti per il gruppo. Fare riferimento a [Visualizzare utenti e gruppi Windows](#).
2. Nella scheda **utenti**, è possibile gestire gli utenti con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un utente	<ol style="list-style-type: none">1. Fare clic su + Add.2. Inserire le informazioni dell'utente.
Modificare un utente	<ol style="list-style-type: none">1. Accanto al nome utente, fare clic su :, Quindi fare clic su Edit (Modifica).2. Modificare le informazioni dell'utente.

Eliminare un utente	<ol style="list-style-type: none"> 1. Selezionare la casella accanto all'utente o agli utenti che si desidera eliminare. 2. Fare clic su  Delete . <p>Nota: è inoltre possibile eliminare un singolo utente facendo clic su  Accanto al nome utente, quindi fare clic su Delete (Elimina).</p>
Modificare la password dell'utente	<ol style="list-style-type: none"> 1. Accanto al nome utente, fare clic su  , Quindi fare clic su Change Password (Modifica password). 2. Inserire la nuova password e confermarla.
Abilitare un utente	<ol style="list-style-type: none"> 1. Selezionare la casella accanto a ciascun utente disattivato che si desidera attivare. 2. Fare clic su  Enable .
Disattivare un utente	<ol style="list-style-type: none"> 1. Selezionare la casella accanto a ciascun utente abilitato che si desidera disattivare. 2. Fare clic su  Disable .


Visualizzare utenti e gruppi UNIX

In System Manager, è possibile visualizzare un elenco di utenti e gruppi UNIX.

Fasi

1. In System Manager, fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, quindi selezionare la scheda **Impostazioni**.
3. Scorrere fino all'area **host Users and Groups** (utenti e gruppi host).

La sezione **UNIX** visualizza un riepilogo del numero di utenti in ciascun gruppo associato alla VM di storage selezionata.

4. Fare clic su  Nella sezione **UNIX**.
5. Fare clic sulla scheda **Groups** (gruppi) per visualizzare i dettagli relativi al gruppo.
6. Per visualizzare gli utenti di un gruppo, selezionare il gruppo, quindi fare clic sulla scheda **utenti**.




Aggiungere, modificare o eliminare un gruppo UNIX

In System Manager, è possibile gestire i gruppi UNIX aggiungendoli, modificandoli o eliminandoli.

Fasi

1. In System Manager, visualizzare l'elenco dei gruppi UNIX. Fare riferimento a [Visualizzare utenti e gruppi UNIX](#).
2. Nella scheda **gruppi**, è possibile gestire i gruppi con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
-------------------------------	------------------------------




Aggiungere un gruppo	<ol style="list-style-type: none"> 1. Fare clic su  Add . 2. Inserire le informazioni del gruppo. 3. (Facoltativo) specificare gli utenti associati.
Modificare un gruppo	<ol style="list-style-type: none"> 1. Selezionare il gruppo. 2. Fare clic su  Edit . 3. Modificare le informazioni del gruppo. 4. (Facoltativo) aggiungere o rimuovere utenti.
Eliminare un gruppo	<ol style="list-style-type: none"> 1. Selezionare il gruppo o i gruppi che si desidera eliminare. 2. Fare clic su  Delete .

Gestire gli utenti UNIX

In System Manager, è possibile gestire gli utenti Windows aggiungendoli, modificandoli o eliminandoli.

Fasi

1. In System Manager, visualizzare l'elenco degli utenti per il gruppo. Fare riferimento a. [Visualizzare utenti e gruppi UNIX](#).
2. Nella scheda **utenti**, è possibile gestire gli utenti con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un utente	<ol style="list-style-type: none"> 1. Fare clic su  Add . 2. Inserire le informazioni dell'utente.
Modificare un utente	<ol style="list-style-type: none"> 1. Selezionare l'utente che si desidera modificare. 2. Fare clic su  Edit . 3. Modificare le informazioni dell'utente.
Eliminare un utente	<ol style="list-style-type: none"> 1. Selezionare l'utente o gli utenti che si desidera eliminare. 2. Fare clic su  Delete .

Monitorare i client attivi NFS

A partire da ONTAP 9.8, System Manager mostra quali connessioni client NFS sono attive quando NFS viene concesso in licenza su un cluster.

Ciò consente di verificare rapidamente quali client NFS si connettono attivamente a una VM di storage, che sono connessi ma inattivi e che sono disconnessi.

Per ogni indirizzo IP del client NFS, il display **NFS Clients** mostra: * Ora dell'ultimo accesso * Indirizzo IP dell'interfaccia di rete * versione della connessione NFS * Nome della Storage VM

Inoltre, un elenco dei client NFS attivi nelle ultime 48 ore viene visualizzato anche nella schermata **Storage>Volumes** e un numero di client NFS viene incluso nella schermata **Dashboard**.

Fase

1. Visualizzare l'attività del client NFS: Fare clic su **hosts > NFS Clients**.

Abilitare lo storage NAS

Abilitare lo storage NAS per i server Linux utilizzando NFS



Creare o modificare le VM di storage per abilitare i server NFS per la distribuzione dei dati ai client Linux.

Questa procedura abilita una VM di storage nuova o esistente per il protocollo NFS. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.



Fasi

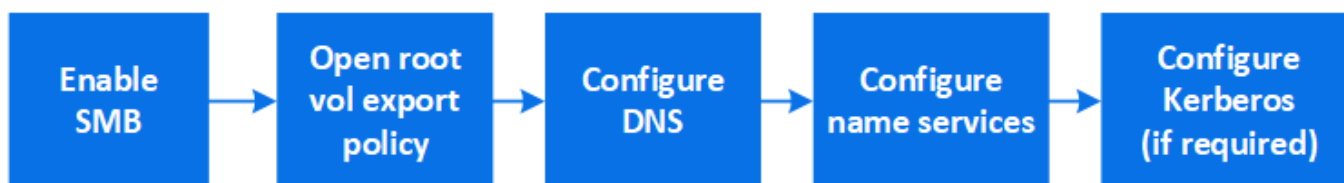
1. Abilitare NFS su una VM di storage.
 - a. Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VMS**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3**, selezionare **Enable NFS** (attiva NFS).
 - Confermare la lingua predefinita.
 - Aggiungere interfacce di rete.
 - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
 - b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **NFS**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
 - a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name _root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
 - b. Fare clic su **Aggiungi** per aggiungere una regola.
 - Specifica del client = 0.0.0.0/0
 - Access Protocol (protocolli di accesso) = NFS
 - Dettagli di accesso = UNIX di sola lettura
3. Configurare DNS for host-name resolution (Configura DNS per la risoluzione del nome host): Fare clic su **Storage > Storage VMS**, selezionare la VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **DNS**.
4. Configurare i name service secondo necessità.
 - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  LDAP o NIS.

- b. Includere eventuali modifiche nel file name Services switch: Fare clic su  Nel riquadro Name Services Switch.
5. Configurare Kerberos se necessario:
 - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, quindi fare clic su **Settings** (Impostazioni).
 - b. Fare clic su  Nel riquadro Kerberos, quindi fare clic su **Aggiungi**.


Abilitare lo storage NAS per i server Windows utilizzando SMB

Creare o modificare le VM di storage per consentire ai server SMB di fornire dati ai client Windows.

Questa procedura consente di abilitare una VM di storage nuova o esistente per il protocollo SMB. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.



Fasi

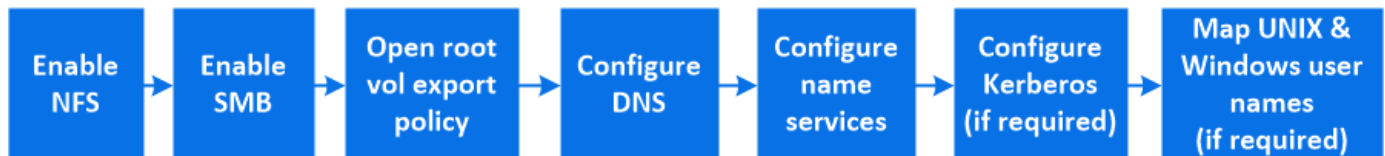
1. Abilitare SMB su una VM di storage.
 - a. Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VM**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3** selezionare **Enable SMB/CIFS** (attiva SMB/CIFS).
 - Inserire le seguenti informazioni:
 - Nome e password dell'amministratore
 - Nome del server
 - Dominio Active Directory
 - Confermare l'unità organizzativa.
 - Confermare i valori DNS.
 - Confermare la lingua predefinita.
 - Aggiungere interfacce di rete.
 - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
 - b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **SMB**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
 - a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name_root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
 - b. Fare clic su **Aggiungi** per aggiungere una regola.
 - Specifica del client = 0.0.0.0/0
 - Access Protocol (protocolli di accesso) = SMB

- Dettagli di accesso = NTFS di sola lettura
3. Configurare il DNS per la risoluzione del nome host:
 - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **DNS**.
 - b. Passare al server DNS e mappare il server SMB.
 - Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dell'interfaccia di rete dati.
 - Se si utilizzano alias NetBIOS, creare una voce di ricerca alias canonical name (CNAME resource record) per associare ciascun alias all'indirizzo IP dell'interfaccia di rete dati del server SMB.
 4. Configurare i name service secondo necessità
 - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **LDAP o NIS**.
 - b. Includere eventuali modifiche nel file name Services switch: Fare clic su  Sotto **Name Services Switch**.
 5. Configurare Kerberos se necessario:
 - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, quindi fare clic su **Settings** (Impostazioni).
 - b. Fare clic su  In **Kerberos**, quindi fare clic su **Aggiungi**.

Abilitare lo storage NAS per Windows e Linux utilizzando sia NFS che SMB








Creare o modificare le VM di storage per consentire ai server NFS e SMB di fornire dati ai client Linux e Windows.

Questa procedura consente a una VM di storage nuova o esistente di servire protocolli NFS e SMB. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.



Fasi

1. Abilitare NFS e SMB su una VM di storage.
 - a. Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VMS**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3**, selezionare **Enable SMB/CIFS** (attiva SMB/CIFS*) e **Enable NFS** (attiva NFS*).
 - Inserire le seguenti informazioni:
 - Nome e password dell'amministratore
 - Nome del server
 - Dominio Active Directory
 - Confermare l'unità organizzativa.
 - Confermare i valori DNS.

- Confermare la lingua predefinita.
 - Aggiungere interfacce di rete.
 - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
- b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, quindi fare clic su **Settings** (Impostazioni). Se NFS o SMB non sono già abilitati, completare i seguenti passaggi secondari.
- Fare clic su  Sotto **NFS**.
 - Fare clic su  Sotto **SMB**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
- a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name_root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
- b. Fare clic su **Aggiungi** per aggiungere una regola.
- Specifica del client = 0.0.0.0/0
 - Access Protocol (protocolli di accesso) = NFS
 - Dettagli di accesso = NFS di sola lettura
3. Configurare il DNS per la risoluzione del nome host:
- a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **DNS**.
- b. Una volta completata la configurazione DNS, passare al server DNS e mappare il server SMB.
- Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dell'interfaccia di rete dati.
 - Se si utilizzano alias NetBIOS, creare una voce di ricerca alias canonical name (CNAME resource record) per associare ciascun alias all'indirizzo IP dell'interfaccia di rete dati del server SMB.
4. Configurare i name service secondo necessità:
- a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Per LDAP o NIS.
- b. Includere eventuali modifiche nel file name Services switch: Fare clic su  Sotto **Name Services Switch**.
5. Configurare Kerberos se necessario: Fare clic su  Nel riquadro Kerberos, quindi fare clic su **Aggiungi**.
6. Se necessario, mappare i nomi utente UNIX e Windows: Fare clic su  In **mappatura nome** e fare clic su **Aggiungi**.

Utilizzare questa procedura solo se il sito dispone di account utente Windows e UNIX che non vengono mappati implicitamente, ovvero quando la versione minuscola di ciascun nome utente Windows corrisponde al nome utente UNIX. Questa procedura può essere eseguita utilizzando LDAP, NIS o utenti locali. Se si dispone di due set di utenti che non corrispondono, è necessario configurare la mappatura dei nomi.

Configurare NFS con la CLI

Panoramica della configurazione di NFS con la CLI

È possibile utilizzare i comandi CLI di ONTAP 9 per configurare l'accesso del client NFS

ai file contenuti in un nuovo volume o qtree in una macchina virtuale di storage (SVM) nuova o esistente.

Attenersi alle seguenti procedure se si desidera configurare l'accesso a un volume o a un qtree nel modo seguente:

- Si desidera utilizzare qualsiasi versione di NFS attualmente supportata da ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2 o NFSv4.1 con pNFS.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Per utilizzare System Manager per configurare l'accesso multiprotocollo NAS, vedere ["Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB"](#).

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.

I dettagli sulla sintassi dei comandi sono disponibili nelle pagine guida CLI e man ONTAP.

- Per proteggere il nuovo volume verranno utilizzate le autorizzazioni per i file UNIX.
- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

Per ulteriori informazioni sulla gamma di funzionalità del protocollo NFS ONTAP, consultare ["Panoramica di riferimento di NFS"](#).

Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Fare riferimento a...
System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive)	"Provisioning dello storage NAS per i server Linux utilizzando NFS"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica della configurazione di NFS"

Workflow di configurazione NFS

La configurazione di NFS implica la valutazione dei requisiti di storage fisico e di rete e la scelta di un workflow specifico per il tuo obiettivo: Configurare l'accesso NFS a una SVM nuova o esistente oppure aggiungere un volume o qtree a una SVM esistente già completamente configurata per l'accesso NFS.

Preparazione

Valutare i requisiti di storage fisico

Prima di eseguire il provisioning dello storage NFS per i client, è necessario assicurarsi che vi sia spazio sufficiente in un aggregato esistente per il nuovo volume. In caso contrario, è possibile aggiungere dischi a un aggregato esistente o creare un nuovo aggregato del tipo desiderato.

Fasi

1. Visualizzare lo spazio disponibile negli aggregati esistenti:

```
storage aggregate show
```

Se esiste un aggregato con spazio sufficiente, registrare il nome nel foglio di lavoro.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

2. Se non sono presenti aggregati con spazio sufficiente, aggiungere dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

Informazioni correlate

["Concetti di ONTAP"](#)

Valutare i requisiti di rete

Prima di fornire storage NFS ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning NFS.

Di cosa hai bisogno

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

Fasi

1. Visualizzare le porte fisiche e virtuali disponibili:

```
network port show
```

- Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
- Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.

2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti: +

```
network subnet show
```

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

3. Visualizzare gli spazi IP disponibili:

```
network ipspace show
```

È possibile utilizzare l'IPSpace predefinito o un IPSpace personalizzato.

4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster:

```
network options ipv6 show
```

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

Decidere dove eseguire il provisioning della nuova capacità di storage NFS

Prima di creare un nuovo volume o qtree NFS, è necessario decidere se posizionarlo in una SVM nuova o esistente e la quantità di configurazione richiesta da SVM. Questa decisione determina il tuo flusso di lavoro.

Scelte

- Se si desidera eseguire il provisioning di un volume o qtree su una nuova SVM o su una SVM esistente con NFS abilitato ma non configurato, completare la procedura descritta in "Configurazione dell'accesso NFS a una SVM" e "aggiunta dello storage NFS a una SVM abilitata per NFS".

[Configurare l'accesso NFS a una SVM](#)

[Aggiungere storage NFS a una SVM abilitata per NFS](#)

È possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando NFS su un cluster per la prima volta.
- Esistono SVM in un cluster in cui non si desidera attivare il supporto NFS.
- Si dispone di una o più SVM abilitate NFS in un cluster e si desidera un altro server NFS in uno spazio dei nomi isolato (scenario multi-tenancy). È inoltre necessario scegliere questa opzione per eseguire il provisioning dello storage su una SVM esistente che ha NFS attivato ma non configurato. Questo potrebbe verificarsi se è stata creata la SVM per l'accesso SAN o se non sono stati attivati protocolli al momento della creazione della SVM.

Dopo aver attivato NFS su SVM, procedere con il provisioning di un volume o qtree.

- Se si desidera eseguire il provisioning di un volume o qtree su una SVM esistente completamente configurata per l'accesso NFS, completare la procedura descritta in "aggiunta dello storage NFS a una SVM abilitata per NFS".

[Aggiunta di storage NFS a una SVM abilitata per NFS](#)

Foglio di lavoro per la raccolta delle informazioni di configurazione NFS

Il foglio di lavoro per la configurazione di NFS consente di raccogliere le informazioni necessarie per impostare l'accesso NFS per i client.

Completare una o entrambe le sezioni del foglio di lavoro in base alla decisione presa in merito al provisioning dello storage:

Se si configura l'accesso NFS a una SVM, completare entrambe le sezioni.

- Configurazione dell'accesso NFS a una SVM
- Aggiunta di capacità di storage a una SVM abilitata per NFS

Se si aggiunge capacità di storage a una SVM abilitata per NFS, è necessario completare solo:

- Aggiunta di capacità di storage a una SVM abilitata per NFS

Per ulteriori informazioni sui parametri, consultare le pagine man dei comandi.

Configurare l'accesso NFS a una SVM

Parametri per la creazione di una SVM

Questi valori vengono forniti con `vserver create` Se si sta creando una nuova SVM.


Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Un nome fornito per la nuova SVM che sia un nome di dominio completo (FQDN) o che segua un'altra convenzione che applica nomi SVM univoci in un cluster.	
<code>-aggregate</code>	Il nome di un aggregato nel cluster con spazio sufficiente per la nuova capacità di storage NFS.	
<code>-rootvolume</code>	Un nome univoco fornito per il volume root SVM.	
<code>-rootvolume-security-style</code>	Utilizzare lo stile di sicurezza UNIX per SVM.	<code>unix</code>

-language	Utilizzare l'impostazione della lingua predefinita in questo flusso di lavoro.	C.UTF-8
ipspace	Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono (macchine virtuali di storage (SVM)).	

Parametri per la creazione di un server NFS

Questi valori vengono forniti con `vserver nfs create` Quando si crea un nuovo server NFS e si specificano le versioni NFS supportate.

Se si attiva NFSv4 o versioni successive, è necessario utilizzare LDAP per una maggiore protezione.

Campo	Descrizione	Il tuo valore
-v3, -v4.0, -v4.1, -v4.1-pnfs	<p>Abilitare le versioni NFS in base alle esigenze.</p> <div>  <p>La versione 4.2 è supportata anche in ONTAP 9.8 e versioni successive quando v4.1 è attivato.</p> </div>	
-v4-id-domain	Nome di dominio di mappatura ID.	
-v4-numeric-ids	Supporto per ID proprietari numerici (abilitati o disabilitati).	

Parametri per la creazione di una LIF

Questi valori vengono forniti con `network interface create` Durante la creazione di LIF.

Se si utilizza Kerberos, è necessario attivare Kerberos su più LIF.

Campo	Descrizione	Il tuo valore
-lif	Un nome fornito per il nuovo LIF.	
-role	Utilizza il ruolo LIF dei dati in questo flusso di lavoro.	data
-data-protocol	Utilizzare solo il protocollo NFS in questo flusso di lavoro.	nfs

<code>-home-node</code>	Il nodo a cui la LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-home-port</code>	La porta o il gruppo di interfacce a cui LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-address</code>	L'indirizzo IPv4 o IPv6 del cluster che verrà utilizzato per l'accesso ai dati dal nuovo LIF.	
<code>-netmask</code>	La maschera di rete e il gateway per LIF.	
<code>-subnet</code>	Un pool di indirizzi IP. Utilizzato al posto di <code>-address</code> e <code>-netmask</code> per assegnare automaticamente indirizzi e netmask.	
<code>-firewall-policy</code>	Utilizzare la policy predefinita del firewall dati in questo flusso di lavoro.	data

Parametri per la risoluzione del nome host DNS

Questi valori vengono forniti con `vserver services name-service dns create` Durante la configurazione del DNS.

Campo	Descrizione	Il tuo valore
<code>-domains</code>	Fino a cinque nomi di dominio DNS.	
<code>-name-servers</code>	Fino a tre indirizzi IP per ciascun server dei nomi DNS.	

Indicare le informazioni sul servizio

Parametri per la creazione di utenti locali

Questi valori vengono forniti se si creano utenti locali utilizzando `vserver services name-service unix-user create` comando. Se si configurano utenti locali caricando un file contenente utenti UNIX da un URI (Uniform Resource Identifier), non è necessario specificare questi valori manualmente.

	Nome utente (<code>-user</code>)	ID utente (<code>-id</code>)	ID gruppo (<code>-primary-gid</code>)	Nome completo (<code>-full-name</code>)
--	------------------------------------	--------------------------------	---	---

Esempio	johnm	123	100	John Miller
1				
2				
3				
...				
n				

Parametri per la creazione di gruppi locali

Questi valori vengono forniti se si creano gruppi locali utilizzando `vserver services name-service unix-group create` comando. Se si configurano gruppi locali caricando un file contenente gruppi UNIX da un URI, non è necessario specificare questi valori manualmente.

	Nome del gruppo (-name)	ID gruppo (-id)
Esempio	Progettazione	100
1		
2		
3		
...		
n		

Parametri per NIS

Questi valori vengono forniti con `vserver services name-service nis-domain create` comando.



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.

Campo	Descrizione	Il tuo valore
<code>-domain</code>	Il dominio NIS che SVM utilizzerà per la ricerca dei nomi.	
<code>-active</code>	Il server di dominio NIS attivo.	true oppure false

<code>-servers</code>	ONTAP 9.0, 9.1: Uno o più indirizzi IP dei server NIS utilizzati dalla configurazione del dominio NIS.	
<code>-nis-servers</code>	ONTAP 9.2: Un elenco separato da virgole di indirizzi IP e nomi host per i server NIS utilizzati dalla configurazione del dominio.	

Parametri per LDAP

Questi valori vengono forniti con `vserver services name-service ldap client create` comando.

È inoltre necessario un certificato CA principale autofirmato `.pem` file.



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

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM per la quale si desidera creare una configurazione del client LDAP.	
<code>-client-config</code>	Il nome assegnato per la nuova configurazione del client LDAP.	
<code>-servers</code>	ONTAP 9.0, 9.1: Uno o più server LDAP in base all'indirizzo IP in un elenco separato da virgole.	
<code>-ldap-servers</code>	ONTAP 9.2: Un elenco separato da virgole di indirizzi IP e nomi host per i server LDAP.	
<code>-query-timeout</code>	Utilizzare l'impostazione predefinita 3 secondi per questo flusso di lavoro.	3
<code>-min-bind-level</code>	Il livello minimo di autenticazione BIND. L'impostazione predefinita è <code>anonymous</code> . Deve essere impostato su <code>sasl</code> se la firma e il sigillo sono configurati.	
<code>-preferred-ad-servers</code>	Uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole.	

Campo	Descrizione	Il tuo valore
-ad-domain	Il dominio Active Directory.	
-schema	Modello di schema da utilizzare. È possibile utilizzare uno schema predefinito o personalizzato.	
-port	Utilizzare la porta predefinita del server LDAP 389 per questo flusso di lavoro.	389
-bind-dn	Il nome distinto dell'utente Bind.	
-base-dn	Il nome distinto di base. L'impostazione predefinita è "" (root).	
-base-scope	Utilizzare l'ambito di ricerca di base predefinito subnet per questo flusso di lavoro.	subnet
-session-security	Attiva la firma o la firma LDAP e il sealing. L'impostazione predefinita è none.	
-use-start-tls	Attiva LDAP su TLS. L'impostazione predefinita è false.	

Parametri per l'autenticazione Kerberos

Questi valori vengono forniti con `vserver nfs kerberos realm create` comando. Alcuni valori variano a seconda che si utilizzi Microsoft Active Directory come server KDC (Key Distribution Center) o MIT o altro server KDC UNIX.

Campo	Descrizione	Il tuo valore
-vserver	SVM che comunicherà con il KDC.	
-realm	L'area di autenticazione Kerberos.	
-clock-skew	Disallineamento del clock consentito tra client e server.	
-kdc-ip	Indirizzo IP KDC.	

<code>-kdc-port</code>	Numero della porta KDC.	
<code>-adserver-name</code>	Solo Microsoft KDC: Nome DEL server AD.	
<code>-adserver-ip</code>	Solo Microsoft KDC: Indirizzo IP DEL SERVER AD.	
<code>-adminserver-ip</code>	Solo KDC UNIX: Indirizzo IP del server di amministrazione.	
<code>-adminserver-port</code>	Solo KDC UNIX: Numero di porta del server di amministrazione.	
<code>-passwordserver-ip</code>	Solo KDC UNIX: Indirizzo IP del server delle password.	
<code>-passwordserver-port</code>	Solo KDC UNIX: Porta del server delle password.	
<code>-kdc-vendor</code>	Vendor KDC.	{ Microsoft
Other }	<code>-comment</code>	Eventuali commenti desiderati.

Questi valori vengono forniti con `vserver nfs kerberos interface enable` comando.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM per la quale si desidera creare una configurazione Kerberos.	
<code>-lif</code>	I dati LIF sui quali attivare Kerberos. È possibile attivare Kerberos su più LIF.	
<code>-spn</code>	Nome del principio di servizio (SPN)	
<code>-permitted-enc-types</code>	I tipi di crittografia consentiti per Kerberos su NFS; <code>aes-256</code> è consigliato, a seconda delle funzionalità del client.	

-admin-username	Le credenziali dell'amministratore KDC per recuperare la chiave segreta SPN direttamente dal KDC. È richiesta una password	
-keytab-uri	Il file keytab del KDC contenente la chiave SPN se non si dispone delle credenziali di amministratore KDC.	
-ou	L'unità organizzativa (OU) in base alla quale verrà creato l'account server Microsoft Active Directory quando si attiva Kerberos utilizzando un realm per Microsoft KDC.	

Aggiunta di capacità di storage a una SVM abilitata per NFS

Parametri per la creazione di policy e regole di esportazione

Questi valori vengono forniti con `vserver export-policy create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM che ospiterà il nuovo volume.	
-policyname	Nome fornito per una nuova policy di esportazione.	

Questi valori vengono forniti per ogni regola con `vserver export-policy rule create` comando.

Campo	Descrizione	Il tuo valore
-clientmatch	Specifica di corrispondenza del client.	
-ruleindex	Posizione della regola di esportazione nell'elenco delle regole.	
-protocol	Utilizza NFS in questo flusso di lavoro.	nfs
-rorule	Metodo di autenticazione per l'accesso in sola lettura.	

<code>-rwrule</code>	Metodo di autenticazione per l'accesso in lettura/scrittura.	
<code>-superuser</code>	Metodo di autenticazione per l'accesso del superutente.	
<code>-anon</code>	ID utente a cui sono mappati gli utenti anonimi.	

È necessario creare una o più regole per ciascun criterio di esportazione.

-ruleindex	-clientmatch	-rorule	-rwrule	-superuser	-anon
Esempi	0.0.0.0/0,@rootaccess_netgroup	qualsiasi	krb5	sis	65534
1					
2					
3					
...					
n					

Parametri per la creazione di un volume

Questi valori vengono forniti con `volume create` se si sta creando un volume invece di un qtree.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome di una SVM nuova o esistente che ospiterà il nuovo volume.	
<code>-volume</code>	Un nome descrittivo univoco fornito per il nuovo volume.	
<code>-aggregate</code>	Il nome di un aggregato nel cluster con spazio sufficiente per il nuovo volume NFS.	
<code>-size</code>	Un numero intero fornito per le dimensioni del nuovo volume.	

-user	Nome o ID dell'utente impostato come proprietario della directory principale del volume.	
-group	Nome o ID del gruppo impostato come proprietario della directory principale del volume.	
--security-style	USA lo stile di sicurezza UNIX per questo flusso di lavoro.	unix
-junction-path	Posizione sotto root (/) dove deve essere montato il nuovo volume.	
-export-policy	Se si intende utilizzare un criterio di esportazione esistente, è possibile immetterne il nome al momento della creazione del volume.	

Parametri per la creazione di un qtree

Questi valori vengono forniti con `volume qtree create` se si sta creando un qtree invece di un volume.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui risiede il volume contenente il qtree.	
-volume	Il nome del volume che conterrà il nuovo qtree.	
-qtree	Un nome descrittivo univoco fornito per il nuovo qtree, massimo 64 caratteri.	
-qtree-path	L'argomento del percorso qtree nel formato <code>/vol/volume_name/qtree_name\></code> può essere specificato invece di specificare volume e qtree come argomenti separati.	
-unix-permissions	Facoltativo: I permessi UNIX per qtree.	

-export-policy	Se si intende utilizzare un criterio di esportazione esistente, è possibile immetterne il nome al momento della creazione del qtree.	
----------------	--	--

Configurare l'accesso NFS a una SVM

Creare una SVM

Se non si dispone di almeno una SVM in un cluster per fornire l'accesso ai dati ai client NFS, è necessario crearne una.

Prima di iniziare

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

Fasi

1. Creare una SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
ipspace_name
```

- Utilizzare l'impostazione UNIX per `-rootvolume-security-style` opzione.
- Utilizzare il C.UTF-8 predefinito `-language` opzione.
- Il `ipspace` l'impostazione è facoltativa.

2. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver vserver_name
```

Il Allowed Protocols Il campo deve includere NFS. È possibile modificare questo elenco in un secondo momento.

Il Vserver Operational State il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPspace ipspaceA:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspaces ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione.

```
cluster1::> vservers show -vservers vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

Verificare che il protocollo NFS sia attivato su SVM

Prima di poter configurare e utilizzare NFS su SVM, è necessario verificare che il

protocollo sia attivato.

A proposito di questa attività

Questa operazione viene generalmente eseguita durante l'installazione di SVM, ma se il protocollo non è stato attivato durante l'installazione, è possibile attivarlo in un secondo momento utilizzando `vserver add-protocols` comando.



Una volta creato, non è possibile aggiungere o rimuovere un protocollo da un LIF.

È inoltre possibile disattivare i protocolli sulle SVM utilizzando `vserver remove-protocols` comando.

Fasi

1. Controllare quali protocolli sono attualmente attivati e disattivati per SVM:

```
vserver show -vserver vserver_name -protocols
```

È inoltre possibile utilizzare `vserver show-protocols` Per visualizzare i protocolli attualmente abilitati su tutte le SVM nel cluster.

2. Se necessario, attivare o disattivare un protocollo:

- ° Per attivare il protocollo NFS:

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- ° Per disattivare un protocollo:

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name  
[,protocol_name,...]
```

3. Verificare che i protocolli attivati e disattivati siano stati aggiornati correttamente:

```
vserver show -vserver vserver_name -protocols
```

Esempio

Il seguente comando visualizza i protocolli attualmente attivati e disattivati (consentiti e non consentiti) sulla SVM denominata vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
```

Vserver	Allowed Protocols	Disallowed Protocols
vs1.example.com	nfs	cifs, fcp, iscsi, ndmp

Il seguente comando consente l'accesso tramite NFS aggiungendo `nfs` All'elenco dei protocolli abilitati sulla SVM denominato vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Aprire la policy di esportazione del volume root SVM

Il criterio di esportazione predefinito del volume root SVM deve includere una regola per

consentire a tutti i client l'accesso aperto tramite NFS. Senza tale regola, a tutti i client NFS viene negato l'accesso a SVM e ai suoi volumi.

A proposito di questa attività

Quando viene creata una nuova SVM, viene creata automaticamente una policy di esportazione predefinita (chiamata predefinita) per il volume root della SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM.

Verificare che l'accesso sia aperto a tutti i client NFS nel criterio di esportazione predefinito e, in seguito, limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per singoli volumi o qtree.

Fasi

1. Se si utilizza una SVM esistente, controllare il criterio di esportazione del volume root predefinito:

```
vserver export-policy rule show
```

L'output del comando dovrebbe essere simile a quanto segue:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Se esiste una regola di questo tipo che consente l'accesso aperto, questa attività è completa. In caso contrario, passare alla fase successiva.

2. Creare una regola di esportazione per il volume root SVM:

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Se la SVM contiene solo volumi protetti da Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e `-superuser` per il volume root a `krb5` oppure `krb5i`. Ad esempio:

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. Verificare la creazione della regola utilizzando `vserver export-policy rule show` comando.

Risultato

Qualsiasi client NFS può ora accedere a qualsiasi volume o qtree creato su SVM.

Creare un server NFS

Dopo aver verificato che NFS sia concesso in licenza sul cluster, è possibile utilizzare `vserver nfs create` Per creare un server NFS su SVM e specificare le versioni NFS supportate.

A proposito di questa attività

SVM può essere configurato per supportare una o più versioni di NFS. Se si supporta NFSv4 o versioni successive:

- Il nome del dominio di associazione ID utente NFSv4 deve essere lo stesso sul server NFSv4 e sui client di destinazione.

Non è necessario che sia uguale a un nome di dominio LDAP o NIS, purché il server NFSv4 e i client utilizzino lo stesso nome.

- I client di destinazione devono supportare l'impostazione NFSv4 Numeric ID (ID numerico NFSv4).
- Per motivi di sicurezza, è necessario utilizzare LDAP per i name service nelle implementazioni NFSv4.

Prima di iniziare

La SVM deve essere stata configurata per consentire il protocollo NFS.

Fasi

1. Verificare che NFS sia concesso in licenza sul cluster:

```
system license show -package nfs
```

In caso contrario, contattare il rappresentante commerciale.

2. Creare un server NFS:

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0  
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids  
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

Puoi scegliere di abilitare qualsiasi combinazione di versioni NFS. Se si desidera supportare pNFS, è necessario abilitare entrambi `-v4.1` e `-v4.1-pnfs` opzioni.

Se si attiva la versione 4 o successiva, assicurarsi che le seguenti opzioni siano impostate correttamente:

- `-v4-id-domain`

Questo parametro opzionale specifica la parte di dominio del formato stringa dei nomi utente e gruppo, come definito dal protocollo NFSv4. Per impostazione predefinita, ONTAP utilizza il dominio NIS se impostato; in caso contrario, viene utilizzato il dominio DNS. Specificare un valore corrispondente al nome di dominio utilizzato dai client di destinazione.

- `-v4-numeric-ids`

Questo parametro opzionale specifica se il supporto per gli identificatori di stringa numerici negli attributi del proprietario NFSv4 è attivato. L'impostazione predefinita è attivata, ma è necessario

verificare che i client di destinazione lo supportino.

È possibile abilitare ulteriori funzionalità NFS in un secondo momento utilizzando `vserver nfs modify` comando.

3. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver vserver_name
```

4. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver vserver_name
```

Esempi

Il seguente comando crea un server NFS sulla SVM denominata `vs1` con NFSv3 e NFSv4.0 abilitati:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

I seguenti comandi verificano lo stato e i valori di configurazione del nuovo server NFS denominato `vs1`:

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
Vserver: vs1  
General NFS Access: true  
NFS v3: enabled  
NFS v4.0: enabled  
UDP Protocol: enabled  
TCP Protocol: enabled  
Default Windows User: -  
NFSv4.0 ACL Support: disabled  
NFSv4.0 Read Delegation Support: disabled  
NFSv4.0 Write Delegation Support: disabled  
NFSv4 ID Mapping Domain: my_domain.com  
...
```

Creare una LIF

LIF è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

Di cosa hai bisogno

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se si utilizza l'autenticazione Kerberos, attivare Kerberos su più LIF.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

A partire da ONTAP 9.4, FC-NVMe è supportato. Se si sta creando una LIF FC-NVMe, tenere presente quanto segue:

- Il protocollo NVMe deve essere supportato dall'adattatore FC su cui viene creato il LIF.
- FC-NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare un LIF che gestisca il traffico di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.
- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- È possibile configurare un solo NVMe LIF che gestisce il traffico dati per SVM

Fasi

1. Creare una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

Opzione	Descrizione
ONTAP 9.5 e versioni precedenti	<code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>

ONTAP 9.6 e versioni successive	<code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>

- Il `-role` Il parametro non è necessario quando si crea una LIF utilizzando una policy di servizio (a partire da ONTAP 9.6).
- Il `-data-protocol` Il parametro deve essere specificato al momento della creazione della LIF e non può essere modificato in seguito senza distruggere e ricreare la LIF dei dati.

Il `-data-protocol` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6).

- `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- `-home-port` È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.

2. Verificare che la LIF sia stata creata correttamente utilizzando `network interface show` comando.
3. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

4. Se si utilizza Kerberos, ripetere i passaggi da 1 a 3 per creare ulteriori LIF.

Kerberos deve essere attivato separatamente su ciascuno di questi LIF.

Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF `datalif1` e `datalif3` sono configurati con indirizzi IPv4 e `datalif4` è configurato con un indirizzo IPv6:

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	clus1	up/up	192.0.2.12/24	node-1	e0a
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2					
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c
5 entries were displayed.					

Il comando seguente mostra come creare una LIF dati NAS assegnata a default-data-files politica di servizio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

Abilitare il DNS per la risoluzione del nome host

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host

vengono risolti utilizzando server DNS esterni.

Di cosa hai bisogno

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

A proposito di questa attività

La *Guida alla gestione della rete* contiene informazioni sulla configurazione del DNS dinamico sulla SVM.

Fasi

1. Abilitare il DNS sulla SVM:

```
vserver services name-service dns create -vserver vserver_name -domains
domain_name -name-servers ip_addresses -state enabled
```

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partire da ONTAP 9.2, la `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

2. Visualizzare le configurazioni del dominio DNS utilizzando `vserver services name-service dns show` comando.

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check` comando.

Il `vserver services name-service dns check` Il comando è disponibile a partire da ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
-----	-----	-----	
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Configurare i name service

Panoramica sulla configurazione dei name service

A seconda della configurazione del sistema storage, ONTAP deve essere in grado di cercare informazioni su host, utenti, gruppi o netgroup per fornire un accesso appropriato ai client. Per ottenere queste informazioni, è necessario configurare i name service per consentire a ONTAP di accedere ai name service locali o esterni.

È necessario utilizzare un servizio di nomi come NIS o LDAP per facilitare la ricerca dei nomi durante l'autenticazione del client. Si consiglia di utilizzare LDAP quando possibile per una maggiore sicurezza, in particolare durante l'implementazione di NFSv4 o versioni successive. È inoltre necessario configurare utenti e gruppi locali nel caso in cui i server dei nomi esterni non siano disponibili.

Le informazioni del servizio di nome devono essere mantenute sincronizzate su tutte le origini.

Configurare la tabella name service switch

È necessario configurare correttamente la tabella dello switch del name service per consentire a ONTAP di consultare i name service locali o esterni per recuperare le informazioni di mappatura di host, utenti, gruppi, netgroup o nomi.

Di cosa hai bisogno

È necessario decidere quali servizi di nomi utilizzare per la mappatura di host, utenti, gruppi, netgroup o nomi, in base all'ambiente in uso.

Se si intende utilizzare netgroup, tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compressi come specificato in RFC 5952.

A proposito di questa attività

Non includere fonti di informazioni che non vengono utilizzate. Ad esempio, se NIS non viene utilizzato nell'ambiente, non specificare `-sources nis` opzione.

Fasi

1. Aggiungere le voci necessarie alla tabella dei name service switch:

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Verificare che la tabella name service switch contenga le voci previste nell'ordine desiderato:

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

Se si desidera apportare delle correzioni, è necessario utilizzare `vserver services name-service ns-switch modify` oppure `vserver services name-service ns-switch delete` comandi.

Esempio

Nell'esempio riportato di seguito viene creata una nuova voce nella tabella name service switch per SVM vs1 che utilizza il file netgroup locale e un server NIS esterno per cercare le informazioni del netgroup in tale ordine:

```
cluster::> vserver services name-service ns-switch create -vserver vs1  
-database netgroup -sources files,nis
```

Al termine

- Per consentire l'accesso ai dati, è necessario configurare i name service specificati per SVM.
- Se si elimina un servizio di nomi per SVM, è necessario rimuoverlo anche dalla tabella di switch del servizio di nomi.

L'accesso del client al sistema di storage potrebbe non funzionare come previsto, se non si riesce a eliminare il name service dalla tabella di switch del name service.

Configurare utenti e gruppi UNIX locali

Panoramica sulla configurazione di utenti e gruppi UNIX locali

È possibile utilizzare utenti e gruppi UNIX locali su SVM per l'autenticazione e la mappatura dei nomi. È possibile creare manualmente utenti e gruppi UNIX oppure caricare un file contenente utenti o gruppi UNIX da un URI (Uniform Resource Identifier).

Per impostazione predefinita, è previsto un limite massimo di 32,768 gruppi di utenti UNIX locali e membri del gruppo combinati nel cluster. L'amministratore del cluster può modificare questo limite.

Creare un utente UNIX locale

È possibile utilizzare `vserver services name-service unix-user create` Per creare utenti UNIX locali. Un utente UNIX locale è un utente UNIX creato sull'opzione SVM as a UNIX name service da utilizzare nell'elaborazione delle mappature dei nomi.

Fase

1. Creare un utente UNIX locale:

```
vserver services name-service unix-user create -vserver vserver_name -user  
user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` specifica il nome utente. La lunghezza del nome utente deve essere pari o inferiore a 64 caratteri.

`-id integer` Specifica l'ID utente assegnato.

`-primary-gid integer` Specifica l'ID del gruppo primario. In questo modo l'utente viene aggiunto al gruppo primario. Dopo aver creato l'utente, è possibile aggiungerlo manualmente a qualsiasi altro gruppo desiderato.

Esempio

Il seguente comando crea un utente UNIX locale denominato johnm (nome completo "John Miller") sulla SVM denominata vs1. L'utente ha l'ID 123 e l'ID del gruppo primario 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user  
johnm -id 123  
-primary-gid 100 -full-name "John Miller"
```

Caricare utenti UNIX locali da un URI

In alternativa alla creazione manuale di singoli utenti UNIX locali in SVM, è possibile semplificare l'attività caricando un elenco di utenti UNIX locali in SVM da un URI (Uniform Resource Identifier) (`vserver services name-service unix-user load-from-uri`).

Fasi

1. Creare un file contenente l'elenco degli utenti UNIX locali che si desidera caricare.

Il file deve contenere informazioni sull'utente in UNIX `/etc/passwd` formato:

```
user_name: password: user_ID: group_ID: full_name
```

Il comando elimina il valore di `password` e i valori dei campi dopo `full_name` campo (`home_directory` e `shell`).

Le dimensioni massime supportate dei file sono 2.5 MB.

2. Verificare che l'elenco non contenga informazioni duplicate.

Se l'elenco contiene voci duplicate, il caricamento dell'elenco non riesce e viene visualizzato un messaggio di errore.

3. Copiare il file su un server.

Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

5. Caricare il file contenente l'elenco degli utenti UNIX locali nelle SVM dall'URI:

```
vserver services name-service unix-user load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true false}` specifica se sovrascrivere le voci. L'impostazione predefinita è `false`.

Esempio

Il seguente comando carica un elenco di utenti UNIX locali dall'URI `ftp://ftp.example.com/passwd` Nella SVM denominata `vs1`. Gli utenti esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/passwd -overwrite false
```

Creare un gruppo UNIX locale

È possibile utilizzare `vserver services name-service unix-group create` Per creare gruppi UNIX locali per SVM. I gruppi UNIX locali vengono utilizzati con gli utenti UNIX locali.

Fase

1. Creare un gruppo UNIX locale:

```
vserver services name-service unix-group create -vserver vserver_name -name  
group_name -id integer
```

`-name group_name` specifica il nome del gruppo. La lunghezza del nome del gruppo non deve superare i 64 caratteri.

`-id integer` Specifica l'ID del gruppo assegnato.

Esempio

Il seguente comando crea un gruppo locale denominato `eng` sulla SVM denominata `vs1`. Il gruppo ha l'ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name  
eng -id 101
```

Aggiungere un utente a un gruppo UNIX locale

È possibile utilizzare `vserver services name-service unix-group adduser` Comando per aggiungere un utente a un gruppo UNIX supplementare locale a SVM.

Fase

1. Aggiunta di un utente a un gruppo UNIX locale:

```
vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name
```

`-name group_name` Specifica il nome del gruppo UNIX a cui aggiungere l'utente oltre al gruppo primario dell'utente.

Esempio

Il seguente comando aggiunge un utente denominato `max` a un gruppo UNIX locale denominato `eng` sulla SVM denominata `vs1`:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name  
eng  
-username max
```

Caricare i gruppi UNIX locali da un URI

In alternativa alla creazione manuale di singoli gruppi UNIX locali, è possibile caricare un elenco di gruppi UNIX locali nelle SVM da un URI (Uniform Resource Identifier) utilizzando `vserver services name-service unix-group load-from-uri` comando.

Fasi

1. Creare un file contenente l'elenco dei gruppi UNIX locali che si desidera caricare.

Il file deve contenere informazioni di gruppo in UNIX `/etc/group` formato:

```
group_name: password: group_ID: comma_separated_list_of_users
```

Il comando elimina il valore di `password` campo.

La dimensione massima supportata del file è di 1 MB.

La lunghezza massima di ciascuna riga del file di gruppo è di 32,768 caratteri.

2. Verificare che l'elenco non contenga informazioni duplicate.

L'elenco non deve contenere voci duplicate, altrimenti il caricamento dell'elenco non riesce. Se sono già presenti voci in SVM, è necessario impostare `-overwrite` parametro a `true` per sovrascrivere tutte le voci esistenti con il nuovo file o assicurarsi che il nuovo file non contenga voci che duplicano le voci esistenti.

3. Copiare il file su un server.

Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

5. Caricare il file contenente l'elenco dei gruppi UNIX locali nella SVM dall'URI:

```
vserver services name-service unix-group load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite true false` specifica se sovrascrivere le voci. L'impostazione predefinita è `false`. Se si specifica questo parametro come `true`, ONTAP sostituisce l'intero database locale dei gruppi UNIX della SVM specificata con le voci del file che si sta caricando.

Esempio

Il seguente comando carica un elenco di gruppi UNIX locali dall'URI `ftp://ftp.example.com/group` Nella SVM denominata `vs1`. I gruppi esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

Lavorare con i netgroup

Panoramica sull'utilizzo dei netgroup

È possibile utilizzare netgroup per l'autenticazione degli utenti e per associare i client nelle regole dei criteri di esportazione. È possibile fornire l'accesso ai netgroup da server di nomi esterni (LDAP o NIS) oppure caricare netgroup da un URI (Uniform Resource Identifier) nelle SVM utilizzando `vserver services name-service netgroup load` comando.

Di cosa hai bisogno

Prima di lavorare con i netgroup, è necessario verificare che siano soddisfatte le seguenti condizioni:

- Tutti gli host nei netgroup, indipendentemente dall'origine (NIS, LDAP o file locali), devono disporre di record DNS sia in avanti (A) che in retromarcia (PTR) per fornire ricerche DNS coerenti in avanti e indietro.

Inoltre, se un indirizzo IP di un client ha più record PTR, tutti questi nomi host devono essere membri del netgroup e avere record A corrispondenti.

- I nomi di tutti gli host nei netgroup, indipendentemente dalla loro origine (NIS, LDAP o file locali), devono essere scritti correttamente e utilizzare il maiuscolo/minuscolo corretto. Le incongruenze dei casi nei nomi host utilizzati nei netgroup possono causare comportamenti imprevisti, come i controlli di esportazione non riusciti.
- Tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compressi come specificato in RFC 5952.

Ad esempio, `2011:hu9:0:0:0:0:3:1` deve essere ridotto a `2011:hu9::3:1`.

A proposito di questa attività

Quando si lavora con netgroup, è possibile eseguire le seguenti operazioni:

- È possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.
- È possibile utilizzare `vserver services name-service getxxbyyy netgrp` per verificare se un client fa parte di un netgroup.

Il servizio sottostante per la ricerca viene selezionato in base all'ordine di switch name service configurato.

Caricare i netgroup nelle SVM

Uno dei metodi che è possibile utilizzare per associare i client nelle regole dei criteri di esportazione consiste nell'utilizzare gli host elencati in netgroup. È possibile caricare netgroup da un URI (Uniform Resource Identifier) in SVM in alternativa all'utilizzo di netgroup memorizzati in server di nomi esterni (`vserver services name-service netgroup load`).

Di cosa hai bisogno

I file netgroup devono soddisfare i seguenti requisiti prima di essere caricati in una SVM:

- Il file deve utilizzare lo stesso formato di file di testo netgroup utilizzato per popolare NIS.

ONTAP controlla il formato del file di testo del netgroup prima di caricarlo. Se il file contiene errori, non viene caricato e viene visualizzato un messaggio che indica le correzioni da eseguire nel file. Dopo aver corretto gli errori, è possibile ricaricare il file netgroup nella SVM specificata.

- I caratteri alfabetici nei nomi host nel file netgroup devono essere minuscoli.
- La dimensione massima supportata del file è di 5 MB.
- Il livello massimo supportato per i netgroup di nidificazione è 1000.
- È possibile utilizzare solo i nomi host DNS primari quando si definiscono i nomi host nel file netgroup.

Per evitare problemi di accesso all'esportazione, i nomi host non devono essere definiti utilizzando i record CNAME DNS o round robin.

- Le porzioni di triplice utente e di dominio nel file netgroup devono essere mantenute vuote perché ONTAP non le supporta.

È supportata solo la parte host/IP.

A proposito di questa attività

ONTAP supporta le ricerche netgroup-by-host per il file netgroup locale. Dopo aver caricato il file netgroup, ONTAP crea automaticamente una mappa netgroup.byhost per abilitare le ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup locali durante l'elaborazione delle regole dei criteri di esportazione per valutare l'accesso al client.

Fase

1. Caricare i netgroup nelle SVM da un URI:

```
vserver services name-service netgroup load -vserver vserver_name -source
```

```
{ftp|http|ftps|https}://uri
```

Il caricamento del file netgroup e la creazione della mappa netgroup.byhost possono richiedere alcuni minuti.

Se si desidera aggiornare i netgroup, è possibile modificare il file e caricare il file netgroup aggiornato nella SVM.

Esempio

Il seguente comando carica le definizioni di netgroup nella SVM denominata vs1 dall'URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1  
-source http://intranet/downloads/corp-netgroup
```

Verificare lo stato delle definizioni dei netgroup

Dopo aver caricato i netgroup nella SVM, è possibile utilizzare `vserver services name-service netgroup status` per verificare lo stato delle definizioni dei netgroup. In questo modo è possibile determinare se le definizioni dei netgroup sono coerenti su tutti i nodi che eseguono la SVM.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare lo stato delle definizioni dei netgroup:

```
vserver services name-service netgroup status
```

È possibile visualizzare ulteriori informazioni in una vista più dettagliata.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

Una volta impostato il livello di privilegio, il seguente comando visualizza lo stato del netgroup per tutte le SVM:

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

Server	Node	Load Time	Hash Value
--------	------	-----------	------------

-----	-----	-----	-----
-----	-----	-----	-----

vs1

	node1	9/20/2006 16:04:53	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node2	9/20/2006 16:06:26	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node3	9/20/2006 16:08:08	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node4	9/20/2006 16:11:33	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

Creare una configurazione di dominio NIS

Se nel proprio ambiente viene utilizzato un NIS (Network Information Service) per i name service, è necessario creare una configurazione di dominio NIS per SVM utilizzando `vserver services name-service nis-domain create` comando.

Di cosa hai bisogno

Tutti i server NIS configurati devono essere disponibili e raggiungibili prima di configurare il dominio NIS sulla SVM.

Se si intende utilizzare NIS per le ricerche nelle directory, le mappe nei server NIS non possono contenere più di 1,024 caratteri per ciascuna voce. Non specificare il server NIS non conforme a questo limite. In caso contrario, l'accesso client dipendente dalle voci NIS potrebbe non riuscire.

A proposito di questa attività

È possibile creare più domini NIS. Tuttavia, è possibile utilizzare solo un'opzione impostata su `active`.

Se il database NIS contiene un `netgroup.byhost` map, ONTAP può utilizzarlo per ricerche più rapide. Il `netgroup.byhost` e `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client. A partire da ONTAP 9.7, NIS `netgroup.byhost` le voci possono essere memorizzate nella cache utilizzando `vserver services name-service nis-domain netgroup-database` comandi.

L'utilizzo di NIS per la risoluzione dei nomi host non è supportato.

Fasi

1. Creare una configurazione di dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain  
domain_name -active true -servers IP_addresses
```

È possibile specificare fino a 10 server NIS.



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.

2. Verificare che il dominio sia stato creato:

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

Esempio

Il seguente comando crea e crea una configurazione di dominio NIS attiva per un dominio NIS chiamato nisdomain sulla SVM denominata vs1 con un server NIS all'indirizzo IP 192.0.2.180:

```
vs1::> vserver services name-service nis-domain create -vserver vs1  
-domain nisdomain -active true -nis-servers 192.0.2.180
```

Utilizzare LDAP

Panoramica sull'utilizzo di LDAP

Se nel proprio ambiente viene utilizzato LDAP per i name service, è necessario collaborare con l'amministratore LDAP per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare SVM come client LDAP.

A partire da ONTAP 9.10.1, l'associazione del canale LDAP è supportata per impostazione predefinita sia per le connessioni LDAP di Active Directory che per quelle di servizi nome. 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 dei canali LDAP con i server dei nomi, utilizzare `-try-channel-binding` con il `ldap client modify` comando.

Per ulteriori informazioni, vedere ["2020 requisiti di binding del canale LDAP e firma LDAP per Windows"](#).

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
 - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
 - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
 - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
 - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).
 - Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

Sono disponibili le seguenti opzioni di sicurezza della sessione:

- Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
- AVVIARE TLS
- LDAPS (LDAP su TLS o SSL)
- Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
 - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
 - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
 - I server Kerberos devono avere record SRV presenti sul server DNS.
- Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
 - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
 - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
 - Nel dominio deve essere già configurato un server dei certificati.
- Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
 - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
 - Bidirezionale
 - Unidirezionale, in cui il primario si affida al dominio di riferimento
 - Genitore-figlio
 - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
 - Le password di dominio devono essere le stesse per autenticare quando --bind-as-cifs-server è impostato su true.

Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.



- Per tutte le versioni di ONTAP:
 - Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
 - Firma e sigillatura LDAP (il `-session-security` opzionale)
 - Connessioni TLS crittografate (il `-use-start-tls` opzionale)
 - Comunicazioni tramite la porta LDAPS 636 (la `-use-ldaps-for-ad-ldap` opzionale)

- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

Per ulteriori informazioni

- ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)
- ["Installare il certificato della CA principale autofirmato su SVM"](#)

Creare un nuovo schema del client LDAP

Se lo schema LDAP nell'ambiente in uso differisce dai valori predefiniti di ONTAP, è necessario creare un nuovo schema del client LDAP per ONTAP prima di creare la configurazione del client LDAP.

A proposito di questa attività

La maggior parte dei server LDAP può utilizzare gli schemi predefiniti forniti da ONTAP:

- MS-ad-BIS (lo schema preferito per la maggior parte dei server ad Windows 2012 e successivi)
- AD-IDMU (server ad Windows 2008, Windows 2012 e versioni successive)
- AD-SFU (server ad Windows 2003 e precedenti)
- RFC-2307 (SERVER LDAP UNIX)

Se è necessario utilizzare uno schema LDAP non predefinito, è necessario crearlo prima di creare la configurazione del client LDAP. Consultare l'amministratore LDAP prima di creare un nuovo schema.

Gli schemi LDAP predefiniti forniti da ONTAP non possono essere modificati. Per creare un nuovo schema, creare una copia e modificarla di conseguenza.

Fasi

1. Visualizzare i modelli di schema del client LDAP esistenti per identificare quello che si desidera copiare:

```
vserver services name-service ldap client schema show
```

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Creare una copia dello schema di un client LDAP esistente:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modificare il nuovo schema e personalizzarlo in base all'ambiente:

```
vserver services name-service ldap client schema modify
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Creare una configurazione del client LDAP

Se si desidera che ONTAP acceda ai servizi LDAP o Active Directory esterni del proprio ambiente, è necessario prima configurare un client LDAP sul sistema di archiviazione.

Di cosa hai bisogno

Uno dei primi tre server nell'elenco dei domini risolti di Active Directory deve essere attivo e fornire i dati. In caso contrario, questa attività non riesce.



Vi sono più server, tra cui più di due server inattivi in qualsiasi momento.

Fasi

1. Rivolgersi all'amministratore LDAP per determinare i valori di configurazione appropriati per `vserver services name-service ldap client create` comando:

- a. Specificare una connessione basata su dominio o su indirizzo ai server LDAP.

Il `-ad-domain` e `-servers` le opzioni si escludono a vicenda.

- Utilizzare `-ad-domain` Opzione per attivare la ricerca del server LDAP nel dominio Active Directory.
 - È possibile utilizzare `-restrict-discovery-to-site` Opzione per limitare il rilevamento del server LDAP al sito predefinito CIFS per il dominio specificato. Se si utilizza questa opzione, è necessario specificare anche il sito predefinito CIFS con `-default-site`.
- È possibile utilizzare `-preferred-ad-servers` Opzione per specificare uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole. Una volta creato il client, è possibile modificare questo elenco utilizzando `vserver services name-service ldap client modify` comando.
- Utilizzare `-servers` Opzione per specificare uno o più server LDAP (Active Directory o UNIX) per indirizzo IP in un elenco delimitato da virgole.



Il `-servers` L'opzione è obsoleta in ONTAP 9.2. Iniziando con ONTAP 9,2, la `-ldap-servers` il campo sostituisce `-servers` campo. Questo campo può contenere un nome host o un indirizzo IP per il server LDAP.

- b. Specificare uno schema LDAP predefinito o personalizzato.

La maggior parte dei server LDAP può utilizzare gli schemi di sola lettura predefiniti forniti da ONTAP. Si consiglia di utilizzare questi schemi predefiniti, a meno che non sia necessario fare diversamente. In tal caso, è possibile creare uno schema personalizzato copiando uno schema predefinito (di sola lettura) e modificando la copia.

Schemi predefiniti:

- MS-AD-BIS

Basato su RFC-2307bis, questo è lo schema LDAP preferito per la maggior parte delle implementazioni LDAP standard di Windows 2012 e versioni successive.

- AD-IDMU

Basato su Active Directory Identity Management per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2008, Windows 2012 e versioni successive.

- AD-SFU

Basato su Active Directory Services per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2003 e precedenti.

- RFC-2307

In base a RFC-2307 (*un approccio per l'utilizzo di LDAP come Network Information Service*), questo schema è appropriato per la maggior parte dei server UNIX ad.

c. Selezionare valori di binding.

- `-min-bind-level {anonymous|simple|sasl}` specifica il livello minimo di autenticazione bind.

Il valore predefinito è **anonymous**.

- `-bind-dn LDAP_DN` specifica l'utente di binding.

Per i server Active Directory, è necessario specificare l'utente nel modulo account (DOMINIO/utente) o principale (user@domain.com). In caso contrario, è necessario specificare l'utente nel formato nome distinto (CN=user,DC=domain,DC=com).

- `-bind-password password` specifica la password di bind.

d. Selezionare le opzioni di sicurezza della sessione, se necessario.

È possibile attivare la firma e il sealing LDAP o LDAP su TLS, se richiesto dal server LDAP.

- `--session-security {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*.

Dovresti anche impostare `-min-bind-level {sasl}` a meno che non si desideri che l'autenticazione bind venga meno a. **anonymous** oppure **simple** se la *sign* e il *sealing* non vengono a buon fine.

- `-use-start-tls {true|false}`

Se impostato su **true** E il server LDAP lo supporta, il client LDAP utilizza una connessione TLS crittografata al server. Il valore predefinito è **false**. Per utilizzare questa opzione, è necessario installare un certificato CA principale autofirmato del server LDAP.



Se nella VM di storage è stato aggiunto un server SMB a un dominio e il server LDAP è uno dei controller di dominio del dominio principale del server SMB, è possibile modificare l' `-session-security-for-ad-ldap` utilizzando l'opzione `vserver cifs security modify` comando.

e. Selezionare i valori di porta, query e base.

I valori predefiniti sono consigliati, ma è necessario verificare con l'amministratore LDAP che siano appropriati per l'ambiente in uso.

- `-port port` Specifica la porta del server LDAP.

Il valore predefinito è 389.

Se si intende utilizzare Start TLS per proteggere la connessione LDAP, è necessario utilizzare la porta predefinita 389. Start TLS (Avvia TLS) inizia come una connessione non crittografata sulla porta predefinita LDAP 389 e la connessione viene quindi aggiornata a TLS. Se si modifica la porta, l'avvio TLS non riesce.

- `-query-timeout integer` specifica il timeout della query in secondi.

L'intervallo consentito va da 1 a 10 secondi. Il valore predefinito è 3 secondi.

- `-base-dn LDAP_DN` Specifica il DN di base.

Se necessario, è possibile inserire più valori (ad esempio, se è attivata la funzione LDAP referral chasing). Il valore predefinito è "" (root).

- `-base-scope {base|onelevel|subtree}` specifica l'ambito di ricerca di base.

Il valore predefinito è subtree.

- `-referral-enabled {true|false}` Specifica se è attivata la funzione LDAP referral chasing.

A partire da ONTAP 9.5, questo consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario restituisce una risposta di riferimento LDAP che indica la presenza dei record desiderati sui server LDAP citati. Il valore predefinito è **false**.

Per cercare i record presenti nei server LDAP indicati, è necessario aggiungere la base dn dei record indicati alla base-dn come parte della configurazione del client LDAP.

2. Creazione di una configurazione del client LDAP sulla VM di storage:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



È necessario fornire il nome della VM di archiviazione quando si crea una configurazione client LDAP.

3. Verificare che la configurazione del client LDAP sia stata creata correttamente:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Esempi

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la Storage VM VS1 da utilizzare con un server Active Directory per LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP su cui è richiesta la firma e la sigillatura e il rilevamento del server LDAP è limitato a un sito specifico per il dominio specificato:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP in cui è richiesta la ricerca del riferimento LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la macchina virtuale di storage VS1 specificando il DN di base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la VM di storage VS1 abilitando la ricerca del riferimento:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

Associare la configurazione del client LDAP alle SVM

Per attivare LDAP su una SVM, è necessario utilizzare `vserver services name-service ldap create` Comando per associare una configurazione del client LDAP a SVM.

Di cosa hai bisogno

- Un dominio LDAP deve già esistere all'interno della rete e deve essere accessibile al cluster su cui si trova la SVM.
- Una configurazione del client LDAP deve esistere su SVM.

Fasi

1. Abilitare LDAP su SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config client_config_name
```



A partire da ONTAP 9.2, la `vserver services name-service ldap create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

Il seguente comando abilita LDAP su "vs1" SVM e lo configura per utilizzare la configurazione del client LDAP "ldap1":

```
cluster1::> vserver services name-service ldap create -vserver vs1  
-client-config ldap1 -client-enabled true
```

2. Convalidare lo stato dei server dei nomi utilizzando il comando di controllo `ldap name-service` dei servizi `vserver`.

Il seguente comando convalida i server LDAP su SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1  
  
| Vserver: vs1 |  
| Client Configuration Name: c1 |  
| LDAP Status: up |  
| LDAP Status Details: Successfully connected to LDAP server  
"10.11.12.13". |
```

Il comando `name service check` è disponibile a partire da ONTAP 9.2.

Verificare le origini LDAP nella tabella `name service switch`

È necessario verificare che le origini LDAP per i servizi nome siano elencate correttamente nella tabella di switch del servizio nome per SVM.

Fasi

1. Visualizza il contenuto della tabella corrente dello switch name service:

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

Il comando seguente mostra i risultati per SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
Source
Vserver      Database      Order
-----
My_SVM       hosts         files,
              dns
My_SVM       group         files,ldap
My_SVM       passwd        files,ldap
My_SVM       netgroup      files
My_SVM       namemap       files
5 entries were displayed.
```

namemap specifica le origini per la ricerca delle informazioni di mappatura dei nomi e in quale ordine. In un ambiente UNIX, questa voce non è necessaria. La mappatura dei nomi è necessaria solo in un ambiente misto che utilizza sia UNIX che Windows.

2. Aggiornare ns-switch voce appropriata:

Se si desidera aggiornare la voce ns-switch per...	Immettere il comando...
Informazioni sull'utente	<code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>
Informazioni sul gruppo	<code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>
Informazioni sul netgroup	<code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code>

Utilizza Kerberos con NFS per una sicurezza elevata

Panoramica sull'utilizzo di Kerberos con NFS per una maggiore sicurezza

Se nel proprio ambiente viene utilizzato Kerberos per l'autenticazione avanzata, è necessario collaborare con l'amministratore Kerberos per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare la SVM come client

Kerberos.

L'ambiente deve soddisfare le seguenti linee guida:

- Prima di configurare Kerberos per ONTAP, l'implementazione del sito deve seguire le Best practice per la configurazione del server e del client Kerberos.
- Se possibile, utilizzare NFSv4 o versioni successive se è richiesta l'autenticazione Kerberos.

NFSv3 può essere utilizzato con Kerberos. Tuttavia, i benefici di sicurezza completi di Kerberos sono realizzati solo nelle implementazioni ONTAP di NFSv4 o versioni successive.

- Per promuovere l'accesso ridondante al server, è necessario attivare Kerberos su diversi file di dati LIF su più nodi del cluster utilizzando lo stesso SPN.
- Quando Kerberos è attivato su SVM, è necessario specificare uno dei seguenti metodi di sicurezza nelle regole di esportazione per volumi o qtree, a seconda della configurazione del client NFS.
 - `krb5` (Protocollo Kerberos v5)
 - `krb5i` (Protocollo Kerberos v5 con controllo dell'integrità mediante checksum)
 - `krb5p` (Protocollo Kerberos v5 con servizio di privacy)

Oltre al server e ai client Kerberos, è necessario configurare i seguenti servizi esterni affinché ONTAP supporti Kerberos:

- Servizio di directory

È necessario utilizzare un servizio directory sicuro nel proprio ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS. Non utilizzare NIS, le cui richieste vengono inviate in testo non crittografato e quindi non sono sicure.

- NTP

È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolvibili correttamente tramite DNS.

Verificare le autorizzazioni per la configurazione Kerberos

Kerberos richiede l'impostazione di determinate autorizzazioni UNIX per il volume root SVM e per utenti e gruppi locali.

Fasi

1. Visualizzare le autorizzazioni pertinenti sul volume root SVM:

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

Il volume root di SVM deve avere la seguente configurazione:

Nome...	Impostazione in corso...
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	755

Se questi valori non vengono visualizzati, utilizzare `volume modify` per aggiornarli.

2. Visualizzare gli utenti UNIX locali:

```
vserver services name-service unix-user show -vserver vserver_name
```

La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	<p>Necessario per la fase DI INIT GSS.</p> <p>Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.</p> <p>L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.</p>
root	0	0	Necessario per il montaggio.

Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-user modify` per aggiornarli.

3. Visualizzare i gruppi UNIX locali:

```
vserver services name-service unix-group show -vserver vserver_name
```

La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0

Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-group modify` per aggiornarli.

Creare una configurazione di autenticazione Kerberos NFS

Se si desidera che ONTAP acceda a server Kerberos esterni nel proprio ambiente, è necessario prima configurare SVM in modo che utilizzi un'area Kerberos esistente. A tale scopo, è necessario raccogliere i valori di configurazione per il server KDC Kerberos, quindi utilizzare `vserver nfs kerberos realm create`. Per creare la configurazione dell'area di autenticazione Kerberos su una SVM.

Di cosa hai bisogno

L'amministratore del cluster deve aver configurato NTP sul sistema di storage, sul client e sul server KDC per evitare problemi di autenticazione. Le differenze di tempo tra un client e un server (disallineamento del clock) sono una causa comune di errori di autenticazione.

Fasi

1. Rivolgersi all'amministratore Kerberos per determinare i valori di configurazione appropriati da fornire con `vserver nfs kerberos realm create` comando.
2. Creare una configurazione di area di autenticazione Kerberos su SVM:

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name  
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Verificare che la configurazione dell'area di autenticazione Kerberos sia stata creata correttamente:

```
vserver nfs kerberos realm show
```

Esempi

Il seguente comando crea una configurazione del realm Kerberos NFS per SVM vs1 che utilizza un server Microsoft Active Directory come server KDC. L'area di autenticazione Kerberos è AUTH.EXAMPLE.COM. Il server Active Directory è denominato ad-1 e il suo indirizzo IP è 10.10.8.14. L'inclinazione dell'orologio consentita è di 300 secondi (impostazione predefinita). L'indirizzo IP del server KDC è 10.10.8.14 e il numero di porta è 88 (impostazione predefinita). "Microsoft Kerberos config" è il commento.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
AUTH.EXAMPLE.COM -adserver-name ad-1  
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88  
-kdc-vendor Microsoft  
-comment "Microsoft Kerberos config"
```

Il seguente comando crea una configurazione di autenticazione Kerberos NFS per SVM vs1 che utilizza un KDC MIT. L'area di autenticazione Kerberos è SECURITY.EXAMPLE.COM. L'inclinazione dell'orologio consentita è di 300 secondi. L'indirizzo IP del server KDC è 10.10.9.1 e il numero di porta è 88. Il vendor di KDC è un altro a indicare un vendor UNIX. L'indirizzo IP del server amministrativo è 10.10.9.1 e il numero di porta è 749 (impostazione predefinita). L'indirizzo IP del server delle password è 10.10.9.1 e il numero di porta è 464 (impostazione predefinita). Il commento è "UNIX Kerberos config".

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurare i tipi di crittografia consentiti per NFS Kerberos

Per impostazione predefinita, ONTAP supporta i seguenti tipi di crittografia per NFS Kerberos: DES, 3DES, AES-128 e AES-256. È possibile configurare i tipi di crittografia consentiti per ogni SVM in modo che si adattino ai requisiti di sicurezza per il proprio ambiente specifico utilizzando `vserver nfs modify` con il `-permitted-enc-types` parametro.

A proposito di questa attività

Per una maggiore compatibilità con i client, ONTAP supporta sia la crittografia DES debole che la crittografia AES avanzata per impostazione predefinita. Ciò significa, ad esempio, che se si desidera aumentare la protezione e l'ambiente lo supporta, è possibile utilizzare questa procedura per disattivare DES e 3DES e richiedere ai client di utilizzare solo la crittografia AES.

Si consiglia di utilizzare la crittografia più efficace disponibile. Per ONTAP, cioè AES-256. Verificare con l'amministratore di KDC che questo livello di crittografia sia supportato nell'ambiente in uso.

- L'attivazione o la disattivazione completa di AES (sia AES-128 che AES-256) su SVM è un'interruzione perché distrugge il file DES principal/keytab originale, richiedendo quindi la disattivazione della configurazione Kerberos su tutti i LIF per SVM.

Prima di apportare questa modifica, verificare che i client NFS non si basino sulla crittografia AES su SVM.

- L'attivazione o la disattivazione DI DES o 3DES non richiede modifiche alla configurazione Kerberos sui LIF.

Fase

1. Attivare o disattivare il tipo di crittografia consentito:

Se si desidera attivare o disattivare...	Attenersi alla procedura descritta di seguito...
DES o 3DES	<p>a. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separare più tipi di crittografia con una virgola.</p> <p>b. Verificare che la modifica sia stata eseguita correttamente:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre>
AES-128 o AES-256	<p>a. Identificare su quali SVM e LIF Kerberos sono attivati:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Disattiva Kerberos su tutti i LIF della SVM il cui tipo di crittografia Kerberos NFS consentiva di modificare:</p> <pre>vserver nfs kerberos interface disable -lif lif_name</pre> <p>c. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separare più tipi di crittografia con una virgola.</p> <p>d. Verificare che la modifica sia stata eseguita correttamente:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> <p>e. Riabilitare Kerberos su tutti i LIF su SVM:</p> <pre>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</pre> <p>f. Verificare che Kerberos sia attivato su tutti i LIF:</p> <pre>vserver nfs kerberos interface show</pre>

Attivare Kerberos su una LIF dati

È possibile utilizzare `vserver nfs kerberos interface enable` Comando per abilitare Kerberos su una LIF dati. In questo modo, SVM può utilizzare i servizi di sicurezza Kerberos per NFS.

A proposito di questa attività

Se si utilizza un KDC Active Directory, i primi 15 caratteri di qualsiasi SPN utilizzato devono essere univoci tra le SVM all'interno di un'area di autenticazione o di un dominio.

Fasi

- 1. Creare la configurazione Kerberos NFS:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP richiede la chiave segreta per l'SPN del KDC per abilitare l'interfaccia Kerberos.

Per i KDC Microsoft, viene contattato il KDC e vengono inviati un prompt di nome utente e password alla CLI per ottenere la chiave segreta. Se è necessario creare l'SPN in un'unità organizzativa diversa dell'area Kerberos, è possibile specificare l'opzione -ou parametro.

Per i KDC non Microsoft, è possibile ottenere la chiave segreta utilizzando uno dei due metodi seguenti:

Se...	È inoltre necessario includere il seguente parametro con il comando...
Disporre delle credenziali di amministratore di KDC per recuperare la chiave direttamente dal KDC	-admin-username kdc_admin_username
Non si dispone delle credenziali di amministratore di KDC, ma di un file keytab del KDC contenente la chiave	-keytab-uri {ftp

- 2. Verificare che Kerberos sia stato attivato su LIF:

```
vserver nfs kerberos-config show
```

- 3. Ripetere i passaggi 1 e 2 per attivare Kerberos su più LIF.

Esempio

Il seguente comando crea e verifica una configurazione Kerberos NFS per la SVM denominata vs1 sull'interfaccia logica ves03-d1, con l'SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM nell'OU lab2ou:

```

vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30 disabled -
vs2      ves01-d1
          10.10.10.40 enabled  nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.

```

Aggiungere capacità di storage a una SVM abilitata per NFS

Aggiunta di capacità di storage a una panoramica SVM abilitata per NFS

Per aggiungere capacità di storage a una SVM abilitata per NFS, è necessario creare un volume o un qtree per fornire un container di storage e creare o modificare un criterio di esportazione per tale container. È quindi possibile verificare l'accesso del client NFS dal cluster e verificare l'accesso dai sistemi client.

Di cosa hai bisogno

- NFS deve essere completamente configurato su SVM.
- Il criterio di esportazione predefinito del volume root SVM deve contenere una regola che consenta l'accesso a tutti i client.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completi.
- Eventuali aggiunte o modifiche a una configurazione Kerberos devono essere completate.

Creare una policy di esportazione

Prima di creare regole di esportazione, è necessario creare un criterio di esportazione per conservarle. È possibile utilizzare `vserver export-policy create` per creare un criterio di esportazione.

Fasi

1. Creare una policy di esportazione:

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

Il nome del criterio può contenere fino a 256 caratteri.

2. Verificare che il criterio di esportazione sia stato creato:

```
vserver export-policy show -policyname policy_name
```

Esempio

I seguenti comandi creano e verificano la creazione di una policy di esportazione denominata exp1 sulla SVM denominata vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

Aggiungere una regola a un criterio di esportazione

Senza regole, i criteri di esportazione non possono fornire l'accesso client ai dati. Per creare una nuova regola di esportazione, è necessario identificare i client e selezionare un formato di corrispondenza client, selezionare i tipi di accesso e di sicurezza, specificare un mapping anonimo dell'ID utente, selezionare un numero di indice della regola e selezionare il protocollo di accesso. È quindi possibile utilizzare `vserver export-policy rule create` per aggiungere la nuova regola a un criterio di esportazione.

Di cosa hai bisogno

- Il criterio di esportazione a cui si desidera aggiungere le regole di esportazione deve già esistere.
- Il DNS deve essere configurato correttamente sui dati SVM e i server DNS devono avere le voci corrette per i client NFS.

Questo perché ONTAP esegue ricerche DNS utilizzando la configurazione DNS dei dati SVM per determinati formati di corrispondenza client, e gli errori nella corrispondenza delle regole dei criteri di esportazione possono impedire l'accesso ai dati del client.

- Se si esegue l'autenticazione con Kerberos, è necessario determinare quale dei seguenti metodi di protezione viene utilizzato sui client NFS:
 - `krb5` (Protocollo Kerberos V5)
 - `krb5i` (Protocollo Kerberos V5 con controllo dell'integrità mediante checksum)
 - `krb5p` (Protocollo Kerberos V5 con servizio di privacy)

A proposito di questa attività

Non è necessario creare una nuova regola se una regola esistente in un criterio di esportazione copre i requisiti di accesso e corrispondenza del client.

Se si esegue l'autenticazione con Kerberos e si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e `-superuser` per il volume root a `krb5`, `krb5i`, o `krb5p`.

Fasi

1. Identificare i client e il formato di corrispondenza del client per la nuova regola.

Il `-clientmatch` option specifica i client a cui si applica la regola. È possibile specificare valori di corrispondenza client singoli o multipli; le specifiche di valori multipli devono essere separate da virgole. È possibile specificare la corrispondenza in uno dei seguenti formati:

Formato di corrispondenza del client	Esempio
Nome di dominio preceduto da "." carattere	<code>.example.com</code> oppure <code>.example.com, .example.net, ...</code>
Nome host	<code>host1</code> oppure <code>host1, host2, ...</code>
Indirizzo IPv4	<code>10.1.12.24</code> oppure <code>10.1.12.24, 10.1.12.25, ...</code>
Indirizzo IPv4 con una subnet mask espressa come numero di bit	<code>10.1.12.10/4</code> oppure <code>10.1.12.10/4, 10.1.12.11/4, ...</code>
Indirizzo IPv4 con una maschera di rete	<code>10.1.16.0/255.255.255.0</code> oppure <code>10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0, ...</code>
Indirizzo IPv6 in formato punteggiato	<code>::1.2.3.4</code> oppure <code>::1.2.3.4, ::1.2.3.5, ...</code>
Indirizzo IPv6 con una subnet mask espressa come numero di bit	<code>ff::00/32</code> oppure <code>ff::00/32, ff::01/32, ...</code>
Un singolo netgroup con il nome del netgroup preceduto dal carattere @	<code>@netgroup1</code> oppure <code>@netgroup1, @netgroup2, ...</code>

È inoltre possibile combinare tipi di definizioni client, ad esempio `.example.com, @netgroup1`.

Quando si specificano gli indirizzi IP, tenere presente quanto segue:

- Non è consentito inserire un intervallo di indirizzi IP, ad esempio `10.1.12.10-10.1.12.70`.

Le voci in questo formato vengono interpretate come una stringa di testo e trattate come nome host.

- Quando si specificano singoli indirizzi IP nelle regole di esportazione per la gestione granulare dell'accesso client, non specificare gli indirizzi IP assegnati in modo dinamico (ad esempio DHCP) o temporaneo (ad esempio IPv6).

In caso contrario, il client perde l'accesso quando cambia l'indirizzo IP.

- Non è consentito inserire un indirizzo IPv6 con una maschera di rete, ad esempio `ff::12/ff::00`.

2. Selezionare i tipi di accesso e di sicurezza per le corrispondenze dei client.

È possibile specificare una o più delle seguenti modalità di accesso per i client che eseguono l'autenticazione con i tipi di protezione specificati:

- `-rorule` (accesso di sola lettura)
- `-rwrule` (accesso di lettura/scrittura)
- `-superuser` (accesso root)



Un client può ottenere l'accesso in lettura/scrittura solo per un tipo di protezione specifico se la regola di esportazione consente l'accesso in sola lettura anche per quel tipo di protezione. Se il parametro di sola lettura è più restrittivo per un tipo di protezione rispetto al parametro di lettura/scrittura, il client potrebbe non ottenere l'accesso di lettura/scrittura. Lo stesso vale per l'accesso dei superutenti.

È possibile specificare un elenco separato da virgole di più tipi di protezione per una regola. Se si specifica il tipo di protezione come `any` oppure `never`, non specificare altri tipi di protezione. Scegliere tra i seguenti tipi di protezione validi:

Quando il tipo di protezione è impostato su...	Un client corrispondente può accedere ai dati esportati...
<code>any</code>	Sempre, indipendentemente dal tipo di sicurezza in entrata.
<code>none</code>	Se elencati da soli, ai client con qualsiasi tipo di protezione viene concesso l'accesso come anonimo. Se elencato con altri tipi di protezione, ai client con un tipo di protezione specificato viene concesso l'accesso e ai client con qualsiasi altro tipo di protezione viene concesso l'accesso come anonimo.
<code>never</code>	Mai, indipendentemente dal tipo di sicurezza in entrata.
<code>krb5</code>	Se autenticato da Kerberos 5. Authentication Only (solo autenticazione): L'intestazione di ogni richiesta e risposta viene firmata.
<code>krb5i</code>	Se autenticato da Kerberos 5i. Autenticazione e integrità: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati.
<code>krb5p</code>	Se autenticato da Kerberos 5p. Autenticazione, integrità e privacy: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati e il payload dei dati NFS viene crittografato.
<code>ntlm</code>	Se autenticato da CIFS NTLM.
<code>sys</code>	Se autenticato da NFS AUTH_SYS.

Il tipo di protezione consigliato è `sys`. Oppure, se si utilizza Kerberos, ``krb5,krb5i,0.krb5p`.

Se si utilizza Kerberos con NFSv3, la regola dei criteri di esportazione deve consentire `-rorule e`. `-rwrule` accesso a `sys` oltre a `krb5`. Ciò è dovuto alla necessità di consentire l'accesso NLM (Network Lock Manager) all'esportazione.

3. Specificare un mapping anonimo dell'ID utente.

Il `-anon` L'opzione specifica un ID utente UNIX o un nome utente mappato alle richieste del client che arrivano con un ID utente 0 (zero), che in genere è associato al nome utente `root`. Il valore predefinito è 65534. I client NFS in genere associano l'ID utente 65534 con il nome utente nessuno (noto anche come *root squashing*). In ONTAP, questo ID utente è associato all'utente `pcuser`. Per disattivare l'accesso da parte di qualsiasi client con un ID utente pari a 0, specificare un valore di 65535.

4. Selezionare l'ordine di indice della regola.

Il `-ruleindex` option specifica il numero di indice per la regola. Le regole vengono valutate in base al loro ordine nell'elenco dei numeri di indice; le regole con numeri di indice inferiori vengono valutate per prime. Ad esempio, la regola con indice numero 1 viene valutata prima della regola con indice numero 2.

Se si desidera aggiungere...	Quindi...
La prima regola per un criterio di esportazione	Invio 1.
Regole aggiuntive per una policy di esportazione	<div>a. Visualizzare le regole esistenti nel criterio: <code>vserver export-policy rule show -instance -policyname <i>your_policy</i></code></div> <div>b. Selezionare un numero di indice per la nuova regola in base all'ordine in cui deve essere valutata.</div>

5. Selezionare il valore di accesso NFS applicabile: `{nfs|nfs3|nfs4}`.

`nfs` corrisponde a qualsiasi versione, `nfs3` e `nfs4` associare solo le versioni specifiche.

6. Creare la regola di esportazione e aggiungerla a un criterio di esportazione esistente:

```
vserver export-policy rule create -vserver vserver_name -policyname policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text | "text,text,..." } -rorule security_type -rwrule security_type -superuser security_type -anon user_ID
```

7. Visualizzare le regole per il criterio di esportazione per verificare la presenza della nuova regola:

```
vserver export-policy rule show -policyname policy_name
```

Il comando visualizza un riepilogo per il criterio di esportazione, incluso un elenco di regole applicate a tale criterio. ONTAP assegna a ogni regola un numero di indice della regola. Una volta conosciuto il numero di indice della regola, è possibile utilizzarlo per visualizzare informazioni dettagliate sulla regola di esportazione specificata.

8. Verificare che le regole applicate ai criteri di esportazione siano configurate correttamente:

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

Esempi

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs1 in un criterio di esportazione denominato rs1. La regola ha il numero di indice 1. La regola corrisponde a qualsiasi client nel dominio eng.company.com e al netgroup @netgroup1. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura e in lettura/scrittura agli utenti autenticati con AUTH_SYS. I client con ID utente UNIX 0 (zero) vengono anonimizzati a meno che non vengano autenticati con Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	expl	1	nfs	eng.company.com, @netgroup1	sys

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: expl
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs2 in un criterio di esportazione denominato expol2. La regola ha il numero di indice 21. La regola consente di confrontare i client con i membri del netgroup dev_netgroup_main. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura per gli utenti autenticati con AUTH_SYS e richiede l'autenticazione Kerberos per l'accesso in lettura-scrittura e root. Ai client con ID utente UNIX 0 (zero) viene negato l'accesso root a meno che non vengano autenticati con Kerberos.

```
vs2::> vsserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs2	expol2	21	nfs	@dev_netgroup_main	sys

```
vs2::> vsserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true

```

Creare un volume o un contenitore di storage qtrees

Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

Prima di iniziare

- NFS deve essere configurato e in esecuzione.
- Lo stile di sicurezza SVM deve essere UNIX.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilità analisi del file system](#).

Fasi

1. Creare il volume con un punto di giunzione:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto root, ad esempio `/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

- In una directory esistente, ad esempio `/existing_dir/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

+ se si intende utilizzare un criterio di esportazione esistente, è possibile specificarlo al momento della creazione del volume. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con `volume modify` comando.

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver svm_name -volume volume_name -junction
```

Esempi

Il seguente comando crea un nuovo volume denominato `users1` su SVM `vs1.example.com` e sull'aggregato `aggr1`. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory /eng/ Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo /eng/home, che diventa la home directory di /eng/ namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando volume qtree create comando.

Di cosa hai bisogno

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere UNIX e NFS deve essere configurato e in esecuzione.

Fasi

1. Creare il qtree:

```
volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path } -security-style unix [-policy
export_policy_name]
```

È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato /vol/volume_name/_qtree_name.

Per impostazione predefinita, i qtree ereditano i criteri di esportazione del volume principale, ma possono essere configurati per l'utilizzo dei propri. Se si intende utilizzare un criterio di esportazione esistente, è possibile specificarlo al momento della creazione del qtree. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con volume qtree modify comando.

2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato:

```
volume qtree show -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path }
```

Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style unix  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: unix  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

Accesso sicuro a NFS tramite policy di esportazione

Accesso sicuro a NFS tramite policy di esportazione

È possibile utilizzare policy di esportazione per limitare l'accesso NFS a volumi o qtree a client che corrispondono a parametri specifici. Quando si effettua il provisioning di nuovo storage, è possibile utilizzare policy e regole esistenti, aggiungere regole a policy esistenti o creare nuove policy e regole. È inoltre possibile verificare la configurazione dei criteri di esportazione



A partire da ONTAP 9.3, è possibile attivare il controllo della configurazione dei criteri di esportazione come processo in background che registra eventuali violazioni delle regole in un elenco di regole di errore. Il `vserver export-policy config-checker` I comandi richiamano il controllo e visualizzano i risultati, che è possibile utilizzare per verificare la configurazione ed eliminare le regole errate dal criterio. I comandi convalidano solo la configurazione di esportazione per i nomi host, i netgroup e gli utenti anonimi.

Gestire l'ordine di elaborazione delle regole di esportazione

È possibile utilizzare `vserver export-policy rule setindex` per impostare manualmente il numero di indice di una regola di esportazione esistente. In questo modo è possibile specificare la precedenza con cui ONTAP applica le regole di esportazione alle richieste del client.

A proposito di questa attività

Se il nuovo numero di indice è già in uso, il comando inserisce la regola nel punto specificato e riordina l'elenco di conseguenza.

Fase

1. Modificare il numero di indice di una regola di esportazione specificata:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname  
policy_name -ruleindex integer -newruleindex integer
```

Esempio

Il seguente comando modifica il numero di indice di una regola di esportazione al numero di indice 3 in quello 2 in una policy di esportazione denominata rs1 sulla SVM denominata vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1  
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Assegnare un criterio di esportazione a un volume

Ogni volume contenuto nella SVM deve essere associato a un criterio di esportazione che contenga regole di esportazione per consentire ai client di accedere ai dati nel volume.

A proposito di questa attività

È possibile associare un criterio di esportazione a un volume quando si crea il volume o in qualsiasi momento dopo averlo creato. È possibile associare un criterio di esportazione al volume, anche se un criterio può essere associato a più volumi.

Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del volume, assegnare un criterio di esportazione al volume:

```
volume modify -vserver vserver_name -volume volume_name -policy  
export_policy_name
```

2. Verificare che il criterio sia stato assegnato al volume:

```
volume show -volume volume_name -fields policy
```

Esempio

I seguenti comandi assegnano il criterio di esportazione `nfs_policy` al volume `vol1` su SVM `vs1` e ne verificano l'assegnazione:

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy  
  
cluster::>volume show -volume vol -fields policy  
vserver volume      policy  
-----  
vs1      vol1      nfs_policy
```

Assegnare un criterio di esportazione a un qtree

Invece di esportare un intero volume, è possibile esportare un qtree specifico su un volume per renderlo direttamente accessibile ai client. È possibile esportare un qtree assegnandogli un criterio di esportazione. È possibile assegnare il criterio di esportazione quando si crea un nuovo qtree o modificando un qtree esistente.

Di cosa hai bisogno

Il criterio di esportazione deve esistere.

A proposito di questa attività

Per impostazione predefinita, i qtree ereditano il criterio di esportazione padre del volume contenente, se non diversamente specificato al momento della creazione.

È possibile associare un criterio di esportazione a un qtree quando si crea il qtree o in qualsiasi momento dopo la creazione del qtree. È possibile associare un criterio di esportazione al qtree, anche se un criterio può essere associato a molti qtree.

Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del qtree, assegnare un criterio di esportazione al qtree:

```
volume qtree modify -vserver vs1 -qtree-path  
/vol/volume_name/qtree_name -export-policy export_policy_name
```

2. Verificare che il criterio sia stato assegnato al qtree:

```
volume qtree show -qtree qtree_name -fields export-policy
```

Esempio

I seguenti comandi assegnano il criterio di esportazione `nfs_policy` al qtree `qt1` su SVM `vs1` e ne verificano l'assegnazione:

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy  
nfs_policy  
  
cluster::>volume qtree show -volume vol1 -fields export-policy  
vserver volume qtree export-policy  
-----  
vs1      data1  qt01  nfs_policy
```

Verificare l'accesso del client NFS dal cluster

È possibile consentire ai client selezionati di accedere alla condivisione impostando le autorizzazioni per i file UNIX su un host di amministrazione UNIX. È possibile controllare l'accesso del client utilizzando `vserver export-policy check-access`, regolando le regole di esportazione secondo necessità.

Fasi

1. Nel cluster, controllare l'accesso del client alle esportazioni utilizzando `vserver export-policy check-access` comando.

Il seguente comando controlla l'accesso in lettura/scrittura per un client NFSv3 con l'indirizzo IP 1.2.3.4 nel volume home2. L'output del comando indica che il volume utilizza il criterio di esportazione `exp-home-dir` e che l'accesso è negato.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

Path	Policy	Policy Owner	Policy Owner Type	Rule Index	Access
/	default	vs1_root	volume	1	read
/eng	default	vs1_root	volume	1	read
/eng/home2	exp-home-dir	home2	volume	1	denied

3 entries were displayed.

2. Esaminare l'output per determinare se il criterio di esportazione funziona come previsto e se l'accesso client si comporta come previsto.

In particolare, è necessario verificare quali criteri di esportazione vengono utilizzati dal volume o dal qtree e il tipo di accesso che ne deriva dal client.

3. Se necessario, riconfigurare le regole dei criteri di esportazione.

Verificare l'accesso NFS dai sistemi client

Dopo aver verificato l'accesso NFS al nuovo oggetto storage, è necessario verificare la configurazione accedendo a un host di amministrazione NFS e leggendo i dati da e scrivendo i dati su SVM. Ripetere il processo come utente non root su un sistema client.

Di cosa hai bisogno

- Il sistema client deve disporre di un indirizzo IP consentito dalla regola di esportazione specificata in precedenza.
- È necessario disporre delle informazioni di accesso per l'utente root.

Fasi

1. Sul cluster, verificare l'indirizzo IP della LIF che ospita il nuovo volume:

```
network interface show -vserver svm_name
```

2. Accedere come utente root al sistema client host di amministrazione.
3. Modificare la directory nella cartella mount:

```
cd /mnt/
```

4. Creare e montare una nuova cartella utilizzando l'indirizzo IP di SVM:

a. Creare una nuova cartella:

```
mkdir /mnt/folder
```

b. Montare il nuovo volume in questa nuova directory:

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. Modificare la directory nella nuova cartella:

```
cd folder
```

I seguenti comandi creano una cartella denominata test1, montano il volume vol1 all'indirizzo IP 192.0.2.130 sulla cartella di montaggio test1 e cambiano nella nuova directory test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Creare un nuovo file, verificarne l'esistenza e scriverne del testo:

a. Creare un file di test:

```
touch filename
```

b. Verificare che il file esista.:

```
ls -l filename
```

c. Immettere:

```
cat > filename
```

Digitare del testo, quindi premere Ctrl+D per scrivere il testo nel file di prova.

d. Visualizzare il contenuto del file di test.

```
cat filename
```

e. Rimuovere il file di test:

```
rm filename
```

f. Tornare alla directory principale:

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Come root, impostare la proprietà e le autorizzazioni UNIX desiderate sul volume montato.

7. Su un sistema client UNIX identificato nelle regole di esportazione, accedere come uno degli utenti autorizzati che ora ha accesso al nuovo volume e ripetere le procedure descritte nei passaggi da 3 a 5 per verificare che sia possibile montare il volume e creare un file.

Dove trovare ulteriori informazioni

Una volta verificato l'accesso al client NFS, è possibile eseguire una configurazione NFS aggiuntiva o aggiungere l'accesso SAN. Una volta completato l'accesso al protocollo, è necessario proteggere il volume root della SVM (Storage Virtual Machine).

Configurazione NFS

È possibile configurare ulteriormente l'accesso NFS utilizzando le seguenti informazioni e report tecnici:

- ["Gestione NFS"](#)

Descrive come configurare e gestire l'accesso ai file utilizzando NFS.

- ["Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"](#)

Funge da guida operativa NFSv3 e NFSv4 e fornisce una panoramica del sistema operativo ONTAP con particolare attenzione a NFSv4.

- ["Report tecnico di NetApp 4073: Autenticazione unificata sicura"](#)

Spiega come configurare ONTAP per l'utilizzo con server Kerberos versione 5 (krb5) basati su UNIX per l'autenticazione dello storage NFS e Active Directory (ad) come provider di identità KDC e LDAP (Lightweight Directory Access Protocol).

- ["Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"](#)

Descrive le Best practice da seguire durante l'implementazione dei componenti NFSv4 su client AIX, Linux o Solaris collegati a sistemi che eseguono ONTAP.

Configurazione di rete

È possibile configurare ulteriormente le funzioni di rete e i servizi di gestione dei nomi utilizzando i seguenti report tecnici e informativi:

- ["Gestione NFS"](#)

Descrive come configurare e gestire il networking ONTAP.

- ["Report tecnico di NetApp 4182: Considerazioni sulla progettazione dello storage Ethernet e Best practice per le configurazioni di Clustered Data ONTAP"](#)

Descrive l'implementazione delle configurazioni di rete ONTAP e fornisce scenari di implementazione di rete comuni e consigli sulle Best practice.

- ["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Spiega come configurare LDAP, NIS, DNS e la configurazione dei file locali per scopi di autenticazione.

Configurazione del protocollo SAN

Se si desidera fornire o modificare l'accesso SAN alla nuova SVM, è possibile utilizzare le informazioni di configurazione FC o iSCSI, disponibili per più sistemi operativi host.

Protezione del volume root

Dopo aver configurato i protocolli su SVM, assicurarsi che il volume root sia protetto:

- ["Protezione dei dati"](#)

Descrive come creare un mirror di condivisione del carico per proteggere il volume root SVM, una Best practice NetApp per le SVM abilitate per NAS. Viene inoltre descritto come eseguire rapidamente il ripristino da guasti o perdite di volume promuovendo il volume root SVM da un mirror di condivisione del carico.

Le differenze tra le esportazioni ONTAP e quelle 7-Mode

Le differenze tra le esportazioni ONTAP e quelle 7-Mode

Se non si ha familiarità con il modo in cui ONTAP implementa le esportazioni NFS, è possibile confrontare i tool di configurazione per l'esportazione di 7-Mode e ONTAP, oltre a 7-Mode di esempio `/etc/exports` file con criteri e regole in cluster.

In ONTAP non c'è `/etc/exports` file e no `exportfs` comando. È invece necessario definire un criterio di esportazione. Le policy di esportazione consentono di controllare l'accesso al client in maniera molto simile a quella di 7-Mode, ma offrono funzionalità aggiuntive come la possibilità di riutilizzare la stessa policy di esportazione per più volumi.

Informazioni correlate


["Gestione NFS"](#)

["Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"](#)

Confronto delle esportazioni in 7-Mode e ONTAP

Le esportazioni in ONTAP sono definite e utilizzate in modo diverso rispetto agli ambienti 7-Mode.

Aree di differenza	7-Mode	ONTAP
Come vengono definite le esportazioni	Le esportazioni sono definite in <code>/etc/exports</code> file.	Le esportazioni vengono definite creando una policy di esportazione all'interno di una SVM. Una SVM può includere più criteri di esportazione.

Scopo dell'esportazione	<ul style="list-style-type: none"> • Le esportazioni si applicano a un percorso di file o qtree specificato. • È necessario creare una voce separata in <code>/etc/exports</code> per ogni percorso di file o qtree. • Le esportazioni sono persistenti solo se sono definite in <code>/etc/exports</code> file. 	<ul style="list-style-type: none"> • I criteri di esportazione si applicano a un intero volume, inclusi tutti i percorsi di file e i qtree contenuti nel volume. • Se si desidera, è possibile applicare i criteri di esportazione a più volumi. • Tutte le policy di esportazione sono persistenti durante i riavvii del sistema.
Recinzione (specifica di accessi diversi per client specifici per le stesse risorse)	Per fornire a client specifici un accesso diverso a una singola risorsa esportata, è necessario elencare ciascun client e l'accesso consentito in <code>/etc/exports</code> file.	Le policy di esportazione sono composte da una serie di regole di esportazione individuali. Ogni regola di esportazione definisce autorizzazioni di accesso specifiche per una risorsa ed elenca i client che dispongono di tali autorizzazioni. Per specificare un accesso diverso per client specifici, è necessario creare una regola di esportazione per ogni set specifico di autorizzazioni di accesso, elencare i client che dispongono di tali autorizzazioni e aggiungere le regole ai criteri di esportazione.
Alias del nome	Quando si definisce un'esportazione, è possibile scegliere di rendere il nome dell'esportazione diverso dal nome del percorso del file. Utilizzare il <code>-actual</code> quando si definisce un'esportazione in <code>/etc/exports</code> file.	<p>È possibile scegliere di rendere il nome del volume esportato diverso dal nome del volume effettivo. A tale scopo, è necessario montare il volume con un nome di percorso di giunzione personalizzato all'interno dello spazio dei nomi SVM.</p> <div>  <p>Per impostazione predefinita, i volumi vengono montati con il relativo nome del volume. Per personalizzare il nome del percorso di giunzione di un volume, è necessario smontarlo, rinominarlo e rimontarlo.</p> </div>

Esempi di policy di esportazione ONTAP

È possibile rivedere criteri di esportazione di esempio per comprendere meglio il funzionamento delle policy di esportazione in ONTAP.

Esempio di implementazione ONTAP di un'esportazione in 7-Mode

Nell'esempio riportato di seguito viene illustrata un'esportazione in 7-Mode così come viene visualizzata in `/etc/export` file:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:  
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Per riprodurre questa esportazione come criterio di esportazione in cluster, è necessario creare un criterio di esportazione con tre regole di esportazione e quindi assegnare il criterio di esportazione al volume vol1.

Regola	Elemento	Valore
Regola 1	-clientmatch (specifica del client)	@readonly_netgroup
-ruleindex(posizione della regola di esportazione nell'elenco delle regole)	1	-protocol
nfs	-rorule(consenti accesso di sola lettura)	sys (Client autenticato con AUTH_SYS)
-rwrule(consenti accesso in lettura/scrittura)	never	-superuser(consenti accesso superutente)
none(root <i>squashed</i> ad anon)	Articolo 2	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	Articolo 3
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs

Regola	Elemento	Valore
-rorule	sys	-rwrule
sys	-superuser	none

1. Creare una policy di esportazione chiamata exp_vol1:

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Creare tre regole con i seguenti parametri nel comando base:

- Comando di base:

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

- Parametri della regola:

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none+ -clientmatch @rootaccess_netgroup -ruleindex
2 -protocol nfs -rorule sys -rwrule sys -superuser sys+ -clientmatch
@readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule
sys -rwrule sys -superuser none
```

3. Assegnare il criterio al volume vol1:

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

Esempio di consolidamento delle esportazioni 7-Mode

L'esempio seguente mostra un 7-Mode /etc/export file che include una riga per ciascuno dei 10 qtree:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP, è necessario uno dei due criteri per ogni qtree: Uno con una regola che include -clientmatch host1519s, o con una regola che include -clientmatch host2057s.

1. Creare due policy di esportazione chiamate exp_vol1q1 e exp_vol1q2:

- vserver export-policy create -vserver NewSVM -policyname exp_vol1q1

- vserver export-policy create -vserver NewSVM -policyname exp_vol1q2

2. Creare una regola per ogni policy:

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vollq1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vollq2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Applicare i criteri alle qtree:

- `volume qtree modify -vserver NewSVM -qtree-path /vol/voll/q_1472 -export -policy exp_vollq1`
- [prossimo 4 qtree...]
- `volume qtree modify -vserver NewSVM -qtree-path /vol/voll/q_2237 -export -policy exp_vollq2`
- [prossimo 4 qtree...]

Se in un secondo momento è necessario aggiungere qtree aggiuntivi per tali host, si utilizzerebbero le stesse policy di esportazione.

Gestisci NFS con la CLI

Panoramica di riferimento di NFS

ONTAP include funzionalità di accesso ai file disponibili per il protocollo NFS. È possibile attivare un server NFS ed esportare volumi o qtree.

Eseguire questa procedura nei seguenti casi:

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

Comprendere l'accesso al file NAS

Spazi dei nomi e punti di giunzione

Panoramica degli spazi dei nomi e dei punti di giunzione

Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share*. SMB. L'esportazione o la condivisione rappresenta l'intero namespace o una posizione intermedia all'interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

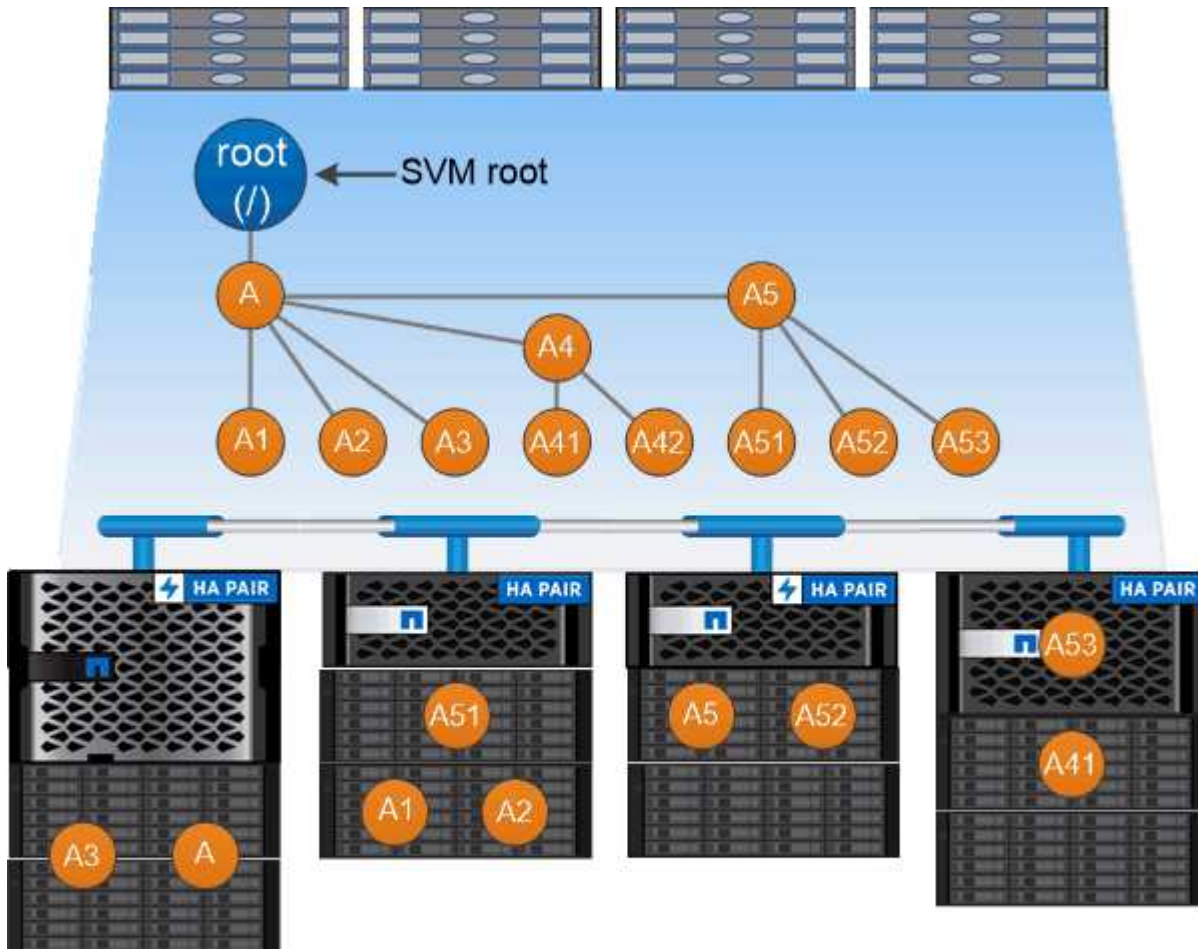
È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all'interno di un volume. Il percorso di

una giunzione di volume per un volume denominato “vol3” potrebbe essere /vol1/vol2/vol3, o. /vol1/dir2/vol3, o persino /dir1/dir2/vol3. Il percorso è chiamato *percorso di giunzione*.

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.



Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

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
```

Quali sono le tipiche architetture dello spazio dei nomi NAS

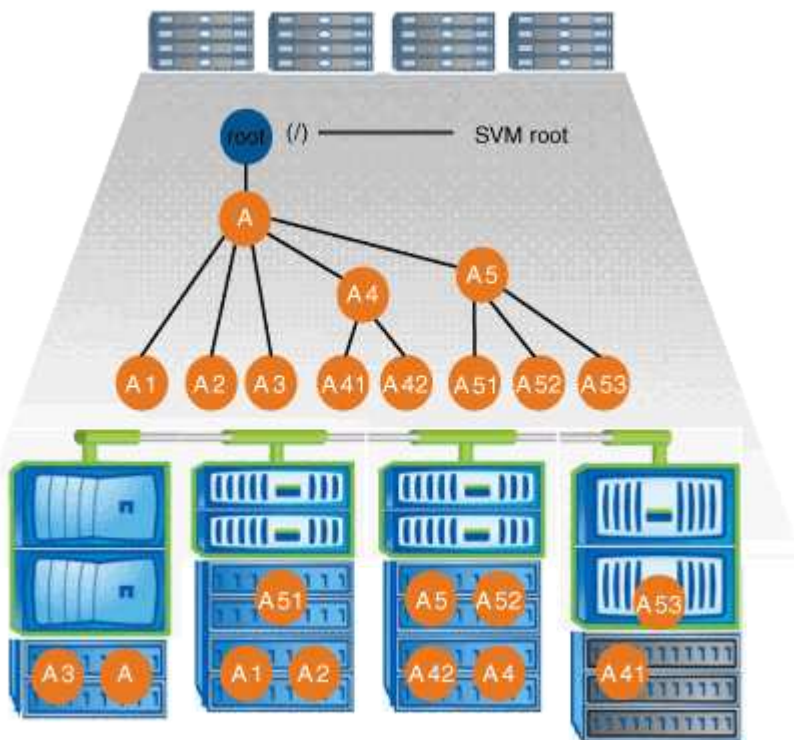
Esistono diverse architetture dello spazio dei nomi NAS tipiche che è possibile utilizzare per creare lo spazio dei nomi SVM. È possibile scegliere l'architettura dello spazio dei nomi che soddisfa le esigenze di business e workflow.

La parte superiore dello spazio dei nomi è sempre il volume root, rappresentato da una barra (/). L'architettura dello spazio dei nomi sotto la radice si suddivide in tre categorie di base:

- Un singolo albero ramificato, con una sola giunzione alla radice dello spazio dei nomi
- Più alberi ramificati, con più punti di giunzione alla radice dello spazio dei nomi
- Più volumi standalone, ciascuno con un punto di giunzione separato per la radice dello spazio dei nomi

Namespace con singolo albero ramificato

Un'architettura con un singolo albero ramificato ha un singolo punto di inserimento alla radice dello spazio dei nomi SVM. Il singolo punto di inserimento può essere un volume giuntato o una directory sotto la root. Tutti gli altri volumi vengono montati nei punti di giunzione sotto il singolo punto di inserimento (che può essere un volume o una directory).

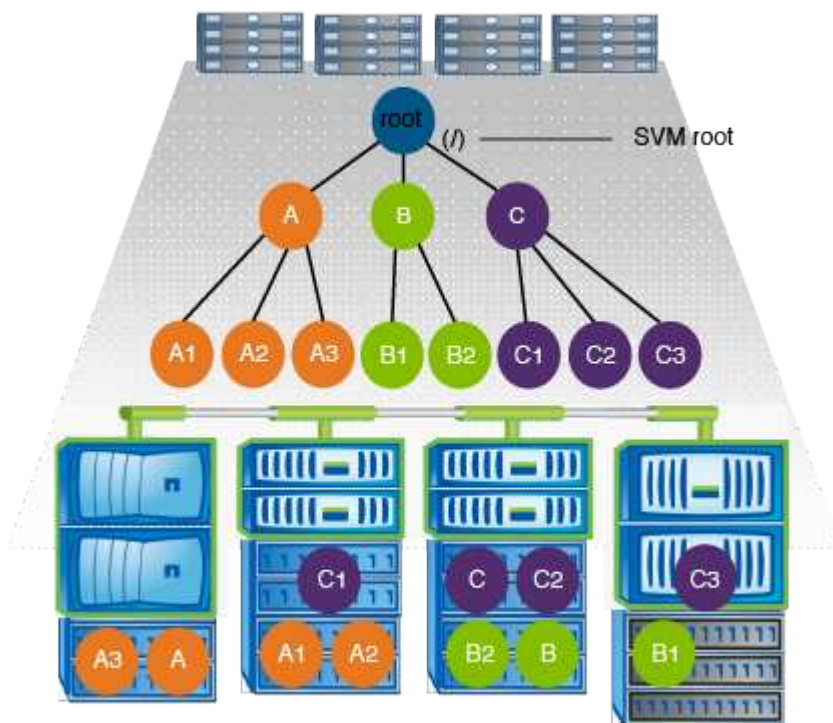


Ad esempio, una configurazione tipica di giunzione di volumi con l'architettura dello spazio dei nomi sopra descritta potrebbe essere simile alla seguente configurazione, in cui tutti i volumi sono congiunti sotto il singolo punto di inserimento, che è una directory denominata "data":

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

Namespace con più alberi ramificati

Un'architettura con più alberi ramificati ha più punti di inserimento alla radice dello spazio dei nomi SVM. I punti di inserimento possono essere volumi congiunti o directory sotto la radice. Tutti gli altri volumi vengono montati nei punti di giunzione sotto i punti di inserimento (che possono essere volumi o directory).

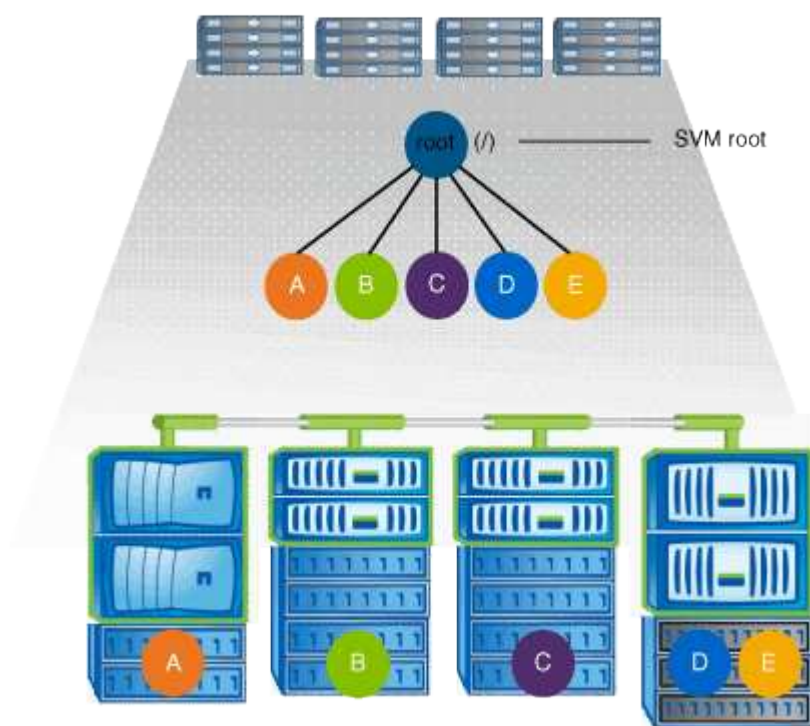


Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti tre punti di inserimento nel volume root della SVM. Due punti di inserimento sono directory denominate "data" e "projects". Un punto di inserimento è un volume giuntato denominato "audit":

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

Namespace con più volumi standalone

In un'architettura con volumi standalone, ogni volume ha un punto di inserimento nella directory principale dello spazio dei nomi SVM; tuttavia, il volume non è giuntato sotto un altro volume. Ogni volume ha un percorso univoco ed è posto direttamente sotto la root oppure posto sotto una directory sotto la root.



Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti cinque punti di inserimento nel volume root della SVM, con ciascun punto di inserimento che rappresenta un percorso per un volume.

Vserver	Volume	Junction		Junction
		Active	Junction Path	Path Source
vs1	eng	true	/eng	RW_volume
vs1	mktg	true	/vol/mktg	RW_volume
vs1	project1	true	/project1	RW_volume
vs1	project2	true	/project2	RW_volume
vs1	sales	true	/sales	RW_volume
vs1	vs1_root	-	/	-

Come ONTAP controlla l'accesso ai file

Panoramica delle modalità di controllo dell'accesso ai file da parte di ONTAP

ONTAP controlla l'accesso ai file in base alle restrizioni basate sull'autenticazione e sui file specificate dall'utente.

Quando un client si connette al sistema di storage per accedere ai file, ONTAP deve eseguire due operazioni:

- Autenticazione

ONTAP deve autenticare il client verificando l'identità con un'origine attendibile. Inoltre, il tipo di autenticazione del client è un metodo che può essere utilizzato per determinare se un client può accedere ai dati durante la configurazione dei criteri di esportazione (facoltativo per CIFS).

- Autorizzazione

ONTAP deve autorizzare l'utente confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory e determinando il tipo di accesso, se presente, da fornire.

Per gestire correttamente il controllo dell'accesso ai file, ONTAP deve comunicare con servizi esterni come server NIS, LDAP e Active Directory. La configurazione di un sistema storage per l'accesso ai file mediante CIFS o NFS richiede la configurazione dei servizi appropriati in base all'ambiente in uso in ONTAP.

Restrizioni basate sull'autenticazione

Con le restrizioni basate sull'autenticazione, è possibile specificare quali macchine client e quali utenti possono connettersi alla SVM (Storage Virtual Machine).

ONTAP supporta l'autenticazione Kerberos da server UNIX e Windows.

Restrizioni basate su file

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei tre livelli di protezione.

Qualsiasi oggetto di storage può contenere fino a tre tipi di livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. 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.



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. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

Come ONTAP gestisce l'autenticazione del client NFS

Panoramica su come ONTAP gestisce l'autenticazione del client NFS

I client NFS devono essere autenticati correttamente prima di poter accedere ai dati sulla SVM. ONTAP autentica i client verificando le credenziali UNIX in base ai servizi di nomi configurati.

Quando un client NFS si connette a SVM, ONTAP ottiene le credenziali UNIX per l'utente controllando i diversi name service, a seconda della configurazione dei name service di SVM. ONTAP può controllare le credenziali per gli account UNIX locali, i domini NIS e i domini LDAP. Almeno uno di questi deve essere configurato in modo che ONTAP possa autenticare correttamente l'utente. È possibile specificare più servizi di nomi e l'ordine in cui ONTAP li cerca.

In un ambiente NFS puro con stili di sicurezza dei volumi UNIX, questa configurazione è sufficiente per autenticare e fornire l'accesso corretto ai file per un utente che si connette da un client NFS.

Se si utilizzano stili di protezione di volumi misti, NTFS o unificati, ONTAP deve ottenere un nome utente SMB per l'utente UNIX per l'autenticazione con un controller di dominio Windows. Ciò può avvenire mappando singoli utenti utilizzando account UNIX locali o domini LDAP oppure utilizzando un utente SMB predefinito. È possibile specificare quali servizi di nomi ONTAP esegue la ricerca in quale ordine o specificare un utente SMB predefinito.

Modalità di utilizzo dei servizi di nome da parte di ONTAP

ONTAP utilizza i name service per ottenere informazioni su utenti e client. ONTAP utilizza queste informazioni per autenticare gli utenti che accedono ai dati sul sistema di storage o ne amministrano l'amministrazione e per mappare le credenziali dell'utente in un

ambiente misto.

Quando si configura il sistema di storage, è necessario specificare i servizi dei nomi che si desidera utilizzare per ottenere le credenziali utente per l'autenticazione di ONTAP. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali (file)
- NIS (External NIS Domain)
- Domini LDAP esterni (LDAP)

Si utilizza `vserver services name-service ns-switch` Famiglia di comandi per configurare le SVM con le origini per la ricerca delle informazioni di rete e l'ordine in cui eseguirne la ricerca. Questi comandi forniscono le funzionalità equivalenti di `/etc/nsswitch.conf` File su sistemi UNIX.

Quando un client NFS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le credenziali UNIX per l'utente. Se i name service sono configurati correttamente e ONTAP è in grado di ottenere le credenziali UNIX, ONTAP autentica correttamente l'utente.

In un ambiente con stili di sicurezza misti, ONTAP potrebbe dover mappare le credenziali dell'utente. Per consentire a ONTAP di mappare correttamente le credenziali dell'utente, è necessario configurare i name service in modo appropriato per l'ambiente in uso.

ONTAP utilizza inoltre i servizi di nome per autenticare gli account amministratore di SVM. È necessario tenere presente questo aspetto durante la configurazione o la modifica dello switch del name service per evitare di disattivare accidentalmente l'autenticazione per gli account amministratore SVM. Per ulteriori informazioni sugli utenti di amministrazione di SVM, vedere ["Autenticazione amministratore e RBAC"](#).

In che modo ONTAP garantisce l'accesso ai file SMB dai client NFS

ONTAP utilizza la semantica di protezione del file system di Windows NT per determinare se un utente UNIX, su un client NFS, ha accesso a un file con autorizzazioni NTFS.

A tale scopo, ONTAP converte l'ID utente UNIX dell'utente in una credenziale SMB e utilizza la credenziale SMB per verificare che l'utente disponga dei diritti di accesso al file. Una credenziale SMB è costituita da un identificatore di protezione (SID) primario, di solito il nome utente Windows dell'utente, e da uno o più SID di gruppo che corrispondono ai gruppi Windows di cui l'utente è membro.

Il tempo impiegato da ONTAP per convertire l'UID UNIX in una credenziale SMB può essere compreso tra decine di millisecondi e centinaia di millisecondi, poiché il processo richiede il contatto con un controller di dominio. ONTAP esegue il mapping dell'UID alla credenziale SMB e inserisce il mapping in una cache delle credenziali per ridurre il tempo di verifica causato dalla conversione.

Come funziona la cache delle credenziali NFS

Quando un utente NFS richiede l'accesso alle esportazioni NFS sul sistema di storage, ONTAP deve recuperare le credenziali dell'utente dai name server esterni o dai file locali per autenticare l'utente. ONTAP memorizza quindi queste credenziali in una cache interna per riferimenti futuri. La comprensione del funzionamento delle cache delle credenziali NFS consente di gestire potenziali problemi di performance e accesso.

Senza la cache delle credenziali, ONTAP dovrebbe eseguire query sui servizi dei nomi ogni volta che un utente NFS ha richiesto l'accesso. In un sistema storage occupato a cui molti utenti accedono, questo può causare rapidamente gravi problemi di performance, causando ritardi indesiderati o addirittura negazioni

dell'accesso al client NFS.

Con la cache delle credenziali, ONTAP recupera le credenziali dell'utente e le memorizza per un periodo di tempo prestabilito per un accesso rapido e semplice nel caso in cui il client NFS invii un'altra richiesta. Questo metodo offre i seguenti vantaggi:

- Semplifica il carico sul sistema storage gestendo meno richieste ai name server esterni (come NIS o LDAP).
- Semplifica il carico sui server dei nomi esterni inviando loro un numero inferiore di richieste.
- Accelera l'accesso degli utenti eliminando i tempi di attesa per ottenere le credenziali da origini esterne prima che l'utente possa essere autenticato.

ONTAP memorizza le credenziali positive e negative nella cache delle credenziali. Le credenziali positive significano che l'utente è stato autenticato e ha ottenuto l'accesso. Le credenziali negative significano che l'utente non è stato autenticato e l'accesso è stato negato.

Per impostazione predefinita, ONTAP memorizza le credenziali positive per 24 ore, ovvero, dopo l'autenticazione iniziale di un utente, ONTAP utilizza le credenziali memorizzate nella cache per tutte le richieste di accesso da parte di tale utente per 24 ore. Se l'utente richiede l'accesso dopo 24 ore, il ciclo ha inizio: ONTAP ignora le credenziali memorizzate nella cache e ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi durante le 24 ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle 24 ore successive.

Per impostazione predefinita, ONTAP memorizza le credenziali negative per due ore, ovvero, dopo aver inizialmente negato l'accesso a un utente, ONTAP continua a negare qualsiasi richiesta di accesso da parte di tale utente per due ore. Se l'utente richiede l'accesso dopo 2 ore, il ciclo ricomincia: ONTAP ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi nelle due ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle due ore successive.

Creare e gestire volumi di dati in spazi dei nomi NAS

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.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).



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 vs1 -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 SMB 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 vs1 -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.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

Fasi

1. Creare il volume senza un punto di giunzione utilizzando il seguente comando:

```
volume create -vserver vs1 -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 vs1 -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 disinstalla e si disconnette un volume, 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	<pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre>
Smontare un volume	<pre>volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name</pre>

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

Il seguente esempio 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.

Fase

1. Eseguire l'azione desiderata:

Se si desidera visualizzare...	Immettere il comando...
Informazioni riepilogative sui volumi montati e non montati su SVM	<code>volume show -vserver vserver_name -junction</code>
Informazioni dettagliate sui volumi montati e non montati su SVM	<code>volume show -vserver vserver_name -volume volume_name -instance</code>

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 vs1 -fields fieldname,...`

Esempi

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

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction 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 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		
NTFS	PMI	ACL NTFS	NTFS	
Misto	NFS o SMB	Bit di modalità NFSv3	UNIX	
		NFSv4.ACL		
		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	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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<code>volume create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume modify</code> e includono <code>-security-style</code> 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	<code>volume qtree create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume qtree modify</code> e includono <code>-security-style</code> 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`

Impostare l'accesso al file utilizzando NFS

Impostare l'accesso al file utilizzando la panoramica NFS

È necessario completare una serie di passaggi per consentire ai client di accedere ai file sulle macchine virtuali di storage (SVM) utilizzando NFS. A seconda della configurazione corrente dell'ambiente, sono disponibili alcuni passaggi aggiuntivi opzionali.

Per consentire ai client di accedere ai file su SVM utilizzando NFS, è necessario completare le seguenti operazioni:

1. Abilitare il protocollo NFS su SVM.

È necessario configurare SVM per consentire l'accesso ai dati dai client tramite NFS.

2. Creare un server NFS su SVM.

Un server NFS è un'entità logica su SVM che consente a SVM di fornire file su NFS. È necessario creare il server NFS e specificare le versioni del protocollo NFS che si desidera consentire.

3. Configurare i criteri di esportazione su SVM.

È necessario configurare i criteri di esportazione per rendere disponibili volumi e qtree ai client.

4. Configurare il server NFS con la sicurezza appropriata e altre impostazioni a seconda della rete e dell'ambiente di storage.

Questo passaggio può includere la configurazione di Kerberos, LDAP, NIS, mappature dei nomi e utenti locali.

Accesso sicuro a NFS tramite policy di esportazione

In che modo le policy di esportazione controllano l'accesso dei client ai volumi o ai qtree

I criteri di esportazione contengono una o più *regole di esportazione* che elaborano ogni richiesta di accesso client. Il risultato del processo determina se al client viene negato o concesso l'accesso e quale livello di accesso. Affinché i client possano accedere ai dati, è necessario che sulla macchina virtuale di storage (SVM) sia presente un criterio di esportazione con regole di esportazione.

Per configurare l'accesso del client al volume o al qtree, è necessario associare esattamente un criterio di

esportazione a ciascun volume o qtree. La SVM può contenere più policy di esportazione. Ciò consente di eseguire le seguenti operazioni per le SVM con più volumi o qtree:

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

Se un client effettua una richiesta di accesso non consentita dalla policy di esportazione applicabile, la richiesta non riesce e viene visualizzato un messaggio di autorizzazione negata. Se un client non corrisponde a nessuna regola nella policy di esportazione, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati.

È possibile modificare dinamicamente un criterio di esportazione su un sistema che esegue ONTAP.

Policy di esportazione predefinita per le SVM

Ogni SVM dispone di un criterio di esportazione predefinito che non contiene regole. Prima che i client possano accedere ai dati su SVM, deve esistere un criterio di esportazione con regole. Ogni volume FlexVol contenuto nella SVM deve essere associato a una policy di esportazione.

Quando si crea una SVM, il sistema storage crea automaticamente una policy di esportazione predefinita chiamata `default` Per il volume root di SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM. In alternativa, è possibile creare una policy di esportazione personalizzata con regole. È possibile modificare e rinominare il criterio di esportazione predefinito, ma non è possibile eliminare il criterio di esportazione predefinito.

Quando si crea un volume FlexVol nella sua SVM contenente, il sistema di storage crea il volume e lo associa alla policy di esportazione predefinita per il volume root della SVM. Per impostazione predefinita, ogni volume creato in SVM è associato al criterio di esportazione predefinito per il volume root. È possibile utilizzare il criterio di esportazione predefinito per tutti i volumi contenuti in SVM oppure creare un criterio di esportazione univoco per ciascun volume. È possibile associare più volumi alla stessa policy di esportazione.

Come funzionano le regole di esportazione

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

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

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

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

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

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

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



A partire da ONTAP 9.3, è possibile attivare il controllo della configurazione dei criteri di esportazione come processo in background che registra eventuali violazioni delle regole in un elenco di regole di errore. Il `vserver export-policy config-checker` i comandi richiamano il controllo e visualizzano i risultati, che è possibile utilizzare per verificare la configurazione ed eliminare le regole errate dal criterio.

I comandi convalidano solo la configurazione di esportazione per i nomi host, i netgroup e gli utenti anonimi.

Esempio

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

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

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

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

Esempio

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

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

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

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

Esempio

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- -rorule any
- -rwrule krb5,ntlm

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

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

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

Gestire i client con un tipo di protezione non elencato

Quando un client si presenta con un tipo di protezione non elencato in un parametro di accesso di una regola di esportazione, è possibile scegliere di negare l'accesso al client o di associarlo all'ID utente anonimo utilizzando invece l'opzione `none` nel parametro `access`.

Un client potrebbe presentarsi con un tipo di protezione non elencato in un parametro di accesso perché autenticato con un tipo di protezione diverso o non autenticato affatto (tipo di protezione AUTH_NONE). Per impostazione predefinita, al client viene automaticamente negato l'accesso a tale livello. Tuttavia, è possibile aggiungere l'opzione `none` al parametro di accesso. Di conseguenza, i client con uno stile di sicurezza non elencato vengono mappati all'ID utente anonimo. Il `-anon` il parametro determina l'ID utente assegnato a tali client. L'ID utente specificato per `-anon` il parametro deve essere un utente valido configurato con le autorizzazioni che si ritiene appropriate per l'utente anonimo.

Valori validi per `-anon` intervallo di parametri da 0 a. 65535.

ID utente assegnato a. <code>-anon</code>	Gestione risultante delle richieste di accesso del client
0 - 65533	La richiesta di accesso client viene mappata all'ID utente anonimo e ottiene l'accesso in base alle autorizzazioni configurate per l'utente.
65534	La richiesta di accesso client viene mappata all'utente nessuno e ottiene l'accesso in base alle autorizzazioni configurate per l'utente. Questa è l'impostazione predefinita.
65535	La richiesta di accesso da qualsiasi client viene negata quando viene mappata a questo ID e il client si presenta con il tipo di sicurezza AUTH_NONE. La richiesta di accesso dai client con ID utente 0 viene negata quando viene mappata a questo ID e il client si presenta con qualsiasi altro tipo di sicurezza.

Quando si utilizza l'opzione `none`, è importante ricordare che il parametro di sola lettura viene elaborato per primo. Per configurare le regole di esportazione per i client con tipi di protezione non elencati, prendere in considerazione le seguenti linee guida:

Include la funzione di sola lettura <code>none</code>	La lettura/scrittura include <code>none</code>	Accesso risultante per i client con tipi di sicurezza non elencati
No	No	Negato
No	Sì	Negato perché viene elaborata per prima la sola lettura
Sì	No	Sola lettura come anonimo
Sì	Sì	Lettura/scrittura anonima

Esempio

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura a qualsiasi tipo di protezione, ma in questo caso si applica solo ai client già filtrati dalla regola di sola lettura.

Pertanto, i client 1 e 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in lettura/scrittura con il proprio ID utente.

Esempio

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

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

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

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura solo come utente anonimo.

Pertanto, il client n. 1 e il client n. 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in sola lettura con il proprio ID utente, ma viene negato l'accesso in lettura/scrittura.

In che modo i tipi di sicurezza determinano i livelli di accesso del client

Il tipo di protezione autenticato dal client gioca un ruolo speciale nelle regole di esportazione. È necessario comprendere in che modo il tipo di protezione determina i livelli di accesso che il client ottiene a un volume o qtree.

I tre livelli di accesso possibili sono i seguenti:

1. Sola lettura
2. Lettura/scrittura
3. Superuser (per client con ID utente 0)

Poiché il livello di accesso in base al tipo di protezione viene valutato in questo ordine, è necessario osservare le seguenti regole quando si costruiscono i parametri del livello di accesso nelle regole di esportazione:

Per ottenere un livello di accesso da parte di un client...	Questi parametri di accesso devono corrispondere al tipo di sicurezza del client...
Utente normale di sola lettura	Sola lettura (<code>-rorule</code>)
Lettura/scrittura utente normale	Sola lettura (<code>-rorule</code>) e read-write (<code>-rwrule</code>)
Superuser di sola lettura	Sola lettura (<code>-rorule</code>) e <code>-superuser</code>
Lettura/scrittura superutente	Sola lettura (<code>-rorule</code>) e read-write (<code>-rwrule</code>) e <code>-superuser</code>

Di seguito sono riportati i tipi di protezione validi per ciascuno di questi tre parametri di accesso:

- `any`
- `none`
- `never`

Questo tipo di protezione non è valido per l'utilizzo con `-superuser` parametro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Quando si abbina un tipo di sicurezza di un client a ciascuno dei tre parametri di accesso, si possono ottenere tre risultati:

Se il tipo di protezione del client...	Quindi il client...
Corrisponde a quello specificato nel parametro di accesso.	Ottiene l'accesso per quel livello con il proprio ID utente.
Non corrisponde a quello specificato, ma il parametro di accesso include l'opzione <code>none</code> .	Ottiene l'accesso per quel livello, ma come utente anonimo con l'ID utente specificato da <code>-anon</code> parametro.
Non corrisponde a quello specificato e il parametro di accesso non include l'opzione <code>none</code> .	Non ottiene alcun accesso per quel livello. questo non si applica a. <code>-superuser</code> parametro perché include sempre <code>none</code> anche se non specificato.

Esempio

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

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo

NFSv3 e non ha eseguito l'autenticazione (AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono a tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura ai client con il proprio ID utente autenticato con AUTH_SYS o Kerberos v5. Il parametro superuser consente l'accesso del superutente ai client con ID utente 0 autenticati con Kerberos v5.

Pertanto, il client n. 1 ottiene l'accesso di lettura/scrittura superutente perché corrisponde a tutti e tre i parametri di accesso. Il client n. 2 ottiene l'accesso in lettura/scrittura ma non l'accesso al superutente. Il client n. 3 ottiene l'accesso in sola lettura, ma non l'accesso al superutente.

Gestire le richieste di accesso dei superutenti

Quando si configurano i criteri di esportazione, è necessario considerare ciò che si desidera che accada se il sistema storage riceve una richiesta di accesso client con ID utente 0, vale a dire come superutente, e impostare le regole di esportazione di conseguenza.

Nel mondo UNIX, un utente con ID utente 0 è noto come superutente, in genere chiamato root, che ha diritti di accesso illimitati su un sistema. L'utilizzo dei privilegi dei superutenti può essere pericoloso per diversi motivi, tra cui la violazione della sicurezza del sistema e dei dati.

Per impostazione predefinita, ONTAP esegue il mapping dei client che presentano l'ID utente 0 all'utente anonimo. Tuttavia, è possibile specificare `-superuser` Parametro nelle regole di esportazione per determinare come gestire i client che presentano ID utente 0 a seconda del tipo di protezione. Di seguito sono riportate le opzioni valide per `-superuser` parametro:

- any
- none

Questa è l'impostazione predefinita se non si specifica `-superuser` parametro.

- krb5
- ntlm
- sys

Esistono due modi diversi per gestire i client che presentano un ID utente 0, a seconda di `-superuser` configurazione dei parametri:

Se il <code>-superuser</code> parametro e tipo di sicurezza del client...	Quindi il client...
Corrispondenza	Ottiene l'accesso al superutente con ID utente 0.
Non corrispondono	Ottiene l'accesso come utente anonimo con l'ID utente specificato da <code>-anon</code> e le relative autorizzazioni assegnate. Ciò indipendentemente dal fatto che il parametro di sola lettura o di lettura/scrittura specifichi l'opzione <code>none</code> .

Se un client presenta l'ID utente 0 per accedere a un volume con lo stile di protezione NTFS e a. `-superuser` il parametro è impostato su `none`, ONTAP utilizza la mappatura dei nomi per l'utente anonimo per ottenere le credenziali corrette.

Esempio

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 746, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

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

Il client n. 2 non ottiene l'accesso superutente. Invece, viene mappato ad anonimo perché `-superuser` parametro non specificato. Ciò significa che il valore predefinito è `none` E mappa automaticamente l'ID utente 0 in anonimo. Il client n. 2 ottiene anche solo l'accesso in sola lettura perché il tipo di protezione non corrisponde al parametro di lettura/scrittura.

Esempio

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

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

utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

La regola di esportazione consente l'accesso al superutente per i client con ID utente 0. Il client n. 1 ottiene l'accesso al superutente perché corrisponde all'ID utente e al tipo di sicurezza per la modalità di sola lettura e. -superuser parametri. Il client n. 2 non ottiene l'accesso in lettura/scrittura o superutente perché il suo tipo di protezione non corrisponde al parametro di lettura/scrittura o a. -superuser parametro. Invece, il client n. 2 viene mappato all'utente anonimo, che in questo caso ha l'ID utente 0.

Modalità di utilizzo delle cache delle policy di esportazione da parte di ONTAP

Per migliorare le performance del sistema, ONTAP utilizza cache locali per memorizzare informazioni come nomi host e netgroup. Ciò consente a ONTAP di elaborare le regole delle policy di esportazione più rapidamente rispetto al recupero delle informazioni da fonti esterne. La comprensione delle cache e delle relative funzioni può aiutare a risolvere i problemi di accesso dei client.

I criteri di esportazione vengono configurati per controllare l'accesso dei client alle esportazioni NFS. Ogni policy di esportazione contiene regole e ogni regola contiene parametri che consentono di associare la regola ai client che richiedono l'accesso. Alcuni di questi parametri richiedono che ONTAP contatti un'origine esterna, ad esempio server DNS o NIS, per risolvere oggetti come nomi di dominio, nomi host o netgroup.

Queste comunicazioni con le fonti esterne richiedono una piccola quantità di tempo. Per aumentare le performance, ONTAP riduce il tempo necessario per risolvere gli oggetti delle regole dei criteri di esportazione memorizzando le informazioni in locale su ciascun nodo in diverse cache.

Nome della cache	Tipo di informazioni memorizzate
Accesso	Mappature dei client ai criteri di esportazione corrispondenti
Nome	Mapping dei nomi utente UNIX agli ID utente UNIX corrispondenti
ID	Mapping degli ID utente UNIX agli ID utente UNIX corrispondenti e agli ID gruppo UNIX estesi
Host	Mapping dei nomi host agli indirizzi IP corrispondenti
Netgroup	Mapping dei netgroup agli indirizzi IP corrispondenti dei membri
Showmount	Elenco delle directory esportate dallo spazio dei nomi SVM

Se si modificano le informazioni sui server dei nomi esterni dell'ambiente dopo il recupero e l'archiviazione in locale da parte di ONTAP, le cache potrebbero ora contenere informazioni obsolete. Sebbene ONTAP aggiorni automaticamente le cache dopo determinati periodi di tempo, diverse cache hanno tempi di scadenza e refresh e algoritmi diversi.

Un'altra possibile ragione per cui le cache contengono informazioni obsolete è quando ONTAP tenta di aggiornare le informazioni memorizzate nella cache ma incontra un errore quando tenta di comunicare con i

server dei nomi. In questo caso, ONTAP continua a utilizzare le informazioni attualmente memorizzate nelle cache locali per evitare interruzioni del client.

Di conseguenza, le richieste di accesso client che dovrebbero avere esito positivo potrebbero non riuscire e le richieste di accesso client che dovrebbero fallire potrebbero avere esito positivo. È possibile visualizzare e svuotare manualmente alcune cache delle policy di esportazione durante la risoluzione di tali problemi di accesso client.

Come funziona la cache di accesso

ONTAP utilizza una cache di accesso per memorizzare i risultati della valutazione delle regole dei criteri di esportazione per le operazioni di accesso client su un volume o qtree. Ciò comporta miglioramenti delle performance in quanto le informazioni possono essere recuperate molto più velocemente dalla cache di accesso rispetto al processo di valutazione delle regole dei criteri di esportazione ogni volta che un client invia una richiesta di i/O.

Ogni volta che un client NFS invia una richiesta di i/o per accedere ai dati su un volume o qtree, ONTAP deve valutare ogni richiesta di i/o per determinare se concedere o negare la richiesta di i/O. Questa valutazione implica il controllo di ogni regola dei criteri di esportazione dei criteri associati al volume o al qtree. Se il percorso al volume o al qtree comporta l'attraversamento di uno o più punti di giunzione, potrebbe essere necessario eseguire questa verifica per più policy di esportazione lungo il percorso.

Si noti che questa valutazione si verifica per ogni richiesta di i/o inviata da un client NFS, come lettura, scrittura, elenco, copia e altre operazioni, non solo per le richieste di montaggio iniziali.

Dopo che ONTAP ha identificato le regole dei criteri di esportazione applicabili e ha deciso se consentire o negare la richiesta, ONTAP crea una voce nella cache di accesso per memorizzare queste informazioni.

Quando un client NFS invia una richiesta di i/o, ONTAP prende nota dell'indirizzo IP del client, dell'ID della SVM e della policy di esportazione associata al volume di destinazione o al qtree, quindi verifica prima la presenza di una voce corrispondente nella cache di accesso. Se nella cache di accesso esiste una voce corrispondente, ONTAP utilizza le informazioni memorizzate per consentire o negare la richiesta di i/O. Se non esiste una voce corrispondente, ONTAP passa attraverso il normale processo di valutazione di tutte le regole di policy applicabili, come spiegato in precedenza.

Le voci della cache di accesso non utilizzate attivamente non vengono aggiornate. In questo modo si riducono le comunicazioni inutili e dispendiose con i name server esterni.

Il recupero delle informazioni dalla cache di accesso è molto più rapido rispetto all'intero processo di valutazione delle regole dei criteri di esportazione per ogni richiesta di i/O. Pertanto, l'utilizzo della cache di accesso migliora notevolmente le performance riducendo l'overhead dei controlli di accesso del client.

Come funzionano i parametri della cache di accesso

Diversi parametri controllano i periodi di refresh per le voci nella cache di accesso. La comprensione del funzionamento di questi parametri consente di modificarli per ottimizzare la cache di accesso e bilanciare le performance con la frequenza delle informazioni memorizzate.

La cache di accesso memorizza le voci costituite da una o più regole di esportazione applicabili ai client che tentano di accedere a volumi o qtree. Queste voci vengono memorizzate per un certo periodo di tempo prima dell'aggiornamento. Il tempo di refresh è determinato dai parametri della cache di accesso e dipende dal tipo di

voce della cache di accesso.

È possibile specificare i parametri della cache di accesso per le singole SVM. In questo modo, i parametri possono variare in base ai requisiti di accesso SVM. Le voci della cache di accesso che non vengono utilizzate attivamente non vengono aggiornate, il che riduce le comunicazioni inutili e dispendiose con i server di nomi esterni.

Tipo di voce della cache di accesso	Descrizione	Periodo di refresh in secondi
Voci positive	Voci della cache di accesso che non hanno portato ad un DOS (Access Denial) per i client.	Minimo: 300 Massimo: 86,400 Predefinito: 3,600
Voci negative	Voci della cache di accesso che hanno portato ad un DOS (Access Denial) per i client.	Minimo: 60 Massimo: 86,400 Predefinito: 3,600

Esempio

Un client NFS tenta di accedere a un volume su un cluster. ONTAP associa il client a una regola dei criteri di esportazione e determina che il client ottiene l'accesso in base alla configurazione della regola dei criteri di esportazione. ONTAP memorizza la regola dei criteri di esportazione nella cache di accesso come voce positiva. Per impostazione predefinita, ONTAP mantiene la voce positiva nella cache di accesso per un'ora (3,600 secondi), quindi aggiorna automaticamente la voce per mantenere aggiornate le informazioni.

Per evitare che la cache di accesso si riempia inutilmente, è disponibile un parametro aggiuntivo per cancellare le voci della cache di accesso esistenti che non sono state utilizzate per un certo periodo di tempo per decidere l'accesso del client. Questo `-harvest-timeout` il parametro ha un intervallo consentito compreso tra 60 e 2,592,000 secondi e un'impostazione predefinita di 86,400 secondi.

Rimuovere un criterio di esportazione da un qtree

Se si decide di non assegnare più un criterio di esportazione specifico a un qtree, è possibile rimuovere il criterio di esportazione modificando il qtree in modo da ereditare il criterio di esportazione del volume contenente. Per eseguire questa operazione, utilizzare `volume qtree modify` con il `-export-policy` e una stringa di nome vuota ("").

Fasi

1. Per rimuovere un criterio di esportazione da un qtree, immettere il seguente comando:

```
volume qtree modify -vserver vserver_name -qtree-path  
/vol/volume_name/qtree_name -export-policy ""
```

2. Verificare che il qtree sia stato modificato di conseguenza:

```
volume qtree show -qtree qtree_name -fields export-policy
```


Convalidare gli ID qtree per le operazioni del file qtree

ONTAP può eseguire un'ulteriore convalida facoltativa degli ID qtree. Questa convalida garantisce che le richieste di operazione del file client utilizzino un ID qtree valido e che i client possano spostare solo i file all'interno dello stesso qtree. È possibile attivare o disattivare questa convalida modificando il `-validate-qtrees-export` parametro. Questo parametro è attivato per impostazione predefinita.

A proposito di questa attività

Questo parametro è valido solo se è stata assegnata una policy di esportazione direttamente a uno o più qtree sulla macchina virtuale di storage (SVM).

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera che la convalida dell'ID qtree sia...	Immettere il seguente comando...
Attivato	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export enabled</pre>
Disattivato	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export disabled</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Restrizioni dei criteri di esportazione e giunzioni nidificate per i volumi FlexVol

Se sono stati configurati criteri di esportazione per impostare un criterio meno restrittivo su una giunzione nidificata ma un criterio più restrittivo su una giunzione di livello superiore, l'accesso alla giunzione di livello inferiore potrebbe non riuscire.

È necessario garantire che le giunzioni di livello superiore abbiano policy di esportazione meno restrittive rispetto alle giunzioni di livello inferiore.

Utilizzo di Kerberos con NFS per una maggiore sicurezza

Supporto ONTAP per Kerberos

Kerberos offre un'autenticazione sicura e sicura per le applicazioni client/server. L'autenticazione consente di verificare le identità di utenti e processi di un server. Nell'ambiente ONTAP, Kerberos fornisce l'autenticazione tra le macchine virtuali di

storage (SVM) e i client NFS.

In ONTAP 9, sono supportate le seguenti funzionalità Kerberos:

- Autenticazione Kerberos 5 con controllo dell'integrità (krb5i)

Krb5i utilizza checksum per verificare l'integrità di ogni messaggio NFS trasferito tra client e server. Ciò è utile sia per motivi di sicurezza (ad esempio, per garantire che i dati non siano stati manomessi) che per motivi di integrità dei dati (ad esempio, per prevenire la corruzione dei dati quando si utilizza NFS su reti non affidabili).

- Autenticazione Kerberos 5 con controllo della privacy (krb5p)

Krb5p utilizza checksum per crittografare tutto il traffico tra il client e il server. Questo è più sicuro e comporta un carico maggiore.

- Crittografia AES a 128 e 256 bit

Advanced Encryption Standard (AES) è un algoritmo di crittografia per la protezione dei dati elettronici. ONTAP supporta AES con chiavi a 128 bit (AES-128) e AES con chiavi a 256 bit (AES-256) per Kerberos per una maggiore protezione.

- Configurazioni di area di autenticazione Kerberos a livello di SVM

Gli amministratori di SVM possono ora creare configurazioni di area di autenticazione Kerberos a livello di SVM. Ciò significa che gli amministratori di SVM non devono più affidarsi all'amministratore del cluster per la configurazione dell'area di autenticazione Kerberos e possono creare singole configurazioni dell'area di autenticazione Kerberos in un ambiente multi-tenancy.

Requisiti per la configurazione di Kerberos con NFS

Prima di configurare Kerberos con NFS sul sistema, è necessario verificare che alcuni elementi dell'ambiente di rete e di storage siano configurati correttamente.



La procedura per configurare l'ambiente dipende dalla versione e dal tipo di sistema operativo client, controller di dominio, Kerberos, DNS e così via. che stai utilizzando. La documentazione di tutte queste variabili non rientra nell'ambito di questo documento. Per ulteriori informazioni, consultare la documentazione relativa a ciascun componente.

Per un esempio dettagliato di come configurare ONTAP e Kerberos 5 con NFSv3 e NFSv4 in un ambiente che utilizza Active Directory di Windows Server 2008 R2 e host Linux, consultare il report tecnico 4073.

È necessario configurare prima i seguenti elementi:

Requisiti dell'ambiente di rete

- Kerberos

È necessario disporre di una configurazione Kerberos funzionante con un centro di distribuzione delle chiavi (KDC), ad esempio Kerberos basato su Windows Active Directory o MIT Kerberos.

I server NFS devono utilizzare `nfs` come componente principale del computer.

- Servizio di directory

È necessario utilizzare un servizio directory sicuro nell'ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS.

- NTP

È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolvibili correttamente tramite DNS.

- Account utente

Ogni client deve disporre di un account utente nell'area Kerberos. I server NFS devono utilizzare "nfs" come componente principale del computer.

Requisiti del client NFS

- NFS

Ciascun client deve essere configurato correttamente per comunicare in rete utilizzando NFSv3 o NFSv4.

I client devono supportare RFC1964 e RFC2203.

- Kerberos

Ciascun client deve essere configurato correttamente per utilizzare l'autenticazione Kerberos, inclusi i seguenti dettagli:

- La crittografia per la comunicazione TGS è attivata.

AES-256 per la massima sicurezza.

- Il tipo di crittografia più sicuro per la comunicazione TGT è attivato.
- Il dominio e l'area di autenticazione Kerberos sono configurati correttamente.
- Il GSS è attivato.

Quando si utilizzano le credenziali del computer:

- Non eseguire `gssd` con `-n` parametro.
- Non eseguire `kinit` come utente root.

- Ogni client deve utilizzare la versione più recente e aggiornata del sistema operativo.

In questo modo si ottiene la migliore compatibilità e affidabilità per la crittografia AES con Kerberos.

- DNS

Ciascun client deve essere configurato correttamente per utilizzare il DNS per la corretta risoluzione dei

nomi.

- NTP

Ciascun client deve essere sincronizzato con il server NTP.

- Informazioni su host e dominio

Di ogni client `/etc/hosts` e `/etc/resolv.conf` i file devono contenere rispettivamente il nome host e le informazioni DNS corretti.

- File keytab

Ogni client deve avere un file keytab dal KDC. L'area di autenticazione deve essere in lettere maiuscole. Il tipo di crittografia deve essere AES-256 per garantire la massima sicurezza.

- Opzionale: Per ottenere le migliori performance, i client traggono vantaggio dalla presenza di almeno due interfacce di rete: Una per la comunicazione con la rete locale e una per la comunicazione con la rete di storage.

Requisiti di sistema per lo storage

- Licenza NFS

Il sistema storage deve avere una licenza NFS valida installata.

- Licenza CIFS

La licenza CIFS è opzionale. È necessario solo per il controllo delle credenziali Windows quando si utilizza la mappatura dei nomi multiprotocollo. Non è richiesto in un ambiente UNIX-only rigoroso.

- SVM

È necessario configurare almeno una SVM sul sistema.

- DNS su SVM

È necessario aver configurato il DNS su ogni SVM.

- Server NFS

È necessario aver configurato NFS su SVM.

- Crittografia AES

Per una maggiore sicurezza, è necessario configurare il server NFS in modo che consenta solo la crittografia AES-256 per Kerberos.

- Server SMB

Se si utilizza un ambiente multiprotocollo, è necessario aver configurato SMB su SVM. Il server SMB è necessario per la mappatura dei nomi multiprotocollo.

- Volumi

È necessario disporre di un volume root e di almeno un volume di dati configurati per l'utilizzo da parte di

SVM.

- Volume root

Il volume root di SVM deve avere la seguente configurazione:

Nome	Impostazione
Stile di sicurezza	UNIX
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	777

A differenza del volume root, i volumi di dati possono avere uno stile di sicurezza.

- Gruppi UNIX

La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0
pcuser	65534 (creato automaticamente da ONTAP quando si crea la SVM)

- Utenti UNIX

La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	Necessario per la fase DI INIT GSS Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.

Nome utente	ID utente	ID gruppo primario	Commento
pcuser	65534	65534	Necessario per l'utilizzo multiprotocollo NFS e CIFS Creato e aggiunto automaticamente al gruppo pcuser da ONTAP quando si crea la SVM.
root	0	0	Necessario per il montaggio

L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.

- Policy e regole di esportazione

È necessario aver configurato i criteri di esportazione con le regole di esportazione necessarie per i volumi root e dati e qtree. Se si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e. `-superuser` per il volume root a. `krb5`, `krb5i`, o. `krb5p`.

- Mappatura dei nomi Kerberos-UNIX

Se si desidera che l'utente identificato dall'utente client NFS SPN disponga delle autorizzazioni root, è necessario creare una mappatura dei nomi nella directory root.

Informazioni correlate

["Report tecnico di NetApp 4073: Autenticazione unificata sicura"](#)

["Tool di matrice di interoperabilità NetApp"](#)

["Amministrazione del sistema"](#)

["Gestione dello storage logico"](#)

Specificare il dominio ID utente per NFSv4

Per specificare il dominio ID utente, è possibile impostare `-v4-id-domain` opzione.

A proposito di questa attività

Per impostazione predefinita, ONTAP utilizza il dominio NIS per il mapping dell'ID utente NFSv4, se impostato. Se non viene impostato un dominio NIS, viene utilizzato il dominio DNS. Potrebbe essere necessario impostare il dominio ID utente se, ad esempio, si dispone di più domini ID utente. Il nome di dominio deve corrispondere alla configurazione del dominio sul controller di dominio. Non è richiesto per NFSv3.

Fase

1. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configurare i name service

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
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	<pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre>
nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	<pre>vserver services name- service ldap</pre>
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	<pre>vserver services name- service dns</pre>

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
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
```

Vserver	Database	Source Order
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

Per cercare gli indirizzi IP degli host, ONTAP consulta innanzitutto i file di origine locali. Se la query non restituisce alcun risultato, i server DNS vengono controllati in seguito.

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.

Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Utilizzare LDAP

Panoramica LDAP

Un server LDAP (Lightweight Directory Access Protocol) consente di gestire centralmente le informazioni dell'utente. Se si memorizza il database utente su un server LDAP nell'ambiente in uso, è possibile configurare il sistema di storage in modo che cerchi le informazioni utente nel database LDAP esistente.

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
 - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
 - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
 - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
 - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).
 - Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

Sono disponibili le seguenti opzioni di sicurezza della sessione:

- Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
- AVVIARE TLS
- LDAPS (LDAP su TLS o SSL)
- Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
 - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
 - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
 - I server Kerberos devono avere record SRV presenti sul server DNS.
- Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
 - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
 - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
 - Nel dominio deve essere già configurato un server dei certificati.
- Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
 - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
 - Bidirezionale
 - Unidirezionale, in cui il primario si affida al dominio di riferimento
 - Genitore-figlio
 - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
 - Le password di dominio devono essere le stesse per autenticare quando `--bind-as-cifs -server` impostare su true.



Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.

- Per tutte le versioni di ONTAP:
- Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
- Firma e sigillatura LDAP (il `-session-security` opzionale)
- Connessioni TLS crittografate (il `-use-start-tls` opzionale)
- Comunicazioni tramite la porta LDAPS 636 (la `-use-ldaps-for-ad-ldap` opzionale)

- A partire da ONTAP 9.11.1, è possibile utilizzare ["LDAP fast bind per l'autenticazione nsswitch."](#)
- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

Per ulteriori informazioni, vedere ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#).

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 NFS 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`. test

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

Concetti LDAPS

È necessario comprendere alcuni termini e concetti relativi al modo in cui ONTAP protegge le comunicazioni LDAP. ONTAP può utilizzare TLS O LDAPS DI AVVIO per impostare sessioni autenticate tra server LDAP integrati in Active Directory o server LDAP basati su UNIX.

Terminologia

È necessario comprendere alcuni termini relativi all'utilizzo di LDAPS da parte di ONTAP per proteggere le comunicazioni LDAP.

• LDAP

(Lightweight Directory Access Protocol) protocollo per l'accesso e la gestione delle directory di informazioni. LDAP viene utilizzato come directory di informazioni per la memorizzazione di oggetti come utenti, gruppi e netgroup. LDAP fornisce inoltre servizi di directory che gestiscono questi oggetti e soddisfano le richieste LDAP dai client LDAP.

• SSL

(Secure Sockets Layer) protocollo sviluppato per l'invio sicuro di informazioni su Internet. SSL è supportato da ONTAP 9 e versioni successive, ma è stato deprecato a favore di TLS.

• TLS

(Transport Layer Security) un protocollo di tracciamento degli standard IETF basato sulle specifiche SSL precedenti. È il successore di SSL. TLS è supportato da ONTAP 9,5 e versioni successive.

• LDAPS (LDAP su SSL o TLS)

Protocollo che utilizza TLS o SSL per proteggere le comunicazioni tra client LDAP e server LDAP. I termini *LDAP su SSL* e *LDAP su TLS* vengono talvolta utilizzati in modo intercambiabile. LDAPS è supportato da ONTAP 9,5 e versioni successive.

- In ONTAP 9.5-9.8, LDAPS può essere attivato solo sulla porta 636. A tale scopo, utilizzare `-use -ldaps-for-ad-ldap` con il `vserver cifs security modify` comando.
- A partire da ONTAP 9.9.1, LDAPS può essere attivato su qualsiasi porta, anche se la porta 636 rimane quella predefinita. A tale scopo, impostare `-ldaps-enabled` parametro a `true` e specificare il desiderato `-port` parametro. Per ulteriori informazioni, consultare `vserver services name-service ldap client create` pagina man



L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.

• Avvia TLS

(Noto anche come *start_tls*, *STARTTLS* e *STARTTLS*) un meccanismo per fornire comunicazioni sicure utilizzando i protocolli TLS.

ONTAP utilizza STARTTLS per proteggere la comunicazione LDAP e la porta LDAP predefinita (389) per comunicare con il server LDAP. Il server LDAP deve essere configurato in modo da consentire le connessioni sulla porta LDAP 389; in caso contrario, le connessioni LDAP TLS dalla SVM al server LDAP non funzionano.

Utilizzo di LDAPS da parte di ONTAP

ONTAP supporta l'autenticazione del server TLS, che consente al client LDAP SVM di confermare l'identità del server LDAP durante l'operazione di binding. I client LDAP abilitati per TLS possono utilizzare tecniche standard di crittografia a chiave pubblica per verificare che il certificato e l'ID pubblico di un server siano validi e siano stati emessi da un'autorità di certificazione (CA) elencata nell'elenco delle CA attendibili del client.

LDAP supporta STARTTLS per crittografare le comunicazioni utilizzando TLS. STARTTLS inizia come connessione non crittografata sulla porta LDAP standard (389) e la connessione viene quindi aggiornata a TLS.

ONTAP supporta:

- LDAPS per il traffico SMB tra i server LDAP integrati in Active Directory e SVM
- LDAPS per il traffico LDAP per la mappatura dei nomi e altre informazioni UNIX

I server LDAP integrati in Active Directory o i server LDAP basati su UNIX possono essere utilizzati per memorizzare informazioni per la mappatura dei nomi LDAP e altre informazioni UNIX, come utenti, gruppi e netgroup.

- Certificati della CA principale autofirmati

Quando si utilizza un LDAP integrato in Active-Directory, il certificato root autofirmato viene generato quando il servizio certificati di Windows Server viene installato nel dominio. Quando si utilizza un server LDAP basato su UNIX per la mappatura dei nomi LDAP, il certificato root autofirmato viene generato e salvato utilizzando i mezzi appropriati per l'applicazione LDAP.

Per impostazione predefinita, LDAPS è disattivato.

Attiva il supporto LDAP RFC2307bis

Se si desidera utilizzare LDAP e si desidera utilizzare le appartenenze a gruppi nidificati, è possibile configurare ONTAP per abilitare il supporto di LDAP RFC2307bis.

Di cosa hai bisogno

È necessario aver creato una copia di uno degli schemi client LDAP predefiniti che si desidera utilizzare.

A proposito di questa attività

Negli schemi client LDAP, gli oggetti di gruppo utilizzano l'attributo `memberUid`. Questo attributo può contenere più valori ed elenca i nomi degli utenti che appartengono a quel gruppo. Negli schemi client LDAP abilitati per RFC2307bis, gli oggetti di gruppo utilizzano l'attributo `uniqueMember`. Questo attributo può contenere il nome distinto completo (DN) di un altro oggetto nella directory LDAP. In questo modo è possibile utilizzare gruppi nidificati poiché i gruppi possono avere altri gruppi come membri.

L'utente non deve essere membro di più di 256 gruppi, inclusi i gruppi nidificati. ONTAP ignora tutti i gruppi che superano il limite di 256 gruppi.

Per impostazione predefinita, il supporto RFC2307bis è disattivato.



Il supporto RFC2307bis viene attivato automaticamente in ONTAP quando viene creato un client LDAP con lo schema MS-ad-BIS.

Per ulteriori informazioni, vedere ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#).

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modificare lo schema del client LDAP RFC2307 copiato per abilitare il supporto RFC2307bis:

```
vserver services name-service ldap client schema modify -vserver vserver_name  
-schema schema-name -enable-rfc2307bis true
```

3. Modificare lo schema in modo che corrisponda alla classe di oggetti supportata nel server LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modificare lo schema in modo che corrisponda al nome dell'attributo supportato nel server LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -unique-member-attribute attribute_name
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Opzioni di configurazione per le ricerche nelle directory LDAP

È possibile ottimizzare le ricerche nelle directory LDAP, incluse le informazioni relative a utenti, gruppi e netgroup, configurando il client LDAP di ONTAP per la connessione ai server LDAP nel modo più appropriato per il proprio ambiente. È necessario capire quando sono sufficienti i valori di ricerca predefiniti di base e ambito LDAP e quali parametri specificare quando i valori personalizzati sono più appropriati.

Le opzioni di ricerca del client LDAP per le informazioni relative a utenti, gruppi e netgroup possono aiutare a evitare query LDAP non riuscite e, di conseguenza, l'accesso del client ai sistemi di storage non riuscito. Inoltre, contribuiscono a garantire che le ricerche siano il più efficienti possibile per evitare problemi di performance del client.

Valori di base e di ricerca dell'ambito predefiniti

La base LDAP è il DN di base predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando il DN di base. Questa opzione è appropriata quando la directory LDAP è relativamente piccola e tutte le voci pertinenti si trovano nello stesso DN.

Se non si specifica un DN di base personalizzato, il valore predefinito è `root`. Ciò significa che ogni query esegue la ricerca nell'intera directory. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

L'ambito di base LDAP è l'ambito di ricerca predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando l'ambito di base. Determina se la query LDAP ricerca solo la voce denominata, le voci di un livello al di sotto del DN o l'intera sottostruttura al di sotto del DN.

Se non si specifica un ambito di base personalizzato, il valore predefinito è `subtree`. Ciò significa che ogni query esegue la ricerca nell'intero sottostruttura sotto il DN. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

Valori di ricerca di base e ambito personalizzati

In alternativa, è possibile specificare valori di base e di ambito separati per le ricerche di utenti, gruppi e netgroup. La limitazione della base di ricerca e dell'ambito delle query in questo modo può migliorare significativamente le prestazioni, poiché limita la ricerca a una sottosezione più piccola della directory LDAP.

Se si specificano valori di base e ambito personalizzati, questi sovrascrivono la base di ricerca predefinita generale e l'ambito per le ricerche di utenti, gruppi e netgroup. I parametri per specificare i valori di base e ambito personalizzati sono disponibili a livello di privilegio avanzato.

Parametro client LDAP...	Specifica custom...
<code>-base-dn</code>	DN di base per tutte le ricerche LDAP è possibile inserire più valori, se necessario (ad esempio, se la funzione LDAP referral chasing è attivata in ONTAP 9.5 e versioni successive).
<code>-base-scope</code>	Ambito di base per tutte le ricerche LDAP
<code>-user-dn</code>	DNS di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di mappatura dei nomi utente.
<code>-user-scope</code>	Ambito di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di associazione dei nomi utente.

<code>-group-dn</code>	DNS di base per tutte le ricerche di gruppi LDAP
<code>-group-scope</code>	Ambito di base per tutte le ricerche di gruppi LDAP
<code>-netgroup-dn</code>	DNS di base per tutte le ricerche dei netgroup LDAP
<code>-netgroup-scope</code>	Ambito di base per tutte le ricerche dei netgroup LDAP

Più valori DN di base personalizzati

Se la struttura della directory LDAP è più complessa, potrebbe essere necessario specificare più DNS di base per cercare determinate informazioni in più parti della directory LDAP. È possibile specificare più DNS per i parametri DN dell'utente, del gruppo e del netgroup separandoli con un punto e virgola (;) e racchiudendo l'intero elenco di ricerca DN con virgolette doppie ("). Se un DN contiene un punto e virgola, è necessario aggiungere un carattere di escape (\) immediatamente prima del punto e virgola nel DN.

Si noti che l'ambito si applica all'intero elenco di DNS specificato per il parametro corrispondente. Ad esempio, se si specifica un elenco di tre diversi DNS utente e sottostruttura per l'ambito utente, l'utente LDAP ricerca nell'intera sottostruttura ciascuno dei tre DNS specificati.

A partire da ONTAP 9.5, è anche possibile specificare LDAP *referral chasing*, che consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario non restituisce una risposta di riferimento LDAP. Il client utilizza i dati di riferimento per recuperare l'oggetto di destinazione dal server descritto nei dati di riferimento. Per cercare oggetti presenti nei server LDAP indicati, è possibile aggiungere la base-dn degli oggetti indicati alla base-dn come parte della configurazione del client LDAP. Tuttavia, gli oggetti referralati vengono ricercati solo quando è attivata la funzione di referral chasing (ricerca riferimenti), utilizzando il `-referral-enabled true` Durante la creazione o la modifica del client LDAP.

Migliorare le performance delle ricerche di directory LDAP netgroup-by-host

Se l'ambiente LDAP è configurato per consentire ricerche netgroup-by-host, è possibile configurare ONTAP in modo che ne tragga vantaggio ed eseguire ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup e ridurre i possibili problemi di accesso al client NFS dovuti alla latenza durante le ricerche dei netgroup.

Di cosa hai bisogno

La directory LDAP deve contenere un `netgroup.byhost` mappa.

I server DNS devono contenere record di ricerca sia in avanti (A) che in retromarcia (PTR) per i client NFS.

Quando si specificano gli indirizzi IPv6 nei netgroup, è sempre necessario accorciare e comprimere ciascun indirizzo come specificato in RFC 5952.

A proposito di questa attività

I server NIS memorizzano le informazioni del netgroup in tre mappe distinte denominate `netgroup`, `netgroup.byuser`, e `netgroup.byhost`. Lo scopo di `netgroup.byuser` e `netgroup.byhost` maps consente di velocizzare le ricerche di netgroup. ONTAP può eseguire ricerche netgroup-by-host sui server NIS per migliorare i tempi di risposta del montaggio.

Per impostazione predefinita, le directory LDAP non dispongono di tale opzione `netgroup.byhost` mappare come i server NIS. Tuttavia, con l'aiuto di strumenti di terze parti, è possibile importare un NIS `netgroup.byhost` eseguire la mappatura nelle directory LDAP per consentire ricerche rapide `netgroup-by-host`. Se l'ambiente LDAP è stato configurato per consentire ricerche `netgroup-by-host`, è possibile configurare il client LDAP ONTAP con `netgroup.byhost` nome mappa, DN e ambito di ricerca per ricerche più rapide tra `netgroup` e `host`.

La ricezione più rapida dei risultati per le ricerche `netgroup-by-host` consente a ONTAP di elaborare più rapidamente le regole di esportazione quando i client NFS richiedono l'accesso alle esportazioni. In questo modo si riduce la possibilità di ritardi di accesso dovuti a problemi di latenza della ricerca nel `netgroup`.

Fasi

1. Ottenere l'esatto nome completo del NIS `netgroup.byhost` mappatura importata nella directory LDAP.

Il DN della mappa può variare a seconda dello strumento di terze parti utilizzato per l'importazione. Per ottenere prestazioni ottimali, specificare il DN esatto della mappa.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Abilitare le ricerche `netgroup-by-host` nella configurazione client LDAP della macchina virtuale di storage (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` Attiva o disattiva la ricerca `netgroup-by-host` delle directory LDAP. L'impostazione predefinita è `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` specifica il nome distinto di `netgroup.byhost` mappare la directory LDAP. Sovrascrive il DN di base per le ricerche `netgroup-by-host`. Se non si specifica questo parametro, ONTAP utilizza invece il DN di base.

`-netgroup-byhost-scope {base|onelevel subtree}` specifica l'ambito di ricerca per le ricerche `netgroup-by-host`. Se non si specifica questo parametro, l'impostazione predefinita è `subtree`.

Se la configurazione del client LDAP non esiste ancora, è possibile attivare le ricerche `netgroup-by-host` specificando questi parametri quando si crea una nuova configurazione del client LDAP utilizzando `vserver services name-service ldap client create` comando.



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

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

Esempio

Il seguente comando modifica la configurazione del client LDAP esistente denominata `ldap_corp` per abilitare le ricerche `netgroup-by-host` utilizzando `netgroup.byhost` mappa denominata `"nisMapName="netgroup.byhost",DC=corp,DC=example,DC=com"` e l'ambito di ricerca predefinito `subtree`:


```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Al termine

Il `netgroup.byhost` e `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client.

Informazioni correlate

["IETF RFC 5952: Una raccomandazione per la rappresentazione del testo dell'indirizzo IPv6"](#)

Utilizza il binding rapido LDAP per l'autenticazione nsswitch

A partire da ONTAP 9.11.1, è possibile sfruttare la funzionalità LDAP *fast bind* (nota anche come *Concurrent BIND*) per richieste di autenticazione client più semplici e veloci. Per utilizzare questa funzionalità, il server LDAP deve supportare la funzionalità di associazione rapida.

A proposito di questa attività

Senza il binding rapido, ONTAP utilizza il binding semplice LDAP per autenticare gli utenti amministratori con il server LDAP. Con questo metodo di autenticazione, ONTAP invia un nome utente o di gruppo al server LDAP, riceve la password hash memorizzata e confronta il codice hash del server con il codice hash generato localmente dalla password utente. Se sono identici, ONTAP concede l'autorizzazione di accesso.

Grazie alla funzionalità di associazione rapida, ONTAP invia solo le credenziali utente (nome utente e password) al server LDAP tramite una connessione sicura. Il server LDAP convalida quindi queste credenziali e richiede a ONTAP di concedere le autorizzazioni di accesso.

Uno dei vantaggi di fast bind è che non è necessario che ONTAP supporti ogni nuovo algoritmo di hashing supportato dai server LDAP, perché l'hashing delle password viene eseguito dal server LDAP.

"Scopri come utilizzare fast bind."

È possibile utilizzare le configurazioni client LDAP esistenti per l'associazione rapida LDAP. Tuttavia, si consiglia vivamente di configurare il client LDAP per TLS o LDAPS; in caso contrario, la password viene inviata via cavo in testo normale.

Per abilitare il binding rapido LDAP in un ambiente ONTAP, è necessario soddisfare i seguenti requisiti:

- Gli utenti admin di ONTAP devono essere configurati su un server LDAP che supporti il fast bind.
- ONTAP SVM deve essere configurato per LDAP nel database name Services switch (nsswitch).
- Gli account di gruppo e utente amministratore di ONTAP devono essere configurati per l'autenticazione nsswitch utilizzando il collegamento rapido.

Fasi

1. Verificare con l'amministratore LDAP che il collegamento rapido LDAP sia supportato sul server LDAP.
2. Assicurarsi che le credenziali dell'utente amministratore di ONTAP siano configurate sul server LDAP.
3. Verificare che l'amministratore o l'SVM dei dati sia configurato correttamente per il binding rapido LDAP.

- a. Per confermare che il server fast bind LDAP è elencato nella configurazione del client LDAP, immettere:

```
vserver services name-service ldap client show
```

["Informazioni sulla configurazione del client LDAP."](#)

- b. Per confermare ldap è una delle sorgenti configurate per nsswitch passwd database, inserire:

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

["Scopri di più sulla configurazione di nsswitch."](#)

4. Assicurarsi che gli utenti admin stiano autenticando con nsswitch e che l'autenticazione LDAP fast bind sia attivata nei propri account.

- Per gli utenti esistenti, immettere `security login modify` e verificare le seguenti impostazioni dei parametri:

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```

- Per i nuovi utenti admin, vedere ["Abilitare l'accesso all'account LDAP o NIS."](#)

Visualizzare le statistiche LDAP

A partire da ONTAP 9.2, è possibile visualizzare le statistiche LDAP per le macchine virtuali di storage (SVM) su un sistema storage per monitorare le performance e diagnosticare i problemi.

Di cosa hai bisogno

- È necessario aver configurato un client LDAP su SVM.
- Gli oggetti LDAP da cui è possibile visualizzare i dati devono essere stati identificati.

Fase

1. Visualizzare i dati delle performance per gli oggetti del contatore:

```
statistics show
```

Esempi

Nell'esempio riportato di seguito vengono illustrati i dati relativi alle prestazioni per l'oggetto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

Object: secd_external_service_op

Instance: vserverName:LDAP (NIS & Name

Mapping):GetUserInfoFromName:1.1.1.1

Start-time: 4/13/2016 22:15:38

End-time: 4/13/2016 22:15:38

Scope: vserverName

Counter	Value
instance_name	vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName: 1.1.1.1
last_modified_time	1460610787
node_name	nodeName
num_not_found_responses	1
num_request_failures	1
num_requests_sent	1
num_responses_received	1
num_successful_responses	0
num_timeouts	0
operation	GetUserInfoFromName
process_name	secd
request_latency	52131us

Configurare le mappature dei nomi

Panoramica sulla configurazione delle mappature dei nomi

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

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 SMB 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 SMB 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 SMB possono essere un trust bidirezionale o uno dei due tipi di trust unidirezionali, un trust in

entrata o un trust in uscita. Il dominio principale è il dominio a cui appartiene il server SMB sulla SVM.

- *Fiducia bidirezionale*

Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server SMB 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 SMB. 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 di *\\	L'utente UNIX "root" viene mappato all'utente "Administrator". Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente "Administrator".

Schema	Sostituzione	Risultato
*	**	<p>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.</p> <div>  <p>Il modello {asterisco}\\{asterisco} è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.</p> </div>

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 riconnersi 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.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Configurare l'utente UNIX predefinito	<code>vserver cifs options modify -default-unix-user user_name</code>
Configurare l'utente Windows predefinito	<code>vserver nfs modify -default-win-user user_name</code>

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	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>
Scambiare la posizione di due mappature dei nomi NOTA: Non è consentito eseguire uno swap quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	<code>vserver name-mapping swap</code>
Modificare una mappatura dei nomi	<code>vserver name-mapping modify</code>

Eliminare una mappatura dei nomi	<code>vserver name-mapping delete</code>
Convalidare la corretta mappatura dei nomi	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

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

Abilitare l'accesso per i client NFS di Windows

ONTAP supporta l'accesso ai file dai client NFSv3 di Windows. Ciò significa che i client che eseguono sistemi operativi Windows con supporto NFSv3 possono accedere ai file delle esportazioni NFSv3 nel cluster. Per utilizzare correttamente questa funzionalità, è necessario configurare correttamente la macchina virtuale di storage (SVM) ed essere consapevoli di determinati requisiti e limitazioni.

A proposito di questa attività

Per impostazione predefinita, il supporto del client Windows NFSv3 è disattivato.

Prima di iniziare

NFSv3 deve essere attivato su SVM.

Fasi

1. Abilitare il supporto del client Windows NFSv3:

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
```

2. Su tutti gli SVM che supportano i client Windows NFSv3, disattivare `-enable-ejukebox` e `-v3 -connection-drop` parametri:

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
```

I client Windows NFSv3 possono ora montare le esportazioni sul sistema storage.

3. Assicurarsi che ogni client Windows NFSv3 utilizzi i supporti rigidi specificando `-o mtype=hard` opzione.

Questo è necessario per garantire montaggi affidabili.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Abilitare la visualizzazione delle esportazioni NFS sui client NFS

I client NFS possono utilizzare `showmount -e` Per visualizzare un elenco delle esportazioni disponibili da un server NFS ONTAP. In questo modo, gli utenti possono identificare il file system che desiderano montare.

A partire da ONTAP 9.2, ONTAP consente ai client NFS di visualizzare l'elenco di esportazione per

impostazione predefinita. Nelle versioni precedenti, il `showmount` opzione di `vserver nfs modify` il comando deve essere attivato in modo esplicito. Per visualizzare l'elenco di esportazione, è necessario attivare NFSv3 su SVM.

Esempio

Il seguente comando mostra la funzione `showmount` sulla SVM denominata `vs1`:

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

Il seguente comando eseguito su un client NFS visualizza l'elenco delle esportazioni su un server NFS con l'indirizzo IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

Gestire l'accesso ai file con NFS

Attivare o disattivare NFSv3

È possibile attivare o disattivare NFSv3 modificando il `-v3` opzione. Ciò consente l'accesso ai file per i client che utilizzano il protocollo NFSv3. Per impostazione predefinita, NFSv3 è attivato.

Fase

- 1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
Disattiva NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

Attivare o disattivare NFSv4.0

È possibile attivare o disattivare NFSv4.0 modificando il `-v4.0` opzione. Questo consente l'accesso al file per i client che utilizzano il protocollo NFSv4.0. In ONTAP 9.9.1, NFSv4.0 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare NFSv4.0	<pre>vserver nfs modify -vserver vserver_name -v4.0 enabled</pre>
Disattiva NFSv4.0	<pre>vserver nfs modify -vserver vserver_name -v4.0 disabled</pre>

Attivare o disattivare NFSv4.1

È possibile attivare o disattivare NFSv4.1 modificando il `-v4.1` opzione. Ciò consente l'accesso ai file per i client che utilizzano il protocollo NFSv4.1. In ONTAP 9.9.1, NFSv4.1 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4.1 enabled</pre>
Disattiva NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4.1 disabled</pre>

Gestire i limiti dello storepool di NFSv4

A partire da ONTAP 9.13, gli amministratori possono consentire ai server NFSv4 di negare le risorse ai client NFSv4 quando raggiungono i limiti di risorse dello storepool per client. Quando i client consumano troppe risorse dello storepool NFSv4, questo può causare il blocco di altri client NFSv4 a causa della mancata disponibilità delle risorse dello storepool NFSv4.

L'attivazione di questa funzionalità consente inoltre ai clienti di visualizzare il consumo attivo delle risorse dello storepool da parte di ciascun client. Ciò semplifica l'identificazione dei client che esauriscono le risorse di sistema e consente di imporre limiti di risorse per client.

Visualizza le risorse dello storepool consumate

Il `vserver nfs storepool show` comando mostra il numero di risorse dello storepool utilizzate. Uno storepool è un pool di risorse utilizzate dai client NFSv4.

Fase

1. In qualità di amministratore, eseguire `vserver nfs storepool show` Per visualizzare le informazioni sullo storepool dei client NFSv4.

Esempio

In questo esempio vengono visualizzate le informazioni sullo storepool dei client NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

Attiva o disattiva i controlli dei limiti dello storepool

Gli amministratori possono utilizzare i seguenti comandi per attivare o disattivare i controlli dei limiti dello storepool.

Fase

1. In qualità di amministratore, eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare i controlli dei limiti dello storepool	<code>vserver nfs storepool config modify -limit-enforce enabled</code>
Disattiva i controlli dei limiti di storepool	<code>vserver nfs storepool config modify -limit-enforce disabled</code>

Visualizzare un elenco di client bloccati

Se il limite di storepool è attivato, gli amministratori possono vedere quali client sono stati bloccati al raggiungimento della soglia di risorse per client. Gli amministratori possono utilizzare il seguente comando per vedere quali client sono stati contrassegnati come client bloccati.

Fasi

1. Utilizzare `vserver nfs storepool blocked-client show` Per visualizzare l'elenco dei client NFSv4 bloccati.

Rimuovere un client dall'elenco dei client bloccati

I client che raggiungono la soglia per client verranno disconnessi e aggiunti alla cache del client a blocchi. Gli amministratori possono utilizzare il seguente comando per rimuovere il client dalla cache del client a blocchi. In questo modo, il client potrà connettersi al server NFSV4 di ONTAP.

Fasi

1. Utilizzare `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando per svuotare la cache del client bloccato nello storepool.
2. Utilizzare `vserver nfs storepool blocked-client show` comando per verificare che il client sia stato rimosso dalla cache del client a blocchi.

Esempio

In questo esempio viene visualizzato un client bloccato con l'indirizzo IP "10.2.1.1" che viene liberato da tutti i nodi.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

Abilitare o disabilitare pNFS

PNFS migliora le performance consentendo ai client NFS di eseguire operazioni di lettura/scrittura direttamente e in parallelo sui dispositivi di storage, ignorando il server NFS come potenziale collo di bottiglia. Per attivare o disattivare pNFS (Parallel NFS), è possibile modificare `-v4.1-pnfs` opzione.

Se la versione di ONTAP è...	Il valore predefinito di pNFS è...
9.8 o versione successiva	disattivato
9.7 o versioni precedenti	attivato

Di cosa hai bisogno

Il supporto di NFSv4.1 è necessario per poter utilizzare pNFS.

Se si desidera attivare pNFS, è necessario prima disattivare i riferimenti NFS. Non è possibile abilitare entrambi contemporaneamente.

Se si utilizza pNFS con Kerberos su SVM, è necessario attivare Kerberos su ogni LIF su SVM.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</pre>
Disattiva pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</pre>

Informazioni correlate

- [Panoramica del trunking NFS](#)

Controlla l'accesso NFS su TCP e UDP

È possibile attivare o disattivare l'accesso NFS alle macchine virtuali di storage (SVM) su TCP e UDP modificando il `-tcp` e `-udp` parametri, rispettivamente. In questo modo è possibile controllare se i client NFS possono accedere ai dati tramite TCP o UDP nel proprio ambiente.

A proposito di questa attività

Questi parametri si applicano solo a NFS. Non influiscono sui protocolli ausiliari. Ad esempio, se NFS su TCP è disattivato, le operazioni di montaggio su TCP continuano a avere successo. Per bloccare completamente il traffico TCP o UDP, è possibile utilizzare le regole dei criteri di esportazione.



È necessario disattivare SnapDiff RPC Server prima di disattivare TCP per NFS per evitare un errore di comando non riuscito. È possibile disattivare il protocollo TCP utilizzando il comando `vserver snapdiff-rpc-server off -vserver vserver_name`.

Fase

1. Eseguire una delle seguenti operazioni:

Se vuoi che l'accesso NFS sia...	Immettere il comando...
Abilitato su TCP	<pre>vserver nfs modify -vserver vserver_name -tcp enabled</pre>
Disattivato su TCP	<pre>vserver nfs modify -vserver vserver_name -tcp disabled</pre>
Abilitato su UDP	<pre>vserver nfs modify -vserver vserver_name -udp enabled</pre>
Disattivato su UDP	<pre>vserver nfs modify -vserver vserver_name -udp disabled</pre>

Controllo delle richieste NFS da porte non riservate

È possibile rifiutare le richieste di montaggio NFS da porte non riservate attivando `-mount-rootonly` opzione. Per rifiutare tutte le richieste NFS da porte non riservate, è possibile attivare `-nfs-rootonly` opzione.

A proposito di questa attività

Per impostazione predefinita, l'opzione `-mount-rootonly` è enabled.

Per impostazione predefinita, l'opzione `-nfs-rootonly` è disabled.

Queste opzioni non si applicano alla procedura NULL.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Consenti richieste di montaggio NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code>
Rifiutare le richieste di montaggio NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>
Consenti tutte le richieste NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>
Rifiutare tutte le richieste NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code>

Gestire l'accesso NFS a volumi NTFS o qtree per utenti UNIX sconosciuti

Se ONTAP non riesce a identificare gli utenti UNIX che tentano di connettersi a volumi o qtree con lo stile di protezione NTFS, non può quindi mappare esplicitamente l'utente a un utente Windows. È possibile configurare ONTAP in modo che neghi l'accesso a tali utenti per una protezione più rigorosa oppure mapparli a un utente Windows predefinito per garantire un livello minimo di accesso a tutti gli utenti.

Di cosa hai bisogno

Se si desidera attivare questa opzione, è necessario configurare un utente Windows predefinito.

A proposito di questa attività

Se un utente UNIX tenta di accedere a volumi o qtree con uno stile di protezione NTFS, l'utente UNIX deve prima essere mappato a un utente Windows in modo che ONTAP possa valutare correttamente le autorizzazioni NTFS. Tuttavia, se ONTAP non riesce a cercare il nome dell'utente UNIX nelle origini del servizio nome informazioni utente configurate, non può eseguire il mapping esplicito dell'utente UNIX a un utente Windows specifico. È possibile decidere come gestire tali utenti UNIX sconosciuti nei seguenti modi:

- Negare l'accesso a utenti UNIX sconosciuti.

In questo modo viene garantita una sicurezza più rigorosa, richiedendo il mapping esplicito per tutti gli utenti UNIX per ottenere l'accesso ai volumi NTFS o ai qtree.

- Associare utenti UNIX sconosciuti a un utente Windows predefinito.

In questo modo si ottiene meno sicurezza, ma maggiore praticità, garantendo a tutti gli utenti un livello minimo di accesso ai volumi NTFS o ai qtree tramite un utente Windows predefinito.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera utilizzare l'utente Windows predefinito per utenti UNIX sconosciuti...	Immettere il comando...
Attivato	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code>
Disattivato	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Considerazioni per i client che montano le esportazioni NFS utilizzando una porta non riservata

Il `-mount-rootonly` L'opzione deve essere disattivata su un sistema storage che deve supportare i client che montano le esportazioni NFS utilizzando una porta non riservata anche quando l'utente è connesso come root. Tali client includono i client Hummingbird e i client NFS/IPv6 di Solaris.

Se il `-mount-rootonly` ONTAP non consente ai client NFS che utilizzano porte non riservate, ovvero porte con numeri superiori a 1,023, di montare le esportazioni NFS.

Eseguire un controllo degli accessi più rigoroso per i netgroup verificando i domini

Per impostazione predefinita, ONTAP esegue un'ulteriore verifica quando valuta l'accesso client per un netgroup. Il controllo aggiuntivo garantisce che il dominio del client corrisponda alla configurazione di dominio della macchina virtuale di storage (SVM). In caso contrario, ONTAP nega l'accesso al client.

A proposito di questa attività

Quando ONTAP valuta le regole dei criteri di esportazione per l'accesso client e una regola dei criteri di esportazione contiene un netgroup, ONTAP deve determinare se l'indirizzo IP di un client appartiene al netgroup. A tale scopo, ONTAP converte l'indirizzo IP del client in un nome host utilizzando DNS e ottiene un nome di dominio completo (FQDN).

Se il file netgroup elenca solo un nome breve per l'host e il nome breve per l'host esiste in più domini, è possibile che un client di un dominio diverso ottenga l'accesso senza questo controllo.

Per evitare che ciò accada, ONTAP confronta il dominio restituito dal DNS per l'host con l'elenco dei nomi di dominio DNS configurati per la SVM. Se corrisponde, l'accesso è consentito. Se non corrisponde, l'accesso viene negato.

Questa verifica è attivata per impostazione predefinita. È possibile gestirlo modificando il `-netgroup-dns-domain-search` che è disponibile al livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera che la verifica del dominio per i netgroup sia...	Inserisci...
Attivato	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</pre>
Disattivato	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</pre>

3. Impostare il livello di privilegio su admin:

```
set -privilege admin
```

Modificare le porte utilizzate per i servizi NFSv3

Il server NFS sul sistema di storage utilizza servizi come mount daemon e Network Lock Manager per comunicare con i client NFS su porte di rete predefinite specifiche. Nella maggior parte degli ambienti NFS, le porte predefinite funzionano correttamente e non richiedono modifiche, ma se si desidera utilizzare diverse porte di rete NFS nell'ambiente NFSv3, è possibile farlo.

Di cosa hai bisogno

La modifica delle porte NFS sul sistema di storage richiede che tutti i client NFS si riconnettano al sistema, pertanto è necessario comunicare queste informazioni agli utenti prima di apportare la modifica.

A proposito di questa attività

È possibile impostare le porte utilizzate dai servizi NFS mount daemon, Network Lock Manager, Network

Status Monitor e NFS quota daemon per ciascuna macchina virtuale di storage (SVM). La modifica del numero di porta influisce sull'accesso dei client NFS ai dati sia su TCP che su UDP.

Le porte per NFSv4 e NFSv4.1 non possono essere modificate.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Disattivare l'accesso a NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Impostare la porta NFS per il servizio NFS specifico:

```
vserver nfs modify -vserver vserver_name nfs_port_parameter port_number
```

Parametro della porta NFS	Descrizione	Porta predefinita
-mountd-port	Daemon di montaggio NFS	635
-nlm-port	Network Lock Manager	4045
-nsm-port	Network Status Monitor (Monitor di stato della rete)	4046
-rquotad-port	Daemon quota NFS	4049

Oltre alla porta predefinita, l'intervallo consentito di numeri di porta è compreso tra 1024 e 65535. Ogni servizio NFS deve utilizzare una porta univoca.

4. Abilitare l'accesso a NFS:

```
vserver nfs modify -vserver vserver_name -access true
```

5. Utilizzare `network connections listening show` per verificare che il numero di porta cambi.

6. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

I seguenti comandi impostano la porta NFS Mount Daemon su 1113 sulla SVM denominata vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true


vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopcp
vs1               data1:4046                   TCP/sm
vs1               data1:4046                   UDP/sm
vs1               data1:4045                   TCP/nlm-v4
vs1               data1:4045                   UDP/nlm-v4
vs1               data1:1113                   TCP/mount
vs1               data1:1113                   UDP/mount
...
vs1::*> set -privilege admin

```

Comandi per la gestione dei server NFS

Esistono comandi ONTAP specifici per la gestione dei server NFS.

Se si desidera...	Utilizzare questo comando...
Creare un server NFS	<code>vserver nfs create</code>
Visualizzare i server NFS	<code>vserver nfs show</code>
Modificare un server NFS	<code>vserver nfs modify</code>
Eliminare un server NFS	<code>vserver nfs delete</code>

<p>Nascondere <code>.snapshot</code> Elenco di directory sotto i punti di montaggio NFSv3</p> <div>  <p>Accesso esplicito a <code>.snapshot</code> la directory sarà comunque consentita anche se l'opzione è attivata.</p> </div>	<p><code>vserver nfs</code> comandi con <code>-v3-hide-snapshot</code> opzione attivata</p>
---	---

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

Risolvere i problemi di name service

Quando i client riscontrano errori di accesso dovuti a problemi di name service, è possibile utilizzare `vserver services name-service getxxbyyy` famiglia di comandi per eseguire manualmente varie ricerche dei name service ed esaminare i dettagli e i risultati della ricerca per agevolare la risoluzione dei problemi.

A proposito di questa attività

- Per ciascun comando, è possibile specificare quanto segue:
 - Nome del nodo o della SVM (Storage Virtual Machine) su cui eseguire la ricerca.

In questo modo è possibile verificare le ricerche name service per un nodo o una SVM specifico per limitare la ricerca di un potenziale problema di configurazione del name service.

- Se visualizzare l'origine utilizzata per la ricerca.

In questo modo è possibile verificare se è stata utilizzata la sorgente corretta.

- ONTAP seleziona il servizio per l'esecuzione della ricerca in base all'ordine di switch name service configurato.
- Questi comandi sono disponibili a livello di privilegio avanzato.

Fasi

1. Eseguire una delle seguenti operazioni:

Per recuperare...	Utilizzare il comando...
Indirizzo IP di un nome host	<code>vserver services name-service getxxbyyy getaddrinfo vserver services name-service getxxbyyy gethostbyname</code> (Solo indirizzi IPv4)
Membri di un gruppo per ID gruppo	<code>vserver services name-service getxxbyyy getgrbygid</code>

Membri di un gruppo in base al nome del gruppo	<code>vserver services name-service getxxbyyy getgrbyname</code>
Elenco dei gruppi a cui appartiene un utente	<code>vserver services name-service getxxbyyy getgrlist</code>
Nome host di un indirizzo IP	<code>vserver services name-service getxxbyyy getnameinfo</code> <code>vserver services name-service getxxbyyy gethostbyaddr</code> (Solo indirizzi IPv4)
Informazioni utente per nome utente	<code>vserver services name-service getxxbyyy getpwbyname</code> È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando <code>-use-rbac</code> parametro <code>as true</code> .
Informazioni utente per ID utente	<code>vserver services name-service getxxbyyy getpwbyuid</code> È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando <code>-use-rbac</code> parametro <code>as true</code> .
Appartenenza a netgroup di un client	<code>vserver services name-service getxxbyyy netgrp</code>
Appartenenza a netgroup di un client mediante la ricerca netgroup-by-host	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

L'esempio seguente mostra un test di ricerca DNS per SVM vs1 tentando di ottenere l'indirizzo IP per l'host `acast1.eng.example.com`:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

L'esempio seguente mostra un test di ricerca NIS per SVM vs1 tentando di recuperare le informazioni utente per un utente con UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

L'esempio seguente mostra un test di ricerca LDAP per SVM vs1 tentando di recuperare le informazioni utente per un utente con il nome ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

L'esempio seguente mostra un test di ricerca di netgroup per SVM vs1 cercando di scoprire se il client dnshost0 è un membro del netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analizzare i risultati del test eseguito e intraprendere le azioni necessarie.

Se...	Controllare...
La ricerca del nome host o dell'indirizzo IP non è riuscita o ha dato risultati errati	Configurazione DNS
La ricerca ha richiesto un'origine errata	Configurazione dello switch name service

Se...	Controllare...
La ricerca di utenti o gruppi non è riuscita o ha prodotto risultati errati	<ul style="list-style-type: none"> • Configurazione dello switch name service • Configurazione di origine (file locali, dominio NIS, client LDAP) • Configurazione di rete (ad esempio, LIF e route)
Ricerca nome host non riuscita o scaduta e il server DNS non risolve i nomi brevi DNS (ad esempio, host1)	Configurazione DNS per query TLD (Top-Level Domain). È possibile disattivare le query TLD utilizzando <code>-is-tld-query-enabled false</code> al <code>vserver services name-service dns modify</code> comando.

Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Verificare le connessioni name service

A partire da ONTAP 9.2, è possibile controllare i server dei nomi DNS e LDAP per verificare che siano connessi a ONTAP. Questi comandi sono disponibili a livello di privilegi di amministratore.

A proposito di questa attività

È possibile verificare la presenza di una configurazione DNS o LDAP name service valida in base alle necessità utilizzando il controllo della configurazione del name service. Questo controllo di convalida può essere avviato dalla riga di comando o in System Manager.

Per le configurazioni DNS, tutti i server sono testati e devono funzionare perché la configurazione sia considerata valida. Per le configurazioni LDAP, se un server è attivo, la configurazione è valida. I comandi name service applicano il controllo della configurazione, a meno che non lo sia `skip-config-validation` il campo è `true` (il valore predefinito è `false`).

Fase

1. Utilizzare il comando appropriato per controllare la configurazione di un name service. L'interfaccia utente visualizza lo stato dei server configurati.

Per verificare...	Utilizzare questo comando...
Stato della configurazione DNS	<code>vserver services name-service dns check</code>
Stato della configurazione LDAP	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

Vserver	Name Server	Status	Status Details
vs0	10.11.12.13	up	Response time (msec): 55
vs0	10.11.12.14	up	Response time (msec): 70
vs0	10.11.12.15	down	Connection refused.

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

La convalida della configurazione ha esito positivo se almeno uno dei server configurati (name-server/ldap-server) è raggiungibile e fornisce il servizio. Se alcuni server non sono raggiungibili, viene visualizzato un avviso.

Comandi per la gestione delle voci di switch name service

È possibile gestire le voci di name service switch creandole, visualizzandole, modificandole ed eliminandole.

Se si desidera...	Utilizzare questo comando...
Creare una voce name service switch	<code>vserver services name-service ns-switch create</code>
Nome visualizzato voci switch servizio	<code>vserver services name-service ns-switch show</code>
Modificare una voce di name service switch	<code>vserver services name-service ns-switch modify</code>
Consente di eliminare una voce di switch name service	<code>vserver services name-service ns-switch delete</code>

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

Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Comandi per la gestione della cache del name service

È possibile gestire la cache del name service modificando il valore TTL (Time To Live). Il valore TTL determina per quanto tempo le informazioni del servizio dei nomi sono persistenti nella cache.

Se si desidera modificare il valore TTL per...	Utilizzare questo comando...
Utenti UNIX	<code>vserver services name-service cache unix-user settings</code>
Gruppi UNIX	<code>vserver services name-service cache unix-group settings</code>
Netgroup UNIX	<code>vserver services name-service cache netgroups settings</code>
Host	<code>vserver services name-service cache hosts settings</code>
Appartenenza al gruppo	<code>vserver services name-service cache group-membership settings</code>

Informazioni correlate

["Comandi di ONTAP 9"](#)

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	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>
Scambiare la posizione di due mappature dei nomi NOTA: Non è consentito eseguire uno swap quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	<code>vserver name-mapping swap</code>
Modificare una mappatura dei nomi	<code>vserver name-mapping modify</code>

Eliminare una mappatura dei nomi	<code>vserver name-mapping delete</code>
Convalidare la corretta mappatura dei nomi	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

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

Comandi per la gestione degli utenti UNIX locali

Esistono comandi ONTAP specifici per la gestione degli utenti UNIX locali.

Se si desidera...	Utilizzare questo comando...
Creare un utente UNIX locale	<code>vserver services name-service unix-user create</code>
Caricare utenti UNIX locali da un URI	<code>vserver services name-service unix-user load-from-uri</code>
Visualizzare gli utenti UNIX locali	<code>vserver services name-service unix-user show</code>
Modificare un utente UNIX locale	<code>vserver services name-service unix-user modify</code>
Eliminare un utente UNIX locale	<code>vserver services name-service unix-user delete</code>

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

Comandi per la gestione di gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei gruppi UNIX locali.

Se si desidera...	Utilizzare questo comando...
Creare un gruppo UNIX locale	<code>vserver services name-service unix-group create</code>
Aggiungere un utente a un gruppo UNIX locale	<code>vserver services name-service unix-group adduser</code>
Caricare i gruppi UNIX locali da un URI	<code>vserver services name-service unix-group load-from-uri</code>
Visualizzare i gruppi UNIX locali	<code>vserver services name-service unix-group show</code>
Modificare un gruppo UNIX locale	<code>vserver services name-service unix-group modify</code>

Eliminare un utente da un gruppo UNIX locale	<code>vserver services name-service unix-group deluser</code>
Eliminare un gruppo UNIX locale	<code>vserver services name-service unix-group delete</code>

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

Limiti per utenti UNIX locali, gruppi e membri del gruppo

ONTAP ha introdotto limiti per il numero massimo di utenti e gruppi UNIX nel cluster e comandi per gestire questi limiti. Questi limiti possono aiutare a evitare problemi di performance impedendo agli amministratori di creare troppi utenti e gruppi UNIX locali nel cluster.

Esiste un limite per il numero combinato di gruppi di utenti UNIX locali e di membri del gruppo. Esiste un limite separato per gli utenti UNIX locali. I limiti sono a livello di cluster. Ciascuno di questi nuovi limiti viene impostato su un valore predefinito che è possibile modificare fino a un limite massimo preassegnato.

Database	Limite predefinito	Limite massimo
Utenti UNIX locali	32,768	65,536
Gruppi UNIX locali e membri del gruppo	32,768	65,536

Gestire i limiti per utenti e gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei limiti per utenti e gruppi UNIX locali. Gli amministratori dei cluster possono utilizzare questi comandi per risolvere i problemi di performance nel cluster che si ritiene siano correlati a un numero eccessivo di utenti e gruppi UNIX locali.

A proposito di questa attività

Questi comandi sono disponibili per l'amministratore del cluster a livello di privilegi avanzati.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Utilizzare il comando...
Visualizza informazioni sui limiti utente UNIX locali	<code>vserver services unix-user max-limit show</code>
Visualizza informazioni sui limiti dei gruppi UNIX locali	<code>vserver services unix-group max-limit show</code>

Se si desidera...	Utilizzare il comando...
Modificare i limiti utente UNIX locali	<code>vserver services unix-user max-limit modify</code>
Modificare i limiti dei gruppi UNIX locali	<code>vserver services unix-group max-limit modify</code>

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

Comandi per la gestione dei netgroup locali

È possibile gestire i netgroup locali caricandoli da un URI, verificandone lo stato tra i nodi, visualizzandoli ed eliminandoli.

Se si desidera...	Utilizzare il comando...
Caricare i netgroup da un URI	<code>vserver services name-service netgroup load</code>
Verificare lo stato dei netgroup nei nodi	<code>vserver services name-service netgroup status</code> Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i netgroup locali	<code>vserver services name-service netgroup file show</code>
Eliminare un netgroup locale	<code>vserver services name-service netgroup file delete</code>

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

Comandi per la gestione delle configurazioni di dominio NIS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di dominio NIS.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione di dominio NIS	<code>vserver services name-service nis-domain create</code>
Visualizzare le configurazioni di dominio NIS	<code>vserver services name-service nis-domain show</code>
Visualizza lo stato di binding di una configurazione di dominio NIS	<code>vserver services name-service nis-domain show-bound</code>
Visualizzare le statistiche NIS	<code>vserver services name-service nis-domain show-statistics</code> Disponibile a un livello di privilegio avanzato e superiore.

Cancellare le statistiche NIS	<code>vserver services name-service nis-domain clear-statistics</code> Disponibile a un livello di privilegio avanzato e superiore.
Modificare una configurazione di dominio NIS	<code>vserver services name-service nis-domain modify</code>
Eliminare una configurazione di dominio NIS	<code>vserver services name-service nis-domain delete</code>
Abilitare il caching per le ricerche netgroup-by-host	<code>vserver services name-service nis-domain netgroup-database config modify</code> Disponibile a un livello di privilegio avanzato e superiore.

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

Comandi per la gestione delle configurazioni del client LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni del client LDAP.



Gli amministratori SVM non possono modificare o eliminare le configurazioni client LDAP create dagli amministratori del cluster.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione del client LDAP	<code>vserver services name-service ldap client create</code>
Visualizzare le configurazioni del client LDAP	<code>vserver services name-service ldap client show</code>
Modificare una configurazione del client LDAP	<code>vserver services name-service ldap client modify</code>
Modificare la password BIND del client LDAP	<code>vserver services name-service ldap client modify-bind-password</code>
Eliminare una configurazione del client LDAP	<code>vserver services name-service ldap client delete</code>

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

Comandi per la gestione delle configurazioni LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni LDAP.

Se si desidera...	Utilizzare questo comando...
-------------------	------------------------------

Creare una configurazione LDAP	<code>vserver services name-service ldap create</code>
Visualizzare le configurazioni LDAP	<code>vserver services name-service ldap show</code>
Modificare una configurazione LDAP	<code>vserver services name-service ldap modify</code>
Eliminare una configurazione LDAP	<code>vserver services name-service ldap delete</code>

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

Comandi per la gestione dei modelli di schema del client LDAP

Esistono comandi ONTAP specifici per la gestione dei modelli di schema del client LDAP.



Gli amministratori di SVM non possono modificare o eliminare gli schemi client LDAP creati dagli amministratori del cluster.

Se si desidera...	Utilizzare questo comando...
Copiare un modello di schema LDAP esistente	<code>vserver services name-service ldap client schema copy</code> Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i modelli di schema LDAP	<code>vserver services name-service ldap client schema show</code>
Modificare un modello di schema LDAP	<code>vserver services name-service ldap client schema modify</code> Disponibile a un livello di privilegio avanzato e superiore.
Eliminare un modello di schema LDAP	<code>vserver services name-service ldap client schema delete</code> Disponibile a un livello di privilegio avanzato e superiore.

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

Comandi per la gestione delle configurazioni dell'interfaccia Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni dell'interfaccia Kerberos NFS.

Se si desidera...	Utilizzare questo comando...
Abilitare NFS Kerberos su una LIF	<code>vserver nfs kerberos interface enable</code>
Visualizzare le configurazioni dell'interfaccia Kerberos NFS	<code>vserver nfs kerberos interface show</code>

Modificare una configurazione dell'interfaccia Kerberos NFS	<code>vserver nfs kerberos interface modify</code>
Disattiva NFS Kerberos su LIF	<code>vserver nfs kerberos interface disable</code>

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

Comandi per la gestione delle configurazioni del realm Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di autenticazione Kerberos NFS.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione di autenticazione Kerberos NFS	<code>vserver nfs kerberos realm create</code>
Visualizzare le configurazioni del realm Kerberos NFS	<code>vserver nfs kerberos realm show</code>
Modificare la configurazione di un realm Kerberos NFS	<code>vserver nfs kerberos realm modify</code>
Eliminare una configurazione di autenticazione Kerberos NFS	<code>vserver nfs kerberos realm delete</code>

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

Comandi per la gestione delle policy di esportazione

Esistono comandi ONTAP specifici per la gestione delle policy di esportazione.

Se si desidera...	Utilizzare questo comando...
Visualizza informazioni sui criteri di esportazione	<code>vserver export-policy show</code>
Rinominare un criterio di esportazione	<code>vserver export-policy rename</code>
Copiare una policy di esportazione	<code>vserver export-policy copy</code>
Eliminare una policy di esportazione	<code>vserver export-policy delete</code>

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

Comandi per la gestione delle regole di esportazione

Esistono comandi ONTAP specifici per la gestione delle regole di esportazione.

Se si desidera...	Utilizzare questo comando...
Creare una regola di esportazione	<code>vserver export-policy rule create</code>
Visualizza le informazioni sulle regole di esportazione	<code>vserver export-policy rule show</code>
Modificare una regola di esportazione	<code>vserver export-policy rule modify</code>
Eliminare una regola di esportazione	<code>vserver export-policy rule delete</code>



Se sono state configurate più regole di esportazione identiche corrispondenti a client diversi, assicurarsi di mantenerle sincronizzate durante la gestione delle regole di esportazione.

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

Configurare la cache delle credenziali NFS

Motivi per modificare il time-to-live della cache delle credenziali NFS

ONTAP utilizza una cache delle credenziali per memorizzare le informazioni necessarie per l'autenticazione dell'utente per l'accesso all'esportazione NFS, in modo da fornire un accesso più rapido e migliorare le performance. È possibile configurare per quanto tempo le informazioni vengono memorizzate nella cache delle credenziali per personalizzarle in base all'ambiente in uso.

La modifica del TTL (Time-to-live) della cache delle credenziali NFS può aiutare a risolvere i problemi in diversi scenari. È necessario comprendere quali sono questi scenari e le conseguenze di tali modifiche.

Motivi

Modificare il TTL predefinito nei seguenti casi:

Problema	Azione correttiva
I name server nel tuo ambiente stanno riscontrando un peggioramento delle performance dovuto a un elevato carico di richieste da parte di ONTAP.	Aumentare il TTL per le credenziali positive e negative memorizzate nella cache per ridurre il numero di richieste da ONTAP ai server dei nomi.
L'amministratore del name server ha apportato delle modifiche per consentire l'accesso agli utenti NFS precedentemente rifiutati.	Ridurre il TTL per le credenziali negative memorizzate nella cache per ridurre il tempo di attesa che gli utenti NFS debbano attendere che ONTAP richieda nuove credenziali ai server dei nomi esterni in modo che possano accedervi.

Problema	Azione correttiva
L'amministratore del name server ha apportato delle modifiche per negare l'accesso agli utenti NFS precedentemente autorizzati.	Riduci il TTL per le credenziali positive memorizzate nella cache per ridurre il tempo prima che ONTAP richieda nuove credenziali ai server dei nomi esterni, in modo che gli utenti NFS non possano accedere.

Conseguenze

È possibile modificare la durata del tempo singolarmente per il caching delle credenziali positive e negative. Tuttavia, è necessario essere consapevoli dei vantaggi e degli svantaggi di tale operazione.

Se...	Il vantaggio è...	Lo svantaggio è...
Aumentare il tempo di cache delle credenziali positive	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Ci vuole più tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.
Ridurre il tempo di cache delle credenziali positive	È necessario meno tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.
Aumentare il tempo di cache delle credenziali negative	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Occorre più tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.
Ridurre il tempo di cache delle credenziali negative	Occorrono meno tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.

Configurare il time-to-live per le credenziali utente NFS memorizzate nella cache

È possibile configurare il periodo di tempo in cui ONTAP memorizza le credenziali degli utenti NFS nella cache interna (time-to-live o TTL) modificando il server NFS della macchina virtuale di storage (SVM). In questo modo è possibile ridurre alcuni problemi legati all'elevato carico sui server dei nomi o alle modifiche delle credenziali che influiscono sull'accesso degli utenti NFS.

A proposito di questa attività

Questi parametri sono disponibili a livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera modificare il TTL per la cache...	Utilizzare il comando...
Credenziali positive	<pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre> <p>Il TTL viene misurato in millisecondi. A partire da ONTAP 9.10.1 e versioni successive, il valore predefinito è 1 ora (3.600.000 millisecondi). In ONTAP 9.9.1 e versioni precedenti, il valore predefinito è 24 ore (86.400.000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).</p>
Credenziali negative	<pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre> <p>Il TTL viene misurato in millisecondi. L'impostazione predefinita è 2 ore (7,200,000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).</p>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Gestire le cache delle policy di esportazione

Svuotare le cache delle policy di esportazione

ONTAP utilizza diverse cache delle policy di esportazione per memorizzare le informazioni relative alle policy di esportazione per un accesso più rapido. L'operazione di cancellazione della policy di esportazione viene eseguita manualmente nella cache (`vserver export-policy cache flush`) Rimuove le informazioni potenzialmente obsolete e costringe ONTAP a recuperare le informazioni correnti dalle risorse esterne appropriate. Questo può aiutare a risolvere una serie di problemi relativi all'accesso client alle esportazioni NFS.

A proposito di questa attività

Le informazioni della cache delle policy di esportazione potrebbero essere obsolete a causa dei seguenti motivi:

- Una recente modifica alle regole dei criteri di esportazione
- Una recente modifica ai record dei nomi host nei server dei nomi
- Una recente modifica alle voci di netgroup nei server dei nomi
- Ripristino da un'interruzione di rete che ha impedito il caricamento completo dei netgroup

Fasi

1. Se la cache del servizio nomi non è attivata, eseguire una delle seguenti operazioni in modalità privilegio avanzato:

Se si desidera eseguire il lavaggio...	Immettere il comando...
Tutte le cache delle policy di esportazione (ad eccezione di showmount)	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name</code>
La policy di esportazione regola l'accesso alla cache	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache access</code> È possibile includere il opzionale <code>-node</code> parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache host</code>
La cache del netgroup	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache netgroup</code> L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.
La cache di showmount	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache showmount</code>

2. Se la cache del name service è attivata, eseguire una delle seguenti operazioni:

Se si desidera eseguire il lavaggio...	Immettere il comando...
La policy di esportazione regola l'accesso alla cache	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache access</code> È possibile includere il opzionale <code>-node</code> parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	<code>vserver services name-service cache</code> <code>hosts forward-lookup delete-all</code>

Se si desidera eseguire il lavaggio...	Immettere il comando...
La cache del netgroup	<pre>vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all</pre> <p>L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.</p>
La cache di showmount	<pre>vserver export-policy cache flush -vserver vserver_name -cache showmount</pre>

Visualizza la coda e la cache del netgroup dei criteri di esportazione

ONTAP utilizza la coda netgroup per importare e risolvere i netgroup e la cache netgroup per memorizzare le informazioni risultanti. Durante la risoluzione dei problemi relativi ai netgroup di policy di esportazione, è possibile utilizzare `vserver export-policy netgroup queue show` e `vserver export-policy netgroup cache show` comandi per visualizzare lo stato della coda netgroup e il contenuto della cache netgroup.

Fase

1. Eseguire una delle seguenti operazioni:

Per visualizzare il netgroup dei criteri di esportazione...	Immettere il comando...
Coda	<code>vserver export-policy netgroup queue show</code>
Cache	<code>vserver export-policy netgroup cache show -vserver vserver_name</code>

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

Verificare se un indirizzo IP del client è membro di un netgroup

Durante la risoluzione dei problemi di accesso al client NFS relativi ai netgroup, è possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.

A proposito di questa attività

La verifica dell'appartenenza a netgroup consente di determinare se ONTAP è consapevole che un client è o meno membro di un netgroup. Consente inoltre di sapere se la cache del netgroup ONTAP si trova in uno stato transitorio durante l'aggiornamento delle informazioni del netgroup. Queste informazioni possono aiutarti a capire perché a un client potrebbe essere concesso o negato l'accesso in modo imprevisto.

Fase

1. Verificare l'appartenenza al netgroup di un indirizzo IP client: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

Il comando può restituire i seguenti risultati:

- Il client è membro del netgroup.

Ciò è stato confermato mediante una ricerca inversa o una ricerca `netgroup-by-host`.

- Il client è membro del netgroup.

È stato trovato nella cache del netgroup di ONTAP.

- Il client non è membro del netgroup.

- L'appartenenza del client non può ancora essere determinata perché ONTAP sta aggiornando la cache del netgroup.

Fino a quando ciò non viene fatto, l'appartenenza non può essere esplicitamente esclusa o esclusa. Utilizzare `vserver export-policy netgroup queue show` comando per monitorare il caricamento del netgroup e riprovare il controllo al termine.

Esempio

Nell'esempio seguente viene verificato se un client con l'indirizzo IP 172.17.16.72 è membro del netgroup Mercury su SVM vs1:

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1  
-netgroup mercury -client-ip 172.17.16.72
```

Ottimizza le performance della cache di accesso

È possibile configurare diversi parametri per ottimizzare la cache di accesso e trovare il giusto equilibrio tra le prestazioni e la corrente delle informazioni memorizzate nella cache di accesso.

A proposito di questa attività

Quando si configurano i periodi di aggiornamento della cache di accesso, tenere presente quanto segue:

- Valori più elevati significano che le voci rimangono più lunghe nella cache di accesso.

Il vantaggio è rappresentato dalle performance migliori, in quanto ONTAP spende meno risorse per il refresh delle voci della cache di accesso. Lo svantaggio è che se le regole dei criteri di esportazione cambiano e le voci della cache di accesso diventano obsolete, l'aggiornamento richiede più tempo. Di conseguenza, i client che dovrebbero ottenere l'accesso potrebbero essere rifiutati e i client che dovrebbero ottenere l'accesso potrebbero ottenere l'accesso.

- Valori più bassi significano che ONTAP aggiorna più spesso le voci della cache di accesso.

Il vantaggio è che le voci sono più aggiornate e i client hanno maggiori probabilità di ottenere o negare l'accesso correttamente. Lo svantaggio è una diminuzione delle performance perché ONTAP spende più

risorse per aggiornare le voci della cache di accesso.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Per modificare...	Inserisci...
Periodo di refresh per voci positive	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</pre>
Periodo di refresh per le voci negative	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</pre>
Periodo di timeout per le voci precedenti	<pre>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</pre>

3. Verificare le nuove impostazioni dei parametri:

```
vserver export-policy access-cache config show-all-vservers
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

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.

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 le impostazioni di protezione dell'elenco di controllo di accesso Windows (ACL) che impediscono agli utenti o alle

applicazioni di rinominare le directory critiche.

Scopri di più ["Come impedire che le directory vengano rinominate mentre i client le accedono"](#).

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 rottura

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	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
L'ID blocco	<code>vserver locks break -lockid UUID</code>

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Come funzionano i filtri FPolicy first-Read e first-write con NFS

I client NFS sperimentano tempi di risposta elevati durante il traffico elevato delle richieste di lettura/scrittura quando FPolicy viene abilitato utilizzando un server FPolicy esterno con operazioni di lettura/scrittura come eventi monitorati. Per i client NFS, l'utilizzo di filtri di prima lettura e prima scrittura in FPolicy riduce il numero di notifiche FPolicy e migliora le performance.

In NFS, il client esegue l'i/o su un file mediante il recupero dell'handle. Questo handle potrebbe rimanere valido per i riavvii del server e del client. Pertanto, il client è libero di memorizzare nella cache l'handle e di inviarne le richieste senza dover recuperare nuovamente gli handle. In una sessione regolare, molte richieste di lettura/scrittura vengono inviate al file server. Se vengono generate notifiche per tutte queste richieste, potrebbero verificarsi i seguenti problemi:

- Un carico maggiore grazie all'elaborazione aggiuntiva delle notifiche e a tempi di risposta più elevati.
- Un gran numero di notifiche inviate al server FPolicy anche se il server non è interessato da tutte le notifiche.

Dopo aver ricevuto la prima richiesta di lettura/scrittura da un client per un determinato file, viene creata una voce della cache e il conteggio di lettura/scrittura viene incrementato. Questa richiesta viene contrassegnata come prima operazione di lettura/scrittura e viene generato un evento FPolicy. Prima di pianificare e creare i filtri FPolicy per un client NFS, è necessario comprendere le nozioni di base sul funzionamento dei filtri FPolicy.

- First-Read (prima lettura): Filtra le richieste di lettura del client per la prima lettura.

Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima lettura per la quale viene elaborato FPolicy.

- First-write: Filtra le richieste di scrittura del client per la first-write.

Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima scrittura per la quale FPolicy ha elaborato.

Le seguenti opzioni vengono aggiunte nel database dei server NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modificare l'ID di implementazione del server NFSv4.1

Il protocollo NFSv4.1 include un ID di implementazione del server che documenta il dominio, il nome e la data del server. È possibile modificare i valori predefiniti dell'ID di implementazione del server. La modifica dei valori predefiniti può essere utile, ad

esempio, per la raccolta di statistiche di utilizzo o la risoluzione dei problemi di interoperabilità. Per ulteriori informazioni, vedere RFC 5661.

A proposito di questa attività

I valori predefiniti per le tre opzioni sono i seguenti:

Opzione	Nome dell'opzione	Valore predefinito
Dominio ID implementazione NFSv4.1	<code>-v4.1-implementation-domain</code>	netapp.com
Nome ID implementazione NFSv4.1	<code>-v4.1-implementation-name</code>	Nome della versione del cluster
Data ID implementazione NFSv4.1	<code>-v4.1-implementation-date</code>	Data di versione del cluster

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera modificare l'ID di implementazione NFSv4.1...	Immettere il comando...
Dominio	<code>vserver nfs modify -v4.1 -implementation-domain domain</code>
Nome	<code>vserver nfs modify -v4.1 -implementation-name name</code>
Data	<code>vserver nfs modify -v4.1 -implementation-date date</code>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Gestire gli ACL NFSv4

Vantaggi dell'abilitazione degli ACL NFSv4

L'abilitazione degli ACL NFSv4 offre numerosi vantaggi.

I vantaggi derivanti dall'abilitazione degli ACL NFSv4 includono:

- Controllo più dettagliato dell'accesso degli utenti per file e directory

- Maggiore sicurezza NFS
- Maggiore interoperabilità con CIFS
- Rimozione del limite NFS di 16 gruppi per utente

Come funzionano gli ACL NFSv4

Un client che utilizza ACL NFSv4 può impostare e visualizzare ACL su file e directory del sistema. Quando viene creato un nuovo file o sottodirectory in una directory che dispone di un ACL, il nuovo file o sottodirectory eredita tutte le voci ACL (ACL) nell'ACL contrassegnate con gli indicatori di ereditarietà appropriati.

Quando viene creato un file o una directory come risultato di una richiesta NFSv4, l'ACL del file o della directory risultante dipende dal fatto che la richiesta di creazione del file includa un ACL o solo permessi di accesso ai file UNIX standard e se la directory principale dispone di un ACL:

- Se la richiesta include un ACL, viene utilizzato tale ACL.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory principale dispone di un ACL, le ACE nell'ACL della directory principale vengono ereditate dal nuovo file o directory, purché le ACE siano state contrassegnate con gli indicatori di ereditarietà appropriati.



Un ACL padre viene ereditato anche se `-v4.0-acl` è impostato su `off`.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale non dispone di un ACL, la modalità file client viene utilizzata per impostare le autorizzazioni di accesso ai file UNIX standard.
- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale dispone di un ACL non ereditabile, il nuovo oggetto viene creato solo con i bit di modalità.



Se il `-chown-mode` il parametro è stato impostato su `restricted` con i comandi in `vserver nfs` oppure `vserver export-policy rule Famiglie`, la proprietà del file può essere modificata solo dal superutente, anche se le autorizzazioni su disco impostate con gli ACL NFSv4 consentono a un utente non root di modificare la proprietà del file. Per ulteriori informazioni, consulta le relative pagine man.

Attiva o disattiva la modifica degli ACL NFSv4

Quando ONTAP riceve un `chmod` Per un file o una directory con un ACL, per impostazione predefinita l'ACL viene conservato e modificato per riflettere la modifica del bit di modalità. È possibile disattivare `-v4-acl-preserve` Parametro per modificare il comportamento se si desidera che l'ACL venga eliminato.

A proposito di questa attività

Quando si utilizza uno stile di sicurezza unificato, questo parametro specifica anche se le autorizzazioni del file NTFS vengono mantenute o interrotte quando un client invia un comando `chmod`, `chgroup` o `chown` per un file o una directory.

L'impostazione predefinita per questo parametro è `Enabled` (attivato).

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Attiva conservazione e modifica degli ACL NFSv4 esistenti (impostazione predefinita)	<pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</pre>
Disattiva la conservazione e disattiva gli ACL NFSv4 quando si modificano i bit di modalità	<pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Come ONTAP utilizza gli ACL NFSv4 per determinare se è in grado di eliminare un file

Per determinare se è possibile eliminare un file, ONTAP utilizza una combinazione del bit DELETE del file e del bit DELETE_CHILD della directory contenente. Per ulteriori informazioni, vedere NFS 4.1 RFC 5661.

Attivare o disattivare gli ACL NFSv4

Per attivare o disattivare gli ACL NFSv4, è possibile modificare `-v4.0-acl` e `-v4.1-acl` opzioni. Queste opzioni sono disattivate per impostazione predefinita.

A proposito di questa attività

Il `-v4.0-acl` oppure `-v4.1-acl` L'opzione controlla l'impostazione e la visualizzazione degli ACL NFSv4; non controlla l'applicazione di questi ACL per il controllo degli accessi.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare gli ACL NFSv4.0	Immettere il seguente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</pre>
Disattivare gli ACL NFSv4.0	Immettere il seguente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre>

Abilitare gli ACL NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>
Disattivare gli ACL NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</code>

Modificare il limite massimo ACE per gli ACL NFSv4

È possibile modificare il numero massimo di ACE consentiti per ogni ACL NFSv4 modificando il parametro `-v4-acl-max-aces`. Per impostazione predefinita, il limite è impostato su 400 ACE per ogni ACL. L'aumento di questo limite può contribuire a garantire una migrazione corretta dei dati con ACL contenenti oltre 400 ACE nei sistemi storage che eseguono ONTAP.

A proposito di questa attività

L'aumento di questo limite potrebbe influire sulle performance dei client che accedono ai file con ACL NFSv4.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modificare il limite massimo ACE per gli ACL NFSv4:

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

L'intervallo valido di

`max_ace_limit` è 192 a 1024.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Gestire le deleghe dei file NFSv4

Attivare o disattivare le deleghe dei file di lettura NFSv4

Per attivare o disattivare le deleghe dei file di lettura NFSv4, è possibile modificare `-v4.0-read-delegation` oppure opzione. Attivando le deleghe dei file di lettura, è possibile eliminare gran parte dell'overhead dei messaggi associato all'apertura e alla chiusura dei file.

A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di lettura sono disattivate.

Lo svantaggio dell'abilitazione delle deleghe dei file in lettura consiste nel fatto che il server e i suoi client devono ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare le deleghe dei file di lettura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled</code>
Abilitare le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando: + <code>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</code>
Disattiva le deleghe dei file di lettura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</code>
Disattiva le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</code>

Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

Attivare o disattivare le deleghe dei file di scrittura NFSv4

Per attivare o disattivare le deleghe dei file di scrittura, è possibile modificare `-v4.0 -write-delegation` oppure opzione. Attivando le deleghe di scrittura dei file, è possibile eliminare gran parte dell'overhead dei messaggi associato al blocco di file e record, oltre all'apertura e alla chiusura dei file.

A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di scrittura sono disattivate.

Lo svantaggio di abilitare le deleghe dei file di scrittura è che il server e i relativi client devono eseguire attività aggiuntive per ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled</code>
Abilitare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled</code>
Disattiva le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</code>
Disattivare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</code>

Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

Configurare il blocco di file e record NFSv4

Informazioni sul blocco di file e record NFSv4

Per i client NFSv4, ONTAP supporta il meccanismo di blocco dei file NFSv4, mantenendo lo stato di tutti i blocchi dei file in un modello basato sul lease.

["Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"](#)

Specificare il periodo di lease di blocco NFSv4

Per specificare il periodo di leasing di blocco NFSv4 (ovvero, il periodo di tempo in cui ONTAP concede irrevocabilmente un blocco a un client), è possibile modificare `-v4 -lease-seconds` opzione. I periodi di leasing più brevi accelerano il ripristino dei server, mentre i periodi di leasing più lunghi sono vantaggiosi per i server che gestiscono un numero molto elevato di client.

A proposito di questa attività

Per impostazione predefinita, questa opzione è impostata su 30. Il valore minimo per questa opzione è 10. Il valore massimo per questa opzione è il periodo di tolleranza di blocco, che è possibile impostare con `locking.lease_seconds` opzione.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Specificare il periodo di tolleranza del blocco NFSv4

Per specificare il periodo di tolleranza del blocco NFSv4 (ovvero il periodo di tempo in cui i client tentano di recuperare il proprio stato di blocco da ONTAP durante il ripristino del server), è possibile modificare `-v4-grace-seconds` opzione.

A proposito di questa attività

Per impostazione predefinita, questa opzione è impostata su 45.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Come funzionano i referral NFSv4

Quando si abilitano i riferimenti NFSv4, ONTAP fornisce i riferimenti “intra-SVM” ai client NFSv4. Il riferimento intra-SVM avviene quando un nodo del cluster che riceve la richiesta NFSv4 fa riferimento al client NFSv4 a un'altra interfaccia logica (LIF) sulla macchina virtuale di storage (SVM).

Il client NFSv4 deve accedere al percorso che ha ricevuto il riferimento alla LIF di destinazione da quel momento in poi. Il nodo del cluster originale fornisce tale riferimento quando determina l'esistenza di una LIF nella SVM residente sul nodo del cluster su cui risiede il volume di dati, consentendo ai client un accesso più rapido ai dati ed evitando comunicazioni del cluster aggiuntive.

Attiva o disattiva i riferimenti NFSv4

È possibile attivare i riferimenti NFSv4 sulle macchine virtuali di storage (SVM) attivando le opzioni `-v4-fsid-change` e `-v4.0-referrals` oppure. L'attivazione dei riferimenti

NFSv4 può accelerare l'accesso ai dati per i client NFSv4 che supportano questa funzionalità.

Di cosa hai bisogno

Se si desidera attivare i riferimenti NFS, è necessario prima disattivare Parallel NFS. Non è possibile attivare entrambi contemporaneamente.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare i riferimenti NFSv4	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</pre>
Disattiva i riferimenti NFSv4	<pre>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</pre>
Abilitare i riferimenti NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</pre>
Disattiva i riferimenti NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Visualizzare le statistiche NFS

È possibile visualizzare le statistiche NFS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NFS da cui è possibile visualizzare i dati.

```
statistics catalog object show -object nfs*
```

2. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Esempio: Monitoraggio delle performance di NFSv3

L'esempio seguente mostra i dati relativi alle prestazioni per il protocollo NFSv3.

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

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Il comando seguente mostra i dati dell'esempio specificando i contatori che mostrano il numero di richieste di lettura e scrittura riuscite rispetto al numero totale di richieste di lettura e scrittura:

```
vs1::> statistics show -sample-id nfs_sample -counter  
read_total|write_total|read_success|write_success
```

Object: nfsv3

Instance: vs1

Start-time: 2/11/2013 15:38:29

End-time: 2/11/2013 15:38:41

Cluster: cluster1

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

Visualizzare le statistiche DNS

È possibile visualizzare le statistiche DNS per le macchine virtuali di storage (SVM) sul sistema di storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti DNS da cui è possibile visualizzare i dati.

```
statistics catalog object show -object external_service_op*
```

2. Utilizzare `statistics start` e `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Monitoraggio delle statistiche DNS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query DNS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id  
dns_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
dns_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di query DNS inviate rispetto al numero di query DNS ricevute, non riuscite o in timeout:

```
vs1::*> statistics show -sample-id dns_sample1 -counter  
num_requests_sent|num_responses_received|num_successful_responses|num_time  
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op  
Instance: vs1:DNS:Query:10.72.219.109  
Start-time: 3/8/2016 11:15:21  
End-time: 3/8/2016 11:16:52  
Elapsed-time: 91s  
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di volte in cui è stato ricevuto un errore specifico per una query DNS sul server specifico:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

Object: external_service_op_error

Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109

Start-time: 3/8/2016 11:23:21

End-time: 3/8/2016 11:24:25

Elapsed-time: 64s

Scope: vs1

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

Visualizzare le statistiche NIS

È possibile visualizzare le statistiche NIS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NIS da cui è possibile visualizzare i dati.

```
statistics catalog object show -object external_service_op*
```

2. Utilizzare `statistics start` e `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Monitoraggio delle statistiche NIS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query NIS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che mostrano il numero di query NIS

inviata rispetto al numero di query NIS ricevute, non riuscite o in timeout:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Il seguente comando visualizza i dati dell'esempio specificando i contatori che indicano il numero di volte in cui è stato ricevuto un errore specifico per una query NIS sul server specifico:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

Supporto per VMware vStorage su NFS

ONTAP supporta alcune API vStorage VMware per l'integrazione degli array (VAAI) in un ambiente NFS.

Funzionalità supportate

Sono supportate le seguenti funzioni:

- Offload delle copie

Consente a un host ESXi di copiare macchine virtuali o dischi di macchine virtuali (VMDK) direttamente tra la posizione dell'archivio dati di origine e di destinazione senza coinvolgere l'host. In questo modo si preservano i cicli della CPU host ESXi e la larghezza di banda della rete. L'offload delle copie preserva l'efficienza dello spazio se il volume di origine è sparso.

- Prenotazione di spazio

Garantisce lo spazio di storage per un file VMDK riservando spazio all'IT.

Limitazioni

VMware vStorage su NFS presenta le seguenti limitazioni:

- Le operazioni di offload della copia possono avere esito negativo nei seguenti scenari:
 - Durante l'esecuzione di wafiron sul volume di origine o di destinazione, in quanto il volume viene temporaneamente disattivato
 - Durante lo spostamento del volume di origine o di destinazione
 - Durante lo spostamento della LIF di origine o di destinazione
 - Durante l'esecuzione di operazioni di Takeover o giveback
 - Durante le operazioni di switchover o switchback
- La copia lato server potrebbe non riuscire a causa delle differenze di formato del file handle nel seguente scenario:

Si tenta di copiare i dati dalle SVM che hanno attualmente o precedentemente esportato qtree in SVM che non hanno mai esportato qtree. Per aggirare questo limite, è possibile esportare almeno un qtree sulla SVM di destinazione.

Informazioni correlate

["Quali operazioni VAAI offloaded sono supportate da Data ONTAP?"](#)

Abilitare o disabilitare VMware vStorage su NFS

È possibile attivare o disattivare il supporto per VMware vStorage su NFS su macchine virtuali di storage (SVM) utilizzando `vserver nfs modify` comando.

A proposito di questa attività

Per impostazione predefinita, il supporto di VMware vStorage su NFS è disattivato.

Fasi

1. Visualizzare lo stato corrente del supporto vStorage per le SVM:

```
vserver nfs show -vserver vserver_name -instance
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare il supporto di VMware vStorage	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
Disattivare il supporto di VMware vStorage	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

Al termine

Prima di utilizzare questa funzionalità, è necessario installare il plug-in NFS per VMware VAAI. Per ulteriori informazioni, consulta la sezione *Installazione del plug-in NetApp NFS per VMware VAAI*.

Informazioni correlate

["Documentazione NetApp: Plug-in NetApp NFS per VMware VAAI"](#)

Attiva o disattiva il supporto rquota

ONTAP supporta il protocollo di quota remota versione 1 (rquota v1). Il protocollo rquota consente ai client NFS di ottenere informazioni sulle quote per gli utenti da un computer remoto. È possibile attivare rquota su macchine virtuali storage (SVM) utilizzando `vserver nfs modify` comando.

A proposito di questa attività

Per impostazione predefinita, rquota è disattivato.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare il supporto rquota per le SVM	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
Disattiva il supporto rquota per le SVM	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

Per ulteriori informazioni sulle quote, vedere ["Gestione dello storage logico"](#).

Miglioramento delle performance di NFSv3 e NFSv4 modificando le dimensioni del trasferimento TCP

È possibile migliorare le prestazioni dei client NFSv3 e NFSv4 che si connettono ai sistemi storage su una rete ad alta latenza modificando le dimensioni massime di

trasferimento TCP.

Quando i client accedono ai sistemi storage su una rete ad alta latenza, ad esempio WAN (Wide Area Network) o MAN (Metro Area Network) con una latenza superiore a 10 millisecondi, è possibile migliorare le prestazioni di connessione modificando le dimensioni massime di trasferimento TCP. I client che accedono a sistemi storage in una rete a bassa latenza, come una LAN (Local Area Network), possono aspettarsi pochi benefici dalla modifica di questi parametri. Se il miglioramento del throughput non supera l'impatto della latenza, non utilizzare questi parametri.

Per determinare se il tuo ambiente di storage potrebbe trarre beneficio dalla modifica di questi parametri, devi prima eseguire una valutazione completa delle performance di un client NFS dalle performance scarse. Verificare se le performance ridotte sono dovute a un'eccessiva latenza di round trip e a una piccola richiesta sul client. In queste condizioni, il client e il server non possono utilizzare completamente la larghezza di banda disponibile perché trascorrono la maggior parte dei loro cicli di lavoro in attesa di piccole richieste e risposte da trasmettere sulla connessione.

Aumentando le dimensioni delle richieste NFSv3 e NFSv4, il client e il server possono utilizzare la larghezza di banda disponibile in modo più efficace per spostare più dati per unità di tempo, aumentando quindi l'efficienza complessiva della connessione.

Tenere presente che la configurazione tra il sistema storage e il client potrebbe variare. Il sistema storage e il client supportano una dimensione massima di 1 MB per le operazioni di trasferimento. Tuttavia, se si configura il sistema di storage in modo che supporti le dimensioni massime di trasferimento di 1 MB ma il client supporta solo 64 KB, la dimensione di trasferimento del mount è limitata a 64 KB o meno.

Prima di modificare questi parametri, è necessario tenere presente che questo comporta un consumo di memoria aggiuntivo nel sistema di storage per il periodo di tempo necessario per assemblare e trasmettere una risposta elevata. Maggiore è la latenza elevata delle connessioni al sistema storage, maggiore è il consumo di memoria aggiuntivo. I sistemi storage con elevata capacità di memoria potrebbero avere un effetto molto ridotto da questo cambiamento. I sistemi storage con capacità di memoria bassa potrebbero riscontrare un notevole peggioramento delle performance.

Il corretto utilizzo di questi parametri dipende dalla capacità di recuperare i dati da più nodi di un cluster. La latenza intrinseca della rete del cluster potrebbe aumentare la latenza complessiva della risposta. La latenza complessiva tende ad aumentare quando si utilizzano questi parametri. Di conseguenza, i carichi di lavoro sensibili alla latenza potrebbero avere un impatto negativo.

Modificare le dimensioni massime di trasferimento TCP NFSv3 e NFSv4

È possibile modificare `-tcp-max-xfer-size` Opzione per configurare le dimensioni massime di trasferimento per tutte le connessioni TCP utilizzando i protocolli NFSv3 e NFSv4.x.

A proposito di questa attività

È possibile modificare queste opzioni singolarmente per ciascuna macchina virtuale di storage (SVM).

A partire da ONTAP 9 `v3-tcp-max-read-size` e `v3-tcp-max-write-size` le opzioni sono obsolete. È necessario utilizzare `-tcp-max-xfer-size` invece.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Modificare le dimensioni massime di trasferimento TCP NFSv3 o NFSv4	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

Opzione	Raggio d'azione	Predefinito
-tcp-max-xfer-size	da 8192 a 1048576 byte	65536 byte



La dimensione massima di trasferimento immessa deve essere un multiplo di 4 KB (4096 byte). Le richieste non allineate correttamente influiscono negativamente sulle performance.

3. Utilizzare `vserver nfs show -fields tcp-max-xfer-size` per verificare le modifiche.
4. Se alcuni client utilizzano i mount statici, smontare e rimontare per rendere effettive le nuove dimensioni dei parametri.

Esempio

Il seguente comando imposta le dimensioni massime di trasferimento TCP NFSv3 e NFSv4.x su 1048576 byte sulla SVM denominata vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurare il numero di ID di gruppo consentiti per gli utenti NFS

Per impostazione predefinita, ONTAP supporta fino a 32 ID di gruppo quando gestisce le credenziali utente NFS utilizzando l'autenticazione Kerberos (RPCSEC_GSS). Quando si utilizza l'autenticazione AUTH_SYS, il numero massimo predefinito di ID gruppo è 16, come definito in RFC 5531. È possibile aumentare il numero massimo fino a 1,024 se si dispone di utenti che fanno parte di un numero di gruppi superiore a quello predefinito.

A proposito di questa attività

Se un utente dispone di un numero di ID di gruppo superiore a quello predefinito nelle proprie credenziali, gli ID di gruppo rimanenti vengono troncati e l'utente potrebbe ricevere errori quando tenta di accedere ai file dal sistema di storage. Impostare il numero massimo di gruppi, per SVM, su un numero che rappresenta il numero massimo di gruppi nell'ambiente.

La seguente tabella mostra i due parametri di `vserver nfs modify` Comando che determina il numero massimo di ID di gruppo in tre configurazioni di esempio:

Parametri	Impostazioni	Limite ID gruppo risultante
-----------	--------------	-----------------------------

-extended-groups-limit	32	RPCSEC_GSS: 32
-auth-sys-extended-groups	disabled	AUTH_SYS: 16
Queste sono le impostazioni predefinite.		
-extended-groups-limit	256	RPCSEC_GSS: 256
-auth-sys-extended-groups	disabled	AUTH_SYS: 16
-extended-groups-limit	512	RPCSEC_GSS: 512
-auth-sys-extended-groups	enabled	AUTH_SYS: 512

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera impostare il numero massimo di gruppi ausiliari consentiti...	Immettere il comando...
Solo per RPCSEC_GSS e lasciare AUTH_SYS impostato sul valore predefinito 16	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</pre>
Per RPCSEC_GSS e AUTH_SYS	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</pre>

3. Verificare -extended-groups-limit Valutare e verificare se AUTH_SYS utilizza gruppi estesi:

```
vserver nfs show -vserver vserver_name -fields auth-sys-extended-  
groups,extended-groups-limit
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

Nell'esempio riportato di seguito vengono abiliti i gruppi estesi per l'autenticazione AUTH_SYS e viene impostato il numero massimo di gruppi estesi su 512 per l'autenticazione AUTH_SYS e RPCSEC_GSS. Queste modifiche vengono apportate solo ai client che accedono alla SVM denominata vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                      512

vs1::*> set -privilege admin

```

Controllare l'accesso dell'utente root ai dati di sicurezza NTFS

È possibile configurare ONTAP per consentire ai client NFS di accedere ai dati di sicurezza NTFS e ai client NTFS per accedere ai dati di sicurezza NFS. Quando si utilizza lo stile di sicurezza NTFS su un archivio dati NFS, è necessario decidere come trattare l'accesso da parte dell'utente root e configurare di conseguenza la macchina virtuale di storage (SVM).

A proposito di questa attività

Quando un utente root accede ai dati di sicurezza NTFS, sono disponibili due opzioni:

- Mappare l'utente root a un utente Windows come qualsiasi altro utente NFS e gestire l'accesso in base agli ACL NTFS.
- Ignorare gli ACL NTFS e fornire l'accesso completo all'utente root.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera che l'utente root...	Immettere il comando...
Essere mappato a un utente Windows	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled</code>
Ignorare il controllo dell'ACL NT	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled</code>

Per impostazione predefinita, questo parametro è disattivato.

Se questo parametro è attivato ma non esiste alcuna mappatura dei nomi per l'utente root, ONTAP utilizza una credenziale di amministratore SMB predefinita per il controllo.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Versioni e client NFS supportati

Panoramica delle versioni e dei client NFS supportati

Prima di poter utilizzare NFS nella rete, è necessario conoscere le versioni e i client NFS supportati da ONTAP.

Questa tabella indica quando le versioni principali e minori dei protocolli NFS sono supportate per impostazione predefinita in ONTAP. Il supporto predefinito non indica che si tratta della prima versione di ONTAP che supporta tale protocollo NFS.

Versione	Attivato per impostazione predefinita
NFSv3	Sì
NFSv4.0	Sì, a partire da ONTAP 9.9.1
NFSv4.1	Sì, a partire da ONTAP 9.9.1
NFSv4.2	Sì, a partire da ONTAP 9.9.1
PNFS	No

Per informazioni aggiornate sui client NFS supportati da ONTAP, consulta la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

Funzionalità NFSv4.0 supportata da ONTAP

ONTAP supporta tutte le funzionalità obbligatorie di NFSv4.0, ad eccezione dei meccanismi di sicurezza SPKM3 e LIPKEY.

Sono supportate le seguenti funzionalità DI NFSV4:

- **COMPOSTO**

Consente a un client di richiedere più operazioni di file in una singola richiesta RPC (Remote procedure Call).

- **Delega del file**

Consente al server di delegare il controllo del file ad alcuni tipi di client per l'accesso in lettura e scrittura.

- **Pseudo-fs**

Utilizzato dai server NFSv4 per determinare i punti di montaggio sul sistema storage. NFSv4 non contiene alcun protocollo di montaggio.

- **Blocco**

Basato sul leasing. Non esistono protocolli NLM (Network Lock Manager) o NSM (Network Status Monitor) separati in NFSv4.

Per ulteriori informazioni sul protocollo NFSv4.0, vedere RFC 3530.

Limitazioni del supporto ONTAP per NFSv4

È necessario conoscere diverse limitazioni del supporto ONTAP per NFSv4.

- La funzione di delega non è supportata da ogni tipo di client.
- In ONTAP 9.4 e versioni precedenti, i nomi con caratteri non ASCII su volumi diversi da UTF8 vengono rifiutati dal sistema di storage.

In ONTAP 9.5 e versioni successive, i volumi creati con l'impostazione del linguaggio utf8mb4 e montati utilizzando NFS v4 non sono più soggetti a questa restrizione.

- Tutti gli handle di file sono persistenti; il server non fornisce handle di file volatili.
- Migrazione e replica non sono supportate.
- I client NFSv4 non sono supportati con mirror di sola lettura per la condivisione del carico.

ONTAP indirizza i client NFSv4 all'origine del mirror di condivisione del carico per l'accesso diretto in lettura e scrittura.

- Gli attributi denominati non sono supportati.
- Sono supportati tutti gli attributi consigliati, ad eccezione di:

- archive
- hidden
- homogeneous
- mimetype
- quota_avail_hard
- quota_avail_soft
- quota_used
- system
- time_backup



Anche se non supporta `quota*` ONTAP supporta le quote utente e di gruppo tramite il protocollo RQUOTA Side Band.

Supporto ONTAP per NFSv4.1

A partire da ONTAP 9.8, la funzionalità `nconnect` è disponibile per impostazione predefinita quando NFSv4.1 è attivato.

Le implementazioni dei client NFS precedenti utilizzano solo una singola connessione TCP con un mount. In ONTAP, una singola connessione TCP può diventare un collo di bottiglia con un aumento degli IOPS. Tuttavia, un client abilitato a `nconnect` può avere più connessioni TCP (fino a 16) associate a un singolo montaggio NFS. Un client NFS di questo tipo moltiplica le operazioni di file su più connessioni TCP in modo round-robin e ottiene così un throughput più elevato dalla larghezza di banda di rete disponibile. `NConnect` è consigliato solo per i supporti NFSv3 e NFSv4.1.

Consultare la documentazione del client NFS per verificare se `nconnect` è supportato nella versione del client.

NFSv4.1 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. Nelle versioni precedenti, è possibile attivarlo specificando `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM).

ONTAP non supporta le deleghe a livello di file e directory NFSv4.1.

Supporto ONTAP per NFSv4.2

A partire da ONTAP 9.8, ONTAP supporta il protocollo NFSv4.2 per consentire l'accesso a client abilitati per NFSv4.2.

NFSv4.2 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. In ONTAP 9.8, è necessario attivare manualmente `v4.2` specificando il `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM). L'abilitazione di NFSv4.1 consente inoltre ai client di utilizzare le funzionalità di NFSv4.1 mentre sono montati come `v4.2`.

Le successive versioni di ONTAP ampliano il supporto per NFSv4.2 funzioni opzionali.

A partire da...	NFSv4.2 caratteristiche opzionali includono ...
ONTAP 9.12.1	<ul style="list-style-type: none">• Attributi estesi NFS• File sparse• Prenotazioni di spazio
ONTAP 9.9.1	Obbligatorio Access Control (MAC) con etichetta NFS

Etichette di sicurezza NFS v4.2

A partire da ONTAP 9.9.1, è possibile attivare le etichette di sicurezza NFS. Sono disattivati per impostazione predefinita.

Con le etichette di sicurezza NFS v4.2, i server NFS ONTAP sono compatibili con il controllo di accesso obbligatorio (MAC), memorizzando e recuperando gli attributi `sec_label` inviati dai client.

Per ulteriori informazioni, vedere ["RFC 7240"](#).

A partire da ONTAP 9.12.1, le etichette di sicurezza NFS v4.2 sono supportate per le operazioni di dump NDMP. Se vengono rilevate etichette di sicurezza su file o directory nelle release precedenti, il dump non riesce.

Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Abilitare le etichette di sicurezza:

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

Attributi estesi NFS

A partire da ONTAP 9.12.1, gli attributi estesi NFS (xattrs) sono attivati per impostazione predefinita.

Gli attributi estesi sono attributi NFS standard definiti da ["RFC 8276"](#) E abilitato nei moderni client NFS. Possono essere utilizzate per collegare metadati definiti dall'utente a oggetti del file system e sono interessanti per implementazioni di sicurezza avanzate.

Gli attributi estesi NFS non sono attualmente supportati per le operazioni di dump NDMP. Se vengono rilevati attributi estesi su file o directory, il dump procede ma non esegue il backup degli attributi estesi su tali file o directory.

Se è necessario disattivare gli attributi estesi, utilizzare `vserver nfs modify -v4.2-xattrs disabled` comando.

Supporto ONTAP per NFS parallelo

ONTAP supporta NFS paralleli (pNFS). Il protocollo pNFS offre miglioramenti delle performance offrendo ai client l'accesso diretto ai dati di un set di file distribuiti su più nodi di un cluster. Aiuta i clienti a individuare il percorso ottimale per un volume.

Utilizzo di supporti rigidi

Durante la risoluzione dei problemi di montaggio, assicurarsi di utilizzare il tipo di montaggio corretto. NFS supporta due tipi di montaggio: Supporti morbidi e hard mount. Per motivi di affidabilità, utilizzare solo supporti rigidi.

Non si consiglia di utilizzare supporti soft, soprattutto quando è possibile che si verificano frequenti timeout NFS. Le condizioni di gara possono verificarsi in seguito a questi timeout, che possono portare alla corruzione dei dati.

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` il 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 `test.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` il 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 creata una mappatura dei caratteri utilizzando i comandi di mappatura dei caratteri CIFS di Vserver, una ricerca di Windows che normalmente non fa distinzione tra maiuscole e minuscole può diventare sensibile al maiuscolo/minuscolo. Ciò significa che le ricerche dei nomi file distinguono tra maiuscole e minuscole solo se la mappatura dei caratteri è stata creata e il nome del file sta utilizzando la mappatura dei caratteri.

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 {...}
```

- Se si utilizza ONTAP 9.6 e versioni precedenti, non è possibile modificare i volumi esistenti per il supporto di utf8mb4; è necessario creare un nuovo volume utf8mb4-ready e quindi migrare i dati utilizzando strumenti di copia basati su client.

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?"](#).

È possibile aggiornare le SVM per il supporto di utf8mb4, ma i volumi esistenti conservano i codici lingua originali.



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.

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
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

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	<code>vserver cifs character-mapping create</code>
Visualizza le informazioni sulle mappature dei caratteri del file	<code>vserver cifs character-mapping show</code>
Modificare le mappature dei caratteri del file esistente	<code>vserver cifs character-mapping modify</code>
Eliminare le mappature dei caratteri del file	<code>vserver cifs character-mapping delete</code>

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

Gestire il trunking NFS

Panoramica del trunking NFS

A partire da ONTAP 9.14.1, i client NFSv4,1 possono sfruttare il trunking di sessione per aprire più connessioni a diverse LIF sul server NFS, aumentando in tal modo la velocità di trasferimento dei dati e fornendo resilienza tramite multipathing.

Il trunking è vantaggioso per l'esportazione di volumi FlexVol in client compatibili con il trunking, in particolare client VMware e Linux, o per NFS su RDMA, TCP o pNFS.

In ONTAP 9.14.1, il trunking è limitato alle LIF in un singolo nodo; il trunking non può estendersi a LIF in più nodi.

I volumi FlexGroup sono supportati per il trunking. Anche se in questo modo è possibile ottenere performance migliori, l'accesso multipath a un volume FlexGroup può essere configurato solo su un singolo nodo.

In questa versione, è supportato solo il trunking di sessione per il multipathing.

Come utilizzare il trunking

Per sfruttare i vantaggi del multipathing offerti dal trunking, è necessario disporre di una serie di LIF, definite *gruppo trunking*, associate alla SVM contenente un server NFS abilitato al trunking. Le LIF in un gruppo trunking devono avere porte home sullo stesso nodo del cluster e devono risiedere in tali porte home. È consigliabile che tutte le LIF in un gruppo trunking siano membri dello stesso gruppo di failover.

ONTAP supporta fino a 16 connessioni trunked per nodo da un determinato client.

Quando un client esegue l'esportazione da un server abilitato al trunking, specifica un numero di indirizzi IP per le LIF in un gruppo trunking. Una volta che il client si connette alla prima LIF, le LIF aggiuntive vengono aggiunte alla sessione NFSv4.1 e utilizzate per il trunking se conformi ai requisiti del gruppo di trunking. Il client distribuisce quindi le operazioni NFS su più connessioni in base al proprio algoritmo (ad esempio round-robin).

Per ottenere performance ottimali, è necessario configurare il trunking in una SVM dedicata all'esportazione multipath, non all'esportazione single-path. In altre parole, è necessario abilitare il trunking su un server NFS in una SVM le cui esportazioni vengono fornite solo ai client abilitati al trunking.

Client supportati

Il server ONTAP NFSv4.1 supporta il trunking con qualsiasi client in grado di utilizzare il trunking di sessione NFSv4.1.

I seguenti client sono stati testati con ONTAP 9.14.1:

- VMware - ESXi 7.0U3F e versioni successive
- Linux - Red Hat Enterprise Linux (RHEL) 8,8 e 9,3



Quando il trunking è abilitato su un server NFS, gli utenti che accedono a condivisioni esportate su client NFS che non supportano il trunking potrebbero riscontrare un calo delle prestazioni. Questo perché viene utilizzata solo una connessione TCP per diversi mount delle LIF dati SVM.

Differenza tra NFS trunking e nconnect

A partire da ONTAP 9.8, la funzionalità nconnect è disponibile per impostazione predefinita quando NFSv4.1 è attivato. Nei client nConnect-capable, un singolo montaggio NFS può avere più connessioni TCP (fino a 16 Gbps) su una singola LIF.

Al contrario, il trunking è la funzionalità *multipathing*, che fornisce più connessioni TCP su LIF multiple. Se si dispone della possibilità di utilizzare schede NIC aggiuntive nell'ambiente, il trunking offre un parallelismo e prestazioni superiori rispetto alle funzionalità di nconnect.

Scopri di più "[nconnettiti](#)."

Configurare un nuovo server NFS ed esportare per il trunking

Creare un server NFS abilitato al trunking

A partire da ONTAP 9.14.1, il trunking può essere abilitato sui server NFS. NFSv4.1 è attivato per impostazione predefinita quando vengono creati i server NFS.

Prima di iniziare

La SVM deve essere:

- supportato da uno storage sufficiente per i requisiti dei dati dei client.
- Abilitato per NFS.
- Dedicato al trunking NFS. Nessun altro client deve essere configurato su di esso.

Fasi

1. Se non esiste una SVM idonea, creane una:

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate  
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver svm_name
```

Scopri di più ["Creazione di una SVM."](#)

3. Creare il server NFS:

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled  
-v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver svm_name
```

5. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver svm_name
```

Scopri di più ["Configurazione del server NFS."](#)

Al termine

Configurare i seguenti servizi in base alle esigenze:

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

Preparare la rete per il trunking

Per sfruttare il trunking NFSv4,1, le LIF di un gruppo trunking devono risiedere sullo stesso nodo e disporre di porte home sullo stesso nodo. Le LIF devono essere configurate in un gruppo di failover sullo stesso nodo.

A proposito di questa attività

Una mappatura uno a uno di LIF e NIC consente di ottenere il massimo guadagno in termini di prestazioni, ma non è necessaria per abilitare il trunking. L'installazione di almeno due NIC può offrire vantaggi in termini di prestazioni, ma non è necessaria.

È possibile disporre di più gruppi di failover, ma il gruppo di failover per il trunking deve includere solo i file LIFS nel gruppo trunking.

È necessario regolare il gruppo di failover trunking ogni volta che si aggiungono o rimuovono connessioni (e NIC sottostanti) da un gruppo di failover.

Prima di iniziare

- Se si desidera creare un gruppo di failover, è necessario conoscere i nomi delle porte associate alle schede NIC.
- Le porte devono essere tutte sullo stesso nodo.

Fasi

1. Verificare i nomi e lo stato delle porte di rete che si intende utilizzare:

```
network port status
```

2. Creare il gruppo di failover:

```
network interface failover-groups create -vserver svm_name -failover-group  
failover_group_name -targets ports_list
```



Non è un requisito per avere un gruppo di failover, ma è vivamente consigliato.

- *svm_name* È il nome della SVM che contiene il server NFS.
- *ports_list* è l'elenco delle porte che verranno aggiunte al gruppo di failover.

Le porte vengono aggiunte nel formato *node_name:port_number*, ad esempio, *node1:e0c*.

Questo comando crea il gruppo di failover FG3 per SVM VS1 e aggiunge tre porte:

```
network interface failover-groups create -vserver vs1 -failover-group fg3  
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Scopri di più ["gruppi di failover."](#)

3. Se necessario, creare LIF per i membri del gruppo trunking:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name  
-home-port port_name -address IP_address -netmask IP_address [-service-policy  
policy] [-auto-revert {true|false}]
```

- *-home-node* - Il nodo da cui la LIF ritorna quando il comando di revert dell'interfaccia di rete viene eseguito sulla LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con *-auto-revert* opzione.

- *-home-port* Indica la porta fisica o logica alla quale la LIF ritorna quando il comando di indirizzamento dell'interfaccia di rete viene eseguito sulla LIF.
- È possibile specificare un indirizzo IP con *-address* e *-netmask* opzioni, non con *-subnet* opzione.

- Quando si assegnano gli indirizzi IP, potrebbe essere necessario configurare un percorso predefinito per un gateway se ci sono client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- `-service-policy` - La politica di servizio per la LIF. Se non viene specificato alcun criterio, viene assegnato automaticamente un criterio predefinito. Utilizzare `network interface service-policy show` per esaminare le politiche di servizio disponibili.
- `-auto-revert` - Consente di specificare se un data LIF viene automaticamente riportato al suo nodo principale in circostanze come l'avvio, modifiche allo stato del database di gestione o quando viene effettuata la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarla su `true` in base ai criteri di gestione della rete nell'ambiente.

Ripetere questo passaggio per ogni LIF nel gruppo trunking.

Viene creato il seguente comando `lif-A` Per SVM `vs1`, sulla porta `e0c` del nodo `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Scopri di più ["Creazione LIF."](#)

4. Verificare che la LIF sia stata creata:

```
network interface show
```

5. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

Esportare i dati per l'accesso client

Per fornire al client l'accesso alle condivisioni di dati, è necessario creare uno o più volumi e il volume deve disporre di policy di esportazione con almeno una regola.

Requisiti di esportazione client:

- I client Linux devono avere un mount separato e un mount point separato per ogni connessione trunking (vale a dire, per ogni LIF).
- I client VMware richiedono solo un punto di montaggio singolo per un volume esportato, con diverse LIF specificate.

I client VMware richiedono l'accesso root nel criterio di esportazione.

Fasi

1. Creare una policy di esportazione:

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

Il nome del criterio può contenere fino a 256 caratteri.

2. Verificare che il criterio di esportazione sia stato creato:

```
vserver export-policy show -policyname policy_name
```

Esempio

I seguenti comandi creano e verificano la creazione di una policy di esportazione denominata exp1 sulla SVM denominata vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. Creare una regola di esportazione e aggiungerla a un criterio di esportazione esistente:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Il `-clientmatch` Il parametro deve identificare i client Linux o VMware che supportano il trunking che montano l'esportazione.

Scopri di più ["creazione di regole di esportazione."](#)

4. Creare il volume con un punto di giunzione:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Scopri di più ["creazione di volumi."](#)

5. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

Creare montaggi client

I client Linux e VMware che supportano il trunking possono montare volumi o condivisioni di dati da un server ONTAP NFSv4.1 abilitato per il trunking.

Quando si immettono i comandi mount sui client, è necessario immettere gli indirizzi IP per ogni LIF nel gruppo trunking.

Scopri di più ["client supportati"](#).

Requisiti del client Linux

È necessario un punto di montaggio separato per ciascuna connessione nel gruppo trunking.

Montare i volumi esportati con comandi simili ai seguenti:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

La versione (`vers`) il valore deve essere 4.1 o versioni successive.

Il `max_connect` il valore corrisponde al numero di connessioni nel gruppo trunking.

Requisiti del client VMware

È necessaria un'istruzione mount che includa un indirizzo IP per ciascuna connessione nel gruppo trunking.

Montare il datastore esportato con un comando simile al seguente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Il `-H` i valori corrispondono alle connessioni nel gruppo trunking.

Adattare le esportazioni NFS esistenti per il trunking

Adattamento della panoramica delle esportazioni a percorso singolo

È possibile adattare un'esportazione NFSv4,1 a percorso singolo (non trunked) esistente per utilizzare il trunking. I client con funzionalità trunking possono trarre vantaggio da prestazioni migliorate non appena il trunking viene abilitato sul server, a condizione che i prerequisiti del server e del client siano soddisfatti.

L'adattamento di un'esportazione a percorso singolo per il trunking consente di mantenere i set di dati esportati in volumi e SVM esistenti. A tale scopo, è necessario abilitare il trunking sul server NFS, aggiornare la configurazione di rete ed esportarla e rimontare la condivisione esportata sui client.

L'attivazione del trunking ha l'effetto di riavviare il server. I client VMware devono quindi rimontare i datastore esportati, mentre i client Linux devono rimontare i volumi esportati con `max_connect` opzione.

Abilitare il trunking sul server NFS

Il trunking deve essere esplicitamente attivato sui server NFS. NFSv4,1 è attivato per impostazione predefinita quando vengono creati i server NFS.

Dopo aver attivato il trunking, verificare che i seguenti servizi siano configurati come necessario.

- "DNS"
- "LDAP"
- "Kerberos"

Fasi

1. Abilitare il trunking e assicurarsi che NFSv4,1 sia abilitato:

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver svm_name
```

3. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver svm_name
```

Scopri di più ["Configurazione del server NFS."](#)

.. Se fornisci client Windows da questa SVM, sposta le condivisioni ed elimina il server.

```
vserver cifs show -vserver svm_name
```

+

```
vserver cifs delete -vserver svm_name
```

Aggiornare la rete per il trunking

Il trunking NFSv4,1 richiede che le LIF di un gruppo trunking risiedano sullo stesso nodo e dispongano di porte home sullo stesso nodo. Tutte le LIF devono essere configurate in un gruppo di failover sullo stesso nodo.

A proposito di questa attività

Una mappatura uno a uno di LIF e NIC consente di ottenere il massimo guadagno in termini di prestazioni, ma non è necessaria per abilitare il trunking.

È possibile disporre di più gruppi di failover, ma il gruppo di failover per il trunking deve includere solo questi LIFS nel gruppo trunking.

È necessario regolare il gruppo di failover trunking ogni volta che si aggiungono o rimuovono connessioni (e NIC sottostanti) da un gruppo di failover.

Prima di iniziare

- Per creare un gruppo di failover, è necessario conoscere i nomi delle porte associate alle schede NIC.
- Le porte devono essere tutte sullo stesso nodo.

Fasi

1. Verificare i nomi e lo stato delle porte di rete che si intende utilizzare:

```
network port show
```

2. Creare un gruppo di failover trunking o modificarne uno esistente per il trunking:

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group failover_group_name -targets ports_list
```



Non è un requisito per avere un gruppo di failover, ma è vivamente consigliato.

- *svm_name* È il nome della SVM che contiene il server NFS.
- *ports_list* è l'elenco delle porte che verranno aggiunte al gruppo di failover.

Le porte vengono aggiunte nel formato *node_name:port_number*, ad esempio, *node1:e0c*.

Il comando seguente crea un gruppo di failover *fg3* Per SVM *VS1* e aggiunge tre porte:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Scopri di più ["gruppi di failover."](#)

3. Creare LIF aggiuntive per i membri del gruppo trunking, se necessario:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- *-home-node* - Il nodo da cui la LIF ritorna quando il comando di revert dell'interfaccia di rete viene eseguito sulla LIF.

Puoi specificare se la LIF deve tornare automaticamente al nodo home e alla porta home con il *-auto-revert* opzione.

- *-home-port* Indica la porta fisica o logica alla quale la LIF ritorna quando il comando di indirizzamento dell'interfaccia di rete viene eseguito sulla LIF.
- È possibile specificare un indirizzo IP con *-address* e. *-netmask* opzioni.
- Quando si assegnano gli indirizzi IP manualmente (senza usare una subnet), potrebbe essere necessario configurare un percorso predefinito per un gateway se ci sono client o controller di dominio su una subnet IP diversa. La pagina man di creazione di percorsi di rete contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- *-service-policy* - La politica di servizio per la LIF. Se non viene specificato alcun criterio, viene assegnato automaticamente un criterio predefinito. Utilizzare `network interface service-policy show` per esaminare le politiche di servizio disponibili.
- *-auto-revert* - Consente di specificare se un data LIF viene automaticamente riportato al suo nodo principale in circostanze come l'avvio, modifiche allo stato del database di gestione o quando viene effettuata la connessione di rete. **L'impostazione predefinita è false**, ma è possibile impostarla su true in base ai criteri di gestione della rete nel proprio ambiente.

Ripetere questo passaggio per ogni LIF aggiuntivo necessario nel gruppo di trunking.

Il seguente comando crea *lif-A* per la SVM *VS1*, sulla porta *e0c* del nodo *cluster1_01*:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Scopri di più ["Creazione LIF."](#)

4. Verificare che la LIF sia stata creata:

```
network interface show
```

5. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

Modificare l'esportazione dei dati per l'accesso client

Per consentire ai client di sfruttare il trunking per le condivisioni di dati esistenti, potrebbe essere necessario modificare i criteri e le regole di esportazione e i volumi a cui sono collegati. Esistono diversi requisiti di esportazione per i client Linux e i datastore VMware.

Requisiti di esportazione client:

- I client Linux devono avere un mount separato e un mount point separato per ogni connessione trunking (vale a dire, per ogni LIF).

Se si esegue l'aggiornamento a ONTAP 9.14.1 ed è già stato esportato un volume, è possibile continuare a utilizzare tale volume in un gruppo trunking.

- I client VMware richiedono solo un punto di montaggio singolo per un volume esportato, con diverse LIF specificate.

I client VMware richiedono l'accesso root nel criterio di esportazione.

Fasi

1. Verificare che sia in vigore un criterio di esportazione esistente:

```
vserver export-policy show
```

2. Verificare che le regole dei criteri di esportazione esistenti siano appropriate per la configurazione trunking:

```
vserver export-policy rule show -policyname policy_name
```

In particolare, verificare che `-clientmatch` Parametro identifica correttamente i client Linux o VMware che supportano il trunking che montano l'esportazione.

Se sono necessarie regolazioni, modificare la regola utilizzando `vserver export-policy rule modify` o creare una nuova regola:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Scopri di più ["creazione di regole di esportazione."](#)

3. Verificare che i volumi esportati esistenti siano online:

```
volume show -vserver svm_name
```

Ristabilire i montaggi dei client

Per convertire le connessioni client non trunked in connessioni trunked, i mount esistenti sui client Linux e VMware devono essere smontati e rimontati utilizzando le informazioni sulle LIF.

Quando si immettono i comandi mount sui client, è necessario immettere gli indirizzi IP per ogni LIF nel gruppo trunking.

Scopri di più ["client supportati"](#).



L'annullamento del montaggio dei client VMware provoca interruzioni per le macchine virtuali presenti nel datastore. Un'alternativa potrebbe essere creare un nuovo datastore abilitato per il trunking e utilizzare **storage vmotion** per spostare le macchine virtuali dal vecchio datastore al nuovo. Per ulteriori informazioni, consultare la documentazione VMware.

Requisiti del client Linux

È necessario un punto di montaggio separato per ciascuna connessione nel gruppo trunking.

Montare i volumi esportati con comandi simili ai seguenti:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

Il `vers` il valore deve essere 4.1 o versioni successive.

Il `max_connect` il valore deve corrispondere al numero di connessioni nel gruppo trunking.

Requisiti del client VMware

È necessaria un'istruzione mount che includa un indirizzo IP per ciascuna connessione nel gruppo trunking.

Montare il datastore esportato con un comando simile al seguente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Il `-H` i valori devono corrispondere alle connessioni nel gruppo trunking.

Gestire NFS su RDMA

NFS su RDMA

NFS su RDMA utilizza adattatori RDMA, che consentono di copiare i dati direttamente tra la memoria del sistema di storage e la memoria del sistema host, eludendo le interruzioni

della CPU e il sovraccarico.

Le configurazioni NFS su RDMA sono progettate per i clienti con carichi di lavoro sensibili alla latenza o a elevata larghezza di banda, come l'apprendimento automatico e l'analisi. NVIDIA ha esteso NFS su RDMA per abilitare GPU Direct Storage (GDS). GDS accelera ulteriormente i carichi di lavoro abilitati alla GPU bypassando la CPU e la memoria principale, utilizzando RDMA per trasferire i dati direttamente tra il sistema di storage e la memoria GPU.

A partire da ONTAP 9.14.1, le configurazioni NFS su RDMA sono supportate per il protocollo NFSv4,1.

A partire da ONTAP 9.10.1, le configurazioni NFS su RDMA sono supportate per il protocollo NFSv4,0 se utilizzato con l'adattatore Mellanox CX-5 o CX-6, che fornisce il supporto per RDMA utilizzando la versione 2 del protocollo RoCE. GDS è supportato solo utilizzando GPU NVIDIA Tesla e Ampere con schede NIC Mellanox e software MOFED.

Il supporto di NFS su RDMA è limitato solo al traffico locale del nodo. FlexVol standard o FlexGroup in cui tutti i componenti si trovano sullo stesso nodo sono supportati e devono essere accessibili da un LIF sullo stesso nodo. Le dimensioni del montaggio NFS superiori a 64k determinano performance instabili con configurazioni NFS su RDMA.

Requisiti

- I sistemi di storage devono eseguire ONTAP 9.10.1 o versione successiva
 - È possibile configurare NFS su RDMA con Gestione di sistema a partire da ONTAP 9.12.1. In ONTAP 9.10.1 e 9.11.1, è necessario utilizzare la CLI per configurare NFS su RDMA.
- Entrambi i nodi della coppia ha devono essere della stessa versione.
- I controller del sistema storage devono disporre del supporto RDMA

Inizio a ONTAP...	I seguenti controller supportano RDMA...
9.10.1 e versioni successive	<ul style="list-style-type: none">• R400• R700• R800
ONTAP 9.14.1 e versioni successive	<ul style="list-style-type: none">• AFF C-Series• R900

- Appliance di storage configurata con hardware supportato da RDMA (ad esempio Mellanox CX-5 o CX-6).
- Le LIF dei dati devono essere configurate per supportare RDMA.
- I client devono utilizzare schede NIC Mellanox RDMA e software di rete Mellanox OFED (MOFED).



I gruppi di interfacce non sono supportati con NFS su RDMA.

Cosa succederà

- [Configurare le NIC per NFS su RDMA](#)
- [Configurare LIF per NFS su RDMA](#)
- [Impostazioni NFS per NFS su RDMA](#)

Informazioni correlate

- ["RDMA"](#)
- [Panoramica del trunking NFS](#)
- ["RFC 7530: Protocollo NFS versione 4"](#)
- ["RFC 8166: Remote Direct Memory Access Transport for Remote procedure Call Version 1"](#)
- ["RFC 8167: Chiamata di procedura remota bidirezionale su porte RPC-over-RDMA"](#)
- ["RFC 8267: Associazione di livello superiore NFS a RPC-over-RDMA versione 1"](#)

Configurare le NIC per NFS su RDMA

NFS su RDMA richiede la configurazione NIC sia per il sistema client che per la piattaforma di storage.

Configurazione della piattaforma di storage

Sul server deve essere installato un adattatore RDMA X1148. Se si utilizza una configurazione ha, è necessario disporre di un adattatore X1148 corrispondente sul partner di failover in modo che il servizio RDMA possa continuare durante il failover. La NIC deve essere compatibile con ROCE.

A partire da ONTAP 9.10.1, è possibile visualizzare un elenco di protocolli di offload RDMA con il comando:

```
network port show -rdma-protocols roce
```

Configurazione del sistema client

I client devono utilizzare schede NIC Mellanox RDMA (ad esempio X1148) e il software di rete Mellanox OFED. Consultare la documentazione di Mellanox per i modelli e le versioni supportate. Sebbene sia possibile collegare direttamente client e server, si consiglia di utilizzare gli switch a causa delle migliori prestazioni di failover con uno switch.

Il client, il server e gli switch e tutte le porte sugli switch devono essere configurati utilizzando frame Jumbo. Assicurarsi inoltre che il controllo di flusso prioritario sia attivo su qualsiasi switch.

Una volta confermata la configurazione, è possibile montare NFS.

System Manager

È necessario utilizzare ONTAP 9.12.1 o versione successiva per configurare le interfacce di rete con NFS su RDMA utilizzando Gestione di sistema.

Fasi

1. Controllare se RDMA è supportato. Accedere a **Network > Ethernet Ports** (rete > Porte Ethernet) e selezionare il nodo appropriato nella vista del gruppo. Quando si espande il nodo, osservare il campo **RDMA Protocol** (protocolli RDMA) per una data porta: Il valore **RoCE** indica che RDMA è supportato; un trattino (-) indica che non è supportato.
2. Per aggiungere una VLAN, selezionare **+ VLAN**. Selezionare il nodo appropriato. Nel menu a discesa **Port** (porta), le porte disponibili visualizzano il testo **RoCE Enabled** (abilitato RoCE) se supportano RDMA; se non supportano RDMA, non viene visualizzato alcun testo.
3. Seguire il flusso di lavoro in [Abilitare lo storage NAS per i server Linux utilizzando NFS](#) Per configurare un nuovo server NFS.

Quando si aggiungono interfacce di rete, è possibile selezionare **Usa porte RoCE**. Selezionare questa opzione per tutte le interfacce di rete che si desidera utilizzare NFS su RDMA.

CLI

1. Controllare se l'accesso RDMA è attivato sul server NFS con il comando:

```
vserver nfs show-vserver SVM_name
```

Per impostazione predefinita, `-rdma` deve essere attivato. In caso contrario, abilitare l'accesso RDMA sul server NFS:

```
vserver nfs modify -vserver SVM_name -rdma enabled
```

2. Montare il client tramite NFSv4.0 su RDMA:

- a. L'input per il parametro `proto` dipende dalla versione del protocollo IP del server. Se si tratta di IPv4, utilizzare `proto=rdma`. Se si tratta di IPv6, utilizzare `proto=rdma6`.
- b. Specificare la porta di destinazione NFS come `port=20049` invece della porta standard 2049:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address  
:/volume_path mount_point
```

3. **OPZIONALE:** Se è necessario smontare il client, eseguire il comando `umount mount_path`

Ulteriori informazioni

- [Creare un server NFS](#)
- [Abilitare lo storage NAS per i server Linux utilizzando NFS](#)

Configurare LIF per NFS su RDMA

Per utilizzare NFS su RDMA, è necessario configurare le LIF (interfaccia di rete) in modo che siano compatibili con RDMA. Sia la LIF che la sua coppia di failover devono essere in grado di supportare RDMA.

Creare una nuova LIF

System Manager

Per creare un'interfaccia di rete per NFS su RDMA con Gestione di sistema, è necessario eseguire ONTAP 9.12.1 o versioni successive.

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **+ Add**.
3. Quando si seleziona **NFS,SMB/CIFS,S3**, si avrà la possibilità di **utilizzare porte RoCE**. Selezionare la casella di controllo **Usa porte RoCE**.
4. Selezionare la VM di storage e il nodo home. Assegnare un nome. Inserire l'indirizzo IP e la subnet mask.
5. Una volta immessi l'indirizzo IP e la subnet mask, System Manager filtra l'elenco dei domini di trasmissione in base a quelli che dispongono di porte compatibili con RoCE. Selezionare un dominio di trasmissione. È possibile aggiungere un gateway.
6. Selezionare **Salva**.

CLI

Fasi

1. Creare una LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy service_policy_name -home-node node_name -home-port port_name {-address IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall -policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

- La politica di servizio deve essere predefinita-data-file o una policy personalizzata che includa il servizio di interfaccia di rete Data-nfs.
- Il `-rdma-protocols` parameter accetta un elenco, che per impostazione predefinita è vuoto. Quando `roce` Viene aggiunto come valore, la LIF può essere configurata solo sulle porte che supportano l'offload RoCE, con conseguenze sulla migrazione e il failover di bot LIF.

Modificare una LIF

System Manager

Per creare un'interfaccia di rete per NFS su RDMA con Gestione di sistema, è necessario eseguire ONTAP 9.12.1 o versioni successive.

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **:** > **Modifica** accanto all'interfaccia di rete che si desidera modificare.
3. Selezionare **Use RoCE Ports** (Usa porte RoCE) per attivare NFS su RDMA o deselezionare la casella per disattivarla. Se l'interfaccia di rete si trova su una porta compatibile con RoCE, viene visualizzata una casella di controllo accanto a **Usa porte RoCE**.
4. Modificare le altre impostazioni in base alle necessità.
5. Selezionare **Save** (Salva) per confermare le modifiche.

CLI

1. È possibile controllare lo stato dei file LIF con `network interface show` comando. La politica di servizio deve includere il servizio di interfaccia di rete dati-nfs. Il `-rdma-protocols` l'elenco deve includere `roce`. Se una di queste condizioni non è vera, modificare la LIF.
2. Per modificare la LIF, eseguire:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```



La modifica di una LIF per richiedere un protocollo di offload specifico quando la LIF non è attualmente assegnata a una porta che supporta tale protocollo genera un errore.

Migrare una LIF

ONTAP consente inoltre di migrare le interfacce di rete (LIF) per utilizzare NFS su RDMA. Quando si esegue questa migrazione, è necessario assicurarsi che la porta di destinazione sia compatibile con RoCE. A partire da ONTAP 9.12.1, è possibile completare questa procedura in Gestore di sistema. Quando si seleziona una porta di destinazione per l'interfaccia di rete, System Manager stabilisce se le porte sono compatibili con RoCE.

È possibile migrare una LIF a una configurazione NFS su RDMA solo se:

- Si tratta di un'interfaccia di rete NFS RDMA (LIF) ospitata su una porta compatibile con RoCE.
- Si tratta di un'interfaccia di rete NFS TCP (LIF) ospitata su una porta compatibile con RoCE.
- Si tratta di un'interfaccia di rete NFS TCP (LIF) ospitata su una porta non compatibile con RoCE.

Per ulteriori informazioni sulla migrazione di un'interfaccia di rete, fare riferimento a [Migrare una LIF](#).

Ulteriori informazioni

- [Creare una LIF](#)
- [Creare una LIF](#)

- [Modificare una LIF](#)
- [Migrare una LIF](#)

Modificare la configurazione NFS

Nella maggior parte dei casi, non sarà necessario modificare la configurazione della VM di storage abilitata NFS per NFS su RDMA.

Tuttavia, se si affrontano problemi relativi ai chip Mellanox e alla migrazione LIF, è necessario aumentare il periodo di tolleranza di blocco NFSv4. Per impostazione predefinita, il periodo di tolleranza è impostato su 45 secondi. A partire da ONTAP 9.10.1, il periodo di tolleranza ha un valore massimo di 180 (secondi).

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

Per ulteriori informazioni su questa attività, vedere [Specifica del periodo di tolleranza del blocco NFSv4](#).

Configurare SMB con la CLI

Panoramica della configurazione SMB con la CLI

È possibile utilizzare i comandi CLI di ONTAP 9 per configurare l'accesso del client SMB ai file contenuti in un nuovo volume o qtree in una SVM nuova o esistente.



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 se si desidera configurare l'accesso SMB a un volume o a un qtree nel modo seguente:

- Si desidera utilizzare SMB versione 2 o successiva.
- Si desidera servire solo client SMB, non client NFS (non una configurazione multiprotocollo).
- Per proteggere il nuovo volume verranno utilizzate le autorizzazioni NTFS.
- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

Per creare SVM e LIFF sono necessari i privilegi di amministratore del cluster. I privilegi di amministratore di SVM sono sufficienti per altre attività di configurazione SMB.

- Si desidera utilizzare la CLI, non System Manager o uno strumento di scripting automatico.

Per utilizzare System Manager per configurare l'accesso multiprotocollo NAS, vedere ["Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB"](#).

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.

I dettagli sulla sintassi dei comandi sono disponibili nelle pagine guida CLI e man ONTAP.

Per ulteriori informazioni sulla gamma di funzionalità del protocollo SMB ONTAP, consultare ["Panoramica di riferimento SMB"](#).

Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Fare riferimento a...
System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive)	"Provisioning dello storage NAS per i server Windows utilizzando SMB"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica della configurazione SMB"

Workflow di configurazione SMB

La configurazione di SMB implica la valutazione dei requisiti di storage fisico e di rete, quindi la scelta di un workflow specifico dell'obiettivo, la configurazione dell'accesso SMB a una SVM nuova o esistente o l'aggiunta di un volume o qtree a una SVM esistente già completamente configurata per l'accesso SMB.

Preparazione

Valutare i requisiti di storage fisico

Prima di eseguire il provisioning dello storage SMB per i client, è necessario assicurarsi che vi sia spazio sufficiente in un aggregato esistente per il nuovo volume. In caso contrario, è possibile aggiungere dischi a un aggregato esistente o creare un nuovo aggregato del tipo desiderato.

Fasi

1. Visualizzare lo spazio disponibile negli aggregati esistenti: `storage aggregate show`

Se esiste un aggregato con spazio sufficiente, registrare il nome nel foglio di lavoro.


```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_4	239.0GB	238.9GB	95%	online	5	node3	raid_dp, normal
aggr_5	239.0GB	239.0GB	95%	online	4	node4	raid_dp, normal

6 entries were displayed.

2. Se non sono presenti aggregati con spazio sufficiente, aggiungere dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

Valutare i requisiti di rete

Prima di fornire storage SMB ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning SMB.

Prima di iniziare

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

Fasi

1. Visualizzare le porte fisiche e virtuali disponibili: `network port show`
 - Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
 - Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.
2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti: `network subnet show`

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

3. Visualizzare gli spazi IP disponibili: `network ipspace show`

È possibile utilizzare l'IPSpace predefinito o un IPSpace personalizzato.

4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster: `network options ipv6 show`

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

Decidere dove eseguire il provisioning della nuova capacità di storage per PMI

Prima di creare un nuovo volume o qtree SMB, è necessario decidere se posizionarlo in una SVM nuova o esistente e la quantità di configurazione richiesta da SVM. Questa decisione determina il tuo flusso di lavoro.

Scelte

- Se si desidera eseguire il provisioning di un volume o qtree su una nuova SVM o su una SVM esistente che ha SMB abilitato ma non configurato, completare la procedura descritta in “Configurazione dell'accesso SMB a una SVM” e “aggiunta di capacità di storage a una SVM abilitata per SMB”.

Configurazione dell'accesso SMB a una SVM

Configurazione dell'accesso del client SMB allo storage condiviso

È possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando SMB su un cluster per la prima volta.
- Esistono SVM in un cluster in cui non si desidera abilitare il supporto SMB.
- Si dispone di una o più SVM abilitate per SMB in un cluster e si desidera una delle seguenti connessioni:
 - A una foresta o a un gruppo di lavoro Active Directory diverso.
 - A un server SMB in uno spazio dei nomi isolato (scenario multi-tenancy). È inoltre necessario scegliere questa opzione per eseguire il provisioning dello storage su una SVM esistente con SMB abilitato ma non configurato. Questo potrebbe verificarsi se è stata creata la SVM per l'accesso SAN o se non sono stati attivati protocolli al momento della creazione della SVM.

Dopo aver attivato SMB su SVM, procedere al provisioning di un volume o qtree.

- Se si desidera eseguire il provisioning di un volume o qtree su una SVM esistente completamente configurata per l'accesso SMB, completare la procedura descritta in “aggiunta di capacità di storage a una SVM abilitata per SMB”.

Configurazione dell'accesso del client SMB allo storage condiviso

Foglio di lavoro per la raccolta delle informazioni di configurazione SMB

Il foglio di lavoro di configurazione SMB consente di raccogliere le informazioni necessarie per impostare l'accesso SMB per i client.

È necessario completare una o entrambe le sezioni del foglio di lavoro, a seconda della decisione presa su dove eseguire il provisioning dello storage:

- Se si configura l'accesso SMB a una SVM, completare entrambe le sezioni.

[Configurazione dell'accesso SMB a una SVM](#)

[Configurazione dell'accesso del client SMB allo storage condiviso](#)

- Se si aggiunge capacità di storage a una SVM abilitata per SMB, completare solo la seconda sezione.

[Configurazione dell'accesso del client SMB allo storage condiviso](#)

Le pagine man dei comandi contengono dettagli sui parametri.

Configurazione dell'accesso SMB a una SVM

Parametri per la creazione di una SVM

Questi valori vengono forniti con `vserver create`. Se si sta creando una nuova SVM.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Un nome fornito per la nuova SVM che sia un nome di dominio completo (FQDN) o che segua un'altra convenzione che applica nomi SVM univoci in un cluster.	
<code>-aggregate</code>	Il nome di un aggregato nel cluster con spazio sufficiente per la nuova capacità di storage SMB.	
<code>-rootvolume</code>	Un nome univoco fornito per il volume root SVM.	
<code>-rootvolume-security-style</code>	Utilizzare lo stile di protezione NTFS per SVM.	<code>ntfs</code>
<code>-language</code>	Utilizzare l'impostazione della lingua predefinita in questo flusso di lavoro.	<code>C.UTF-8</code>
<code>ipspace</code>	Opzionale: Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono le SVM.	

Parametri per la creazione di una LIF

Questi valori vengono forniti con `network interface create`. Durante la creazione di LIF.

Campo	Descrizione	Il tuo valore
<code>-lif</code>	Un nome fornito per il nuovo LIF.	
<code>-role</code>	Utilizza il ruolo LIF dei dati in questo flusso di lavoro.	<code>data</code>
<code>-data-protocol</code>	Utilizzare solo il protocollo SMB in questo flusso di lavoro.	<code>cifs</code>
<code>-home-node</code>	Il nodo a cui la LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-home-port</code>	La porta o il gruppo di interfacce a cui LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-address</code>	L'indirizzo IPv4 o IPv6 del cluster che verrà utilizzato per l'accesso ai dati dal nuovo LIF.	
<code>-netmask</code>	La maschera di rete e il gateway per LIF.	
<code>-subnet</code>	Un pool di indirizzi IP. Utilizzato al posto di <code>-address</code> e <code>-netmask</code> per assegnare automaticamente indirizzi e netmask.	
<code>-firewall-policy</code>	Utilizzare la policy predefinita del firewall dati in questo flusso di lavoro.	<code>data</code>
<code>-auto-revert</code>	Facoltativo: Specifica se un LIF dei dati viene automaticamente riportato al nodo principale all'avvio o in altre circostanze. L'impostazione predefinita è <code>false</code> .	

Parametri per la risoluzione del nome host DNS

Questi valori vengono forniti con `vserver services name-service dns create` Durante la configurazione del DNS.

Campo	Descrizione	Il tuo valore
<code>-domains</code>	Fino a cinque nomi di dominio DNS.	
<code>-name-servers</code>	Fino a tre indirizzi IP per ciascun server dei nomi DNS.	

Configurazione di un server SMB in un dominio Active Directory

Parametri per la configurazione del servizio Time

Questi valori vengono forniti con `cluster time-service ntp server create` quando si configurano i servizi orari.

Campo	Descrizione	Il tuo valore
<code>-server</code>	Il nome host o l'indirizzo IP del server NTP per il dominio Active Directory.	

Parametri per la creazione di un server SMB in un dominio Active Directory

Questi valori vengono forniti con `vserver cifs create` Quando si crea un nuovo server SMB e si specificano le informazioni di dominio.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare il server SMB.	
<code>-cifs-server</code>	Il nome del server SMB (fino a 15 caratteri).	
<code>-domain</code>	Il nome di dominio completo (FQDN) del dominio Active Directory da associare al server SMB.	
<code>-ou</code>	Facoltativo: L'unità organizzativa all'interno del dominio Active Directory da associare al server SMB. Per impostazione predefinita, questo parametro è impostato su CN=computer.	
<code>-netbios-aliases</code>	Facoltativo: Un elenco di alias NetBIOS, che sono nomi alternativi al nome del server SMB.	

Campo	Descrizione	Il tuo valore
<code>-comment</code>	Facoltativo: Un commento di testo per il server. I client Windows possono visualizzare questa descrizione del server SMB quando esplorano i server della rete.	

Configurazione di un server SMB in un gruppo di lavoro

Parametri per la creazione di un server SMB in un gruppo di lavoro

Questi valori vengono forniti con `vserver cifs create` Quando si crea un nuovo server SMB e si specificano le versioni SMB supportate.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare il server SMB.	
<code>-cifs-server</code>	Il nome del server SMB (fino a 15 caratteri).	
<code>-workgroup</code>	Il nome del gruppo di lavoro (fino a 15 caratteri).	
<code>-comment</code>	Facoltativo: Un commento di testo per il server. I client Windows possono visualizzare questa descrizione del server SMB quando esplorano i server della rete.	

Parametri per la creazione di utenti locali

Questi valori vengono forniti quando si creano utenti locali utilizzando `vserver cifs users-and-groups local-user create` comando. Sono richiesti per i server SMB nei gruppi di lavoro e opzionali nei domini ad.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare l'utente locale.	
<code>-user-name</code>	Il nome dell'utente locale (fino a 20 caratteri).	

Campo	Descrizione	Il tuo valore
-full-name	Facoltativo: Il nome completo dell'utente. Se il nome completo contiene uno spazio, racchiudere il nome completo tra virgolette doppie.	
-description	Facoltativo: Una descrizione per l'utente locale. Se la descrizione contiene uno spazio, racchiudere il parametro tra virgolette.	
-is-account-disabled	Facoltativo: Consente di specificare se l'account utente è attivato o disattivato. Se questo parametro non viene specificato, l'impostazione predefinita prevede l'attivazione dell'account utente.	

Parametri per la creazione di gruppi locali

Questi valori vengono forniti quando si creano gruppi locali utilizzando `vserver cifs users-and-groups local-group create` comando. Sono opzionali per i server SMB nei domini e nei gruppi di lavoro ad.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare il gruppo locale.	
-group-name	Il nome del gruppo locale (fino a 256 caratteri).	
-description	Facoltativo: Una descrizione per il gruppo locale. Se la descrizione contiene uno spazio, racchiudere il parametro tra virgolette.	

Aggiunta di capacità di storage a una SVM abilitata per SMB

Parametri per la creazione di un volume

Questi valori vengono forniti con `volume create` se si sta creando un volume invece di un qtree.

Campo	Descrizione	Il tuo valore
-vserver	Il nome di una SVM nuova o esistente che ospiterà il nuovo volume.	

Campo	Descrizione	Il tuo valore
-volume	Un nome descrittivo univoco fornito per il nuovo volume.	
-aggregate	Il nome di un aggregato nel cluster con spazio sufficiente per il nuovo volume SMB.	
-size	Un numero intero fornito per le dimensioni del nuovo volume.	
-security-style	USA lo stile di sicurezza NTFS per questo flusso di lavoro.	ntfs
-junction-path	Posizione sotto root (/) dove deve essere montato il nuovo volume.	

Parametri per la creazione di un qtree

Questi valori vengono forniti con `volume qtree create` se si sta creando un qtree invece di un volume.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui risiede il volume contenente il qtree.	
-volume	Il nome del volume che conterrà il nuovo qtree.	
-qtree	Un nome descrittivo univoco fornito per il nuovo qtree, massimo 64 caratteri.	
-qtree-path	L'argomento del percorso qtree nel formato <code>/vol/volume_name/qtree_name\></code> può essere specificato invece di specificare volume e qtree come argomenti separati.	

Parametri per la creazione di condivisioni SMB

Questi valori vengono forniti con `vserver cifs share create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare la condivisione SMB.	

Campo	Descrizione	Il tuo valore
-share-name	Il nome della condivisione SMB che si desidera creare (fino a 256 caratteri).	
-path	Il nome del percorso della condivisione SMB (fino a 256 caratteri). Questo percorso deve esistere in un volume prima di creare la condivisione.	
-share-properties	Facoltativo: Un elenco delle proprietà di condivisione. Le impostazioni predefinite sono oplocks, browsable, changenotify, e. show-previous-versions.	
-comment	Facoltativo: Un commento di testo per il server (fino a 256 caratteri). I client Windows possono visualizzare questa descrizione della condivisione SMB durante la navigazione in rete.	

Parametri per la creazione di elenchi di controllo degli accessi di condivisione SMB (ACL)

Questi valori vengono forniti con `vserver cifs share access-control create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare l'ACL SMB.	
-share	Il nome della condivisione SMB su cui creare.	
-user-group-type	Il tipo di utente o gruppo da aggiungere all'ACL della condivisione. Il tipo predefinito è windows	windows
-user-or-group	L'utente o il gruppo da aggiungere all'ACL della condivisione. Se si specifica il nome utente, è necessario includere il dominio dell'utente nel formato "domain\ nomeutente".	

Campo	Descrizione	Il tuo valore
-permission	Specifica le autorizzazioni per l'utente o il gruppo.	`[No_access
Read	Change	Full_Control]`

Configurare l'accesso SMB a una SVM

Configurare l'accesso SMB a una SVM

Se non si dispone già di una SVM configurata per l'accesso al client SMB, è necessario creare e configurare una nuova SVM o configurare una SVM esistente. La configurazione di SMB implica l'apertura dell'accesso al volume root SVM, la creazione di un server SMB, la creazione di una LIF, l'abilitazione della risoluzione dei nomi host, la configurazione dei servizi dei nomi e, se lo si desidera, Attivazione della sicurezza Kerberos.

Creare una SVM

Se non si dispone già di almeno una SVM in un cluster per fornire l'accesso ai dati ai client SMB, è necessario crearne una.

Prima di iniziare

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

Fasi

1. Creare una SVM: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
 - Utilizzare l'impostazione NTFS per `-rootvolume-security-style` opzione.
 - Utilizzare il C.UTF-8 predefinito `-language` opzione.
 - Il `ipspace` l'impostazione è facoltativa.

2. Verificare la configurazione e lo stato della SVM appena creata: `vserver show -vserver vserver_name`

Il Allowed Protocols Il campo deve includere CIFS. È possibile modificare questo elenco in un secondo momento.

Il Vserver Operational State il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPspace `ipspaceA`:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione.

```
cluster1::> vservers show -vservers vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

Verificare che il protocollo SMB sia attivato su SVM

Prima di poter configurare e utilizzare SMB su SVM, è necessario verificare che il

protocollo sia attivato.

A proposito di questa attività

Questa operazione viene generalmente eseguita durante l'installazione di SVM, ma se il protocollo non è stato attivato durante l'installazione, è possibile attivarlo in un secondo momento utilizzando `vserver add-protocols` comando.



Una volta creato, non è possibile aggiungere o rimuovere un protocollo da un LIF.

È inoltre possibile disattivare i protocolli sulle SVM utilizzando `vserver remove-protocols` comando.

Fasi

1. Controllare quali protocolli sono attualmente attivati e disattivati per SVM: `vserver show -vserver vserver_name -protocols`

È inoltre possibile utilizzare `vserver show-protocols` Per visualizzare i protocolli attualmente abilitati su tutte le SVM nel cluster.

2. Se necessario, attivare o disattivare un protocollo:

- Per attivare il protocollo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
- Per disattivare un protocollo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Verificare che i protocolli attivati e disattivati siano stati aggiornati correttamente: `vserver show -vserver vserver_name -protocols`

Esempio

Il seguente comando visualizza i protocolli attualmente attivati e disattivati (consentiti e non consentiti) sulla SVM denominata vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                        nfs, fcp, iscsi, ndmp
```

Il seguente comando consente l'accesso tramite SMB aggiungendo `cifs` All'elenco dei protocolli abilitati sulla SVM denominato vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Aprire la policy di esportazione del volume root SVM

Il criterio di esportazione predefinito del volume root SVM deve includere una regola per consentire a tutti i client l'accesso aperto tramite SMB. Senza tale regola, a tutti i client SMB viene negato l'accesso a SVM e ai relativi volumi.

A proposito di questa attività

Quando viene creata una nuova SVM, viene creata automaticamente una policy di esportazione predefinita (chiamata predefinita) per il volume root della SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM.

Verificare che tutti gli accessi SMB siano aperti nel criterio di esportazione predefinito e, in seguito, limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per singoli volumi o qtree.

Fasi

1. Se si utilizza una SVM esistente, controllare il criterio di esportazione del volume root predefinito: `vserver export-policy rule show`

L'output del comando dovrebbe essere simile a quanto segue:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                                Policy Name: default
                                Rule Index: 1
                                Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                                Superuser Security Types: any
                                Honor SetUID Bits in SETATTR: true
                                Allow Creation of Devices: true
```

Se esiste una regola di questo tipo che consente l'accesso aperto, questa attività è completa. In caso contrario, passare alla fase successiva.

2. Creare una regola di esportazione per il volume root SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verificare la creazione della regola utilizzando `vserver export-policy rule show` comando.

Risultati

Qualsiasi client SMB può ora accedere a qualsiasi volume o qtree creato su SVM.

Creare una LIF

LIF è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore `up` stato.

- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

Fasi

1. Creare una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

ONTAP 9.5 e versioni precedenti

```
`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node
node_name -home-port port_name {-address IP_address -netmask IP_address
-subnet-name subnet_name} -firewall-policy data -auto-revert {true
false}`
```

ONTAP 9.6 e versioni successive

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home
-node node_name -home-port port_name {-address IP_address -netmask IP_address
-subnet-name subnet_name} -firewall-policy data -auto-revert {true
false}`
```

- Il `-role` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6).
- Il `-data-protocol` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6). Quando si utilizza ONTAP 9,5 e versioni precedenti, il `-data-protocol` Il parametro deve essere specificato al momento della creazione della LIF e non può essere modificato in seguito senza distruggere e ricreare la LIF dei dati.

- `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- `-home-port` È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.

2. Verificare che la LIF sia stata creata correttamente:

```
network interface show
```

3. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e. `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data  
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145  
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data  
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name  
client1_sub -firewall-policy data -auto-revert true
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF datalif1 e datalif3 sono configurati con indirizzi IPv4 e datalif4 è configurato con un indirizzo IPv6:


```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
true					
node-1					
clus1	up/up	192.0.2.12/24	node-1	e0a	
true					
clus2	up/up	192.0.2.13/24	node-1	e0b	
true					
mgmt1	up/up	192.0.2.68/24	node-1	e1a	
true					
node-2					
clus1	up/up	192.0.2.14/24	node-2	e0a	
true					
clus2	up/up	192.0.2.15/24	node-2	e0b	
true					
mgmt1	up/up	192.0.2.69/24	node-2	e1a	
true					
vs1.example.com					
datalif1	up/down	192.0.2.145/30	node-1	e1c	
true					
vs3.example.com					
datalif3	up/up	192.0.2.146/30	node-2	e0c	
true					
datalif4	up/up	2001::2/64	node-2	e0c	
true					

5 entries were displayed.

Il comando seguente mostra come creare una LIF dati NAS assegnata a default-data-files politica di servizio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

Abilitare il DNS per la risoluzione del nome host

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host

vengono risolti utilizzando server DNS esterni.

Prima di iniziare

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

A proposito di questa attività

La *Guida alla gestione della rete* contiene informazioni sulla configurazione del DNS dinamico sulla SVM.

Fasi

1. Abilitare il DNS sulla SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partire da ONTAP 9.2, la `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

2. Visualizzare le configurazioni del dominio DNS utilizzando `vserver services name-service dns show` comando. ``

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
```

			Name
Vserver	State	Domains	Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check` comando.

Il `vserver services name-service dns check` Il comando è disponibile a partire da ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
-----	-----	-----	
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Configurare un server SMB in un dominio Active Directory

Configurare i servizi di gestione dell'orario

Prima di creare un server SMB in un controller di dominio attivo, è necessario assicurarsi che il tempo del cluster e quello dei controller di dominio del dominio a cui il server SMB appartiene corrispondano entro cinque minuti.

A proposito di questa attività

È necessario configurare i servizi NTP del cluster in modo che utilizzino gli stessi server NTP per la sincronizzazione dell'ora utilizzati dal dominio Active Directory.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

Fasi

1. Configurare i servizi di gestione del tempo utilizzando `cluster time-service ntp server create` comando.
 - Per configurare i servizi temporali senza autenticazione simmetrica, immettere il seguente comando:
`cluster time-service ntp server create -server server_ip_address`
 - Per configurare i servizi temporali con autenticazione simmetrica, immettere il seguente comando:
`cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`


2. Verificare che i servizi di orario siano impostati correttamente utilizzando `cluster time-service ntp server show` comando.


```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

Comandi per la gestione dell'autenticazione simmetrica sui server NTP

A partire da ONTAP 9.5, è supportato il protocollo NTP (Network Time Protocol) versione 3. NTPv3 include l'autenticazione simmetrica utilizzando chiavi SHA-1 che aumenta la sicurezza della rete.

A tal fine...	Utilizzare questo comando...
Configurare un server NTP senza autenticazione simmetrica	<code>cluster time-service ntp server create -server server_name</code>
Configurare un server NTP con autenticazione simmetrica	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Abilitare l'autenticazione simmetrica per un server NTP esistente. È possibile modificare il server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configurare una chiave NTP condivisa	<div><code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code></div> <div> Le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP</div>
Configurare un server NTP con un ID chiave sconosciuto	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>

A tal fine...	Utilizzare questo comando...
Configurare un server con un ID chiave non configurato sul server NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>L'ID, il tipo e il valore della chiave devono essere identici all'ID, al tipo e al valore della chiave configurati sul server NTP.</p> </div>
Disattiva autenticazione simmetrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Creare un server SMB in un dominio Active Directory

È possibile utilizzare `vserver cifs create` Per creare un server SMB su SVM e specificare il dominio Active Directory (ad) a cui appartiene.

Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM e a un domain controller ad del dominio a cui si desidera accedere al server SMB.

Qualsiasi utente autorizzato a creare account di computer nel dominio ad a cui si sta entrando nel server SMB può creare il server SMB su SVM. Questo può includere utenti di altri domini.

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.

A proposito di questa attività

Quando si crea un server SMB in un dominio di Activity Directory:

- Quando si specifica il dominio, è necessario utilizzare il nome di dominio completo (FQDN).
- L'impostazione predefinita prevede l'aggiunta dell'account della macchina server SMB all'oggetto CN=computer di Active Directory.
- È possibile scegliere di aggiungere il server SMB a un'unità organizzativa (OU) diversa utilizzando `-ou` opzione.
- È possibile scegliere di aggiungere un elenco delimitato da virgole di uno o più alias NetBIOS (fino a 200) per il server SMB.

La configurazione degli alias NetBIOS per un server SMB può essere utile quando si consolidano i dati da altri file server al server SMB e si desidera che il server SMB risponda ai nomi dei server originali.

Il `vserver cifs` le pagine man contengono ulteriori parametri opzionali e requisiti di denominazione.



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

A partire da ONTAP 9.8, è possibile specificare che le connessioni ai controller di dominio siano crittografate. ONTAP richiede la crittografia per le comunicazioni del controller di dominio 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. .

"[Gestione delle PMI](#)" Contiene ulteriori informazioni sulle opzioni di configurazione del server SMB.

Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

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.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un dominio ad: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Quando si entra in un dominio, il completamento di questo comando potrebbe richiedere alcuni minuti.

Il seguente comando crea il server SMB "smb_server01" nel dominio "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

Il seguente comando crea il server SMB "smb_server02" nel dominio "mydomain.com" e autentica l'amministratore ONTAP con un file keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

In questo esempio, l'output del comando mostra che un server SMB denominato "SMB_SERVER01" è stato creato su SVM vs1.example.com ed è stato Unito al dominio "example.com".

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

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
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: -
```

4. Se lo si desidera, attivare la comunicazione crittografata con il controller di dominio (ONTAP 9.8 e versioni successive): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

Esempi

Il seguente comando crea un server SMB denominato “smb_server02” su SVM vs2.example.com nel dominio “example.com”. L’account del computer viene creato nel contenitore “OU=eng,OU=corp,DC=example,DC=com”. Al server SMB viene assegnato un alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
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: OLD_CIFS_SERVER01
```

Il seguente comando consente a un utente di un dominio diverso, in questo caso un amministratore di un dominio attendibile, di creare un server SMB denominato “smb_server03” su SVM vs3.example.com. Il `-domain` Option specifica il nome del dominio principale (specificato nella configurazione DNS) in cui si desidera creare il server SMB. Il `username` consente di specificare l’amministratore del dominio attendibile.

- Dominio domestico: example.com
- Dominio attendibile: trust.lab.com
- Nome utente del dominio trusted: Administrator1

```
cluster1::> vsync cifs create -vsync vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
```

```
Password: . . .
```

Creare file keytab per l'autenticazione SMB

A partire da ONTAP 9.7, ONTAP supporta l'autenticazione SVM con server Active Directory (ad) utilizzando file keytab. Gli amministratori DEGLI ANNUNCI generano un file keytab e lo rendono disponibile agli amministratori di ONTAP come URI (Uniform Resource Identifier), che viene fornito quando `vsync cifs` I comandi richiedono l'autenticazione Kerberos con il dominio ad.

Gli amministratori DEGLI ANNUNCI possono creare i file keytab utilizzando Windows Server standard `ktpass` comando. Il comando deve essere eseguito sul dominio primario in cui è richiesta l'autenticazione. Il `ktpass` il comando può essere utilizzato per generare i file keytab solo per gli utenti del dominio primario; le chiavi generate utilizzando gli utenti del dominio trusted non sono supportate.

I file keytab vengono generati per specifici utenti amministratori di ONTAP. Se la password dell'utente amministratore non viene modificata, le chiavi generate per il tipo di crittografia e il dominio specifico non verranno modificate. Pertanto, è necessario un nuovo file keytab ogni volta che viene modificata la password dell'utente amministratore.

Sono supportati i seguenti tipi di crittografia:

- AES256-SHA1
- DES-CBC-MD5



ONTAP non supporta il tipo di crittografia DES-CBC-CRC.

- RC4-HMAC

AES256 è il tipo di crittografia più elevato e deve essere utilizzato se abilitato sul sistema ONTAP.

I file keytab possono essere generati specificando la password admin o utilizzando una password generata casualmente. Tuttavia, in qualsiasi momento è possibile utilizzare una sola opzione di password, poiché sul server ad è necessaria una chiave privata specifica per l'utente amministratore per decifrare le chiavi all'interno del file keytab. Qualsiasi modifica della chiave privata per un amministratore specifico invaliderà il file keytab.

Configurare un server SMB in un gruppo di lavoro

Configurare un server SMB in una panoramica del gruppo di lavoro

L'impostazione di un server SMB come membro di un gruppo di lavoro consiste nella creazione del server SMB e quindi nella creazione di utenti e gruppi locali.

È possibile configurare un server SMB in un gruppo di lavoro quando l'infrastruttura di dominio Microsoft Active Directory non è disponibile.

Un server SMB in modalità workgroup supporta solo l'autenticazione NTLM e non l'autenticazione Kerberos.

Creare un server SMB in un gruppo di lavoro

È possibile utilizzare `vserver cifs create` Per creare un server SMB sulla SVM e specificare il gruppo di lavoro a cui appartiene.

Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM.

A proposito di questa attività

I server SMB in modalità workgroup non supportano le seguenti funzionalità SMB:

- Protocollo di controllo SMB3
- Condivisioni SMB3 CA
- SQL su SMB
- Reindirizzamento cartelle
- Profili roaming
- Oggetto Criteri di gruppo (GPO)
- Servizio Volume Snapshot (VSS)

Il `vserver cifs` le pagine man contengono ulteriori parametri di configurazione opzionali e requisiti di denominazione.

Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

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.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un gruppo di lavoro: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

Il seguente comando crea il server SMB "smb_server01" nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
SMB_SERVER01 -workgroup workgroup01
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

Nell'esempio seguente, l'output del comando mostra che un server SMB denominato "smb_server01" è stato creato su SVM vs1.example.com nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

Al termine

Per un server CIFS in un gruppo di lavoro, è necessario creare utenti locali e, facoltativamente, gruppi locali su SVM.

Informazioni correlate

["Gestione delle PMI"](#)

Creare account utente locali

È possibile creare un account utente locale da utilizzare per autorizzare l'accesso ai dati contenuti nella SVM tramite una connessione SMB. È inoltre possibile utilizzare account utente locali per l'autenticazione quando si crea una sessione SMB.

A proposito di questa attività

La funzionalità utente locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un account utente locale, è necessario specificare un nome utente e la SVM a cui associare l'account.

Il `vserver cifs users-and-groups local-user` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

Fasi

1. Creare l'utente locale: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Potrebbero essere utili i seguenti parametri opzionali:

- `-full-name`

Il nome completo dell'utente.

- `-description`

Una descrizione per l'utente locale.

◦ `-is-account-disabled {true|false}`

Specifica se l'account utente è attivato o disattivato. Se questo parametro non viene specificato, l'impostazione predefinita prevede l'attivazione dell'account utente.

Il comando richiede la password dell'utente locale.

2. Immettere una password per l'utente locale, quindi confermarla.
3. Verificare che l'utente sia stato creato correttamente: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Esempio

Nell'esempio seguente viene creato un utente locale "SMB_SERVER01 `Ssue", con il nome completo "ue Chang", associato a SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator    Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

Creare gruppi locali

È possibile creare gruppi locali che possono essere utilizzati per autorizzare l'accesso ai dati associati alla SVM tramite una connessione SMB. È inoltre possibile assegnare privilegi che definiscono i diritti o le funzionalità di un membro del gruppo.

A proposito di questa attività

La funzionalità del gruppo locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un gruppo locale, è necessario specificare un nome per il gruppo e la SVM a cui associare il gruppo. È possibile specificare un nome di gruppo con o senza il nome di dominio locale ed è possibile specificare una descrizione per il gruppo locale. Non è possibile aggiungere un gruppo locale a un altro gruppo locale.

Il `vserver cifs users-and-groups local-group` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

Fasi

1. Creare il gruppo locale: `vserver cifs users-and-groups local-group create -vserver`

```
vserver_name -group-name group_name
```

Potrebbe essere utile il seguente parametro opzionale:

- ° -description

Una descrizione per il gruppo locale.

2. Verificare che il gruppo sia stato creato correttamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Esempio

Nell'esempio seguente viene creato un gruppo locale "SMB_SERVER01\engineering" associato a SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver  
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver  
vs1.example.com
```

Vserver	Group Name	Description
-----	-----	-----
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
group		
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
		privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

Al termine

È necessario aggiungere membri al nuovo gruppo.

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

Se non si desidera più che un utente locale, un utente di dominio o un gruppo di dominio disponga di diritti di accesso o privilegi in base all'appartenenza a un gruppo, è possibile rimuovere il membro dal gruppo.

Quando si aggiungono membri a un gruppo locale, è necessario tenere presente quanto segue:

- Non è possibile aggiungere utenti al gruppo speciale *Everyone*.

- 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, ONTAP deve essere in grado di risolvere il nome in un SID.

Quando rimuovi membri da un gruppo locale, devi tenere presente quanto segue:

- Non puoi rimuovere membri dal gruppo speciale *Everyone*.
- Per rimuovere un membro da un gruppo locale, ONTAP deve essere in grado di risolvere il proprio nome in un SID.

Fasi

1. Aggiungere o rimuovere un membro da un gruppo.

- Aggiungere un membro: `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: `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.

Esempi

Nell'esempio seguente viene aggiunto un utente locale "SMB_SERVER01\ sue" al gruppo locale "SMB_SERVER01 engineering" su SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Nell'esempio seguente vengono rimossi gli utenti locali "SMB_SERVER01\ sue" e "SMB_SERVER01 \Sjames" dal gruppo locale "SMB_SERVER01 Engineering" su SVM vs1.example.com:

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

Verificare le versioni SMB abilitate

La release di ONTAP 9 determina quali versioni SMB sono abilitate per impostazione predefinita per le connessioni con client e controller di dominio. Verificare che il server SMB supporti i client e le funzionalità richieste nell'ambiente.

A proposito di questa attività

Per le connessioni con client e controller di dominio, è necessario attivare SMB 2.0 e versioni successive, se

possibile. Per motivi di sicurezza, è consigliabile evitare di utilizzare SMB 1.0 e disattivarlo se si è verificato che non è richiesto nell'ambiente in uso.

In ONTAP 9, le versioni SMB 2.0 e successive sono attivate per impostazione predefinita per le connessioni client, ma la versione di SMB 1.0 attivata per impostazione predefinita dipende dalla versione di ONTAP in uso.

- A partire da ONTAP 9.1 P8, SMB 1.0 può essere disattivato sulle SVM.

Il `-smb1-enabled` al `vserver cifs options modify` Il comando attiva o disattiva SMB 1.0.

- A partire da ONTAP 9.3, viene disattivato per impostazione predefinita sui nuovi SVM.

Se il server SMB si trova in un dominio Active Directory (ad), è possibile abilitare SMB 2.0 per la connessione a un controller di dominio (DC) che inizia con ONTAP 9.1. Questa operazione è necessaria se SMB 1.0 è stato disattivato sui controller di dominio. A partire da ONTAP 9.2, SMB 2.0 è attivato per impostazione predefinita per le connessioni DC.



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.

"Gestione delle PMI" Contiene dettagli sulle versioni e sulle funzionalità SMB supportate.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare quali versioni SMB sono abilitate:

```
vserver cifs options show
```

È possibile scorrere l'elenco per visualizzare le versioni SMB abilitate per le connessioni client e, se si configura un server SMB in un dominio ad, per le connessioni di dominio ad.

3. Attivare o disattivare il protocollo SMB per le connessioni client secondo necessità:

- Per attivare una versione SMB:

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- Per disattivare una versione SMB:

```
vserver cifs options modify -vserver vserver_name smb_version false
```

Valori possibili per `smb_version`:

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

Il seguente comando abilita SMB 3.1 su SVM vs1.example.com:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. Se il server SMB si trova in un dominio Active Directory, attivare o disattivare il protocollo SMB per le connessioni DC come richiesto:

- Per attivare una versione SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- Per disattivare una versione SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Mappare il server SMB sul server DNS

Il server DNS del sito deve avere una voce che punta il nome del server SMB e qualsiasi alias NetBIOS all'indirizzo IP del LIF dei dati, in modo che gli utenti Windows possano mappare un disco al nome del server SMB.

Prima di iniziare

È necessario disporre dell'accesso amministrativo al server DNS del sito. Se non si dispone dell'accesso amministrativo, è necessario chiedere all'amministratore DNS di eseguire questa attività.

A proposito di questa attività

Se si utilizzano alias NetBIOS per il nome del server SMB, si consiglia di creare punti di ingresso del server DNS per ciascun alias.

Fasi

1. Accedere al server DNS.

2. Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dei dati LIF.
3. Se si utilizzano alias NetBIOS, creare una voce di ricerca Alias Canonical name (CNAME resource record) per mappare ciascun alias all'indirizzo IP dei dati LIF del server SMB.

Risultati

Una volta propagata la mappatura in rete, gli utenti di Windows possono mappare un disco al nome del server SMB o ai relativi alias NetBIOS.

Configurare l'accesso del client SMB allo storage condiviso

Configurare l'accesso del client SMB allo storage condiviso

Per fornire l'accesso del client SMB allo storage condiviso su una SVM, è necessario creare un volume o un qtree per fornire un container di storage, quindi creare o modificare una condivisione per tale container. È quindi possibile configurare le autorizzazioni di condivisione e file e verificare l'accesso dai sistemi client.

Prima di iniziare

- SMB deve essere completamente configurato sulla SVM.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completi.
- Eventuali aggiunte o modifiche a un dominio Active Directory o alla configurazione del gruppo di lavoro devono essere completate.

Creare un volume o un contenitore di storage qtree

Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

Prima di iniziare

- SMB deve essere configurato e funzionante.
- Lo stile di sicurezza SVM deve essere NTFS.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

Fasi

1. Creare il volume con un punto di giunzione: `volume create -vserver svm_name -volume`


```
volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]}  
-security-style ntfs -junction-path junction_path]
```

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto root, ad esempio `/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

- In una directory esistente, ad esempio `/existing_dir/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

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

Esempi

Il seguente comando crea un nuovo volume denominato `users1` su SVM `vs1.example.com` e sull'aggregato `aggr1`. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users  
-aggregate aggr1 -size 750g -junction-path /users  
[Job 1642] Job succeeded: Successful
```



```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory `/eng/` Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo `/eng/home`, che diventa la home directory di `/eng/` namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando volume qtree create comando.

Prima di iniziare

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere NTFS e SMB deve essere configurato e in esecuzione.

Fasi

1. Creare il qtree: volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs

È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato /vol/volume_name/_qtree_name.

2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato: volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }

Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style ntfs  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: ntfs  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

Requisiti e considerazioni per la creazione di una condivisione SMB

Prima di creare una condivisione SMB, è necessario comprendere i requisiti per i percorsi di condivisione e le proprietà di condivisione, in particolare per le home directory.

La creazione di una condivisione SMB richiede la specifica di una struttura di percorso di directory (utilizzando l' `-path` in `vserver cifs share create` a cui accederanno i client. Il percorso della directory corrisponde al percorso di giunzione di un volume o qtree creato nello spazio dei nomi SVM. Il percorso di directory e il percorso di giunzione corrispondente devono esistere prima di creare la condivisione.

I percorsi di condivisione hanno i seguenti requisiti:

- Il nome di un percorso di directory può contenere fino a 255 caratteri.
- Se nel nome del percorso è presente uno spazio, l'intera stringa deve essere inserita tra virgolette (ad esempio, `"/new volume/mount here"`).
- Se il percorso UNC (`\\servername\sharename\filepath`) Della condivisione contiene più di 256 caratteri (escludendo l'iniziale `""` nel percorso UNC), quindi 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.

È possibile modificare le impostazioni predefinite della proprietà di condivisione:

- Le proprietà iniziali predefinite per tutte le condivisioni sono `oplocks`, `browsable`, `changenotify`, e `show-previous-versions`.
- È facoltativo specificare le proprietà di condivisione quando si crea una condivisione.

Tuttavia, se si specificano le proprietà di condivisione quando si crea la condivisione, le impostazioni predefinite non vengono utilizzate. Se si utilizza `-share-properties` parametro quando si crea una condivisione, è necessario specificare tutte le proprietà della condivisione che si desidera applicare alla condivisione utilizzando un elenco delimitato da virgole.

- Per designare una condivisione della home directory, utilizzare `homedirectory` proprietà.

Questa funzione consente di configurare una condivisione mappata a diverse directory in base all'utente che si connette ad essa e a una serie di variabili. Invece di dover creare condivisioni separate per ciascun utente, è possibile configurare una singola condivisione con alcuni parametri della home directory per definire la relazione di un utente tra un punto di ingresso (la condivisione) e la propria home directory (una directory sulla SVM).



Non è possibile aggiungere o rimuovere questa proprietà dopo aver creato la condivisione.

Le condivisioni home directory hanno i seguenti requisiti:

- Prima di creare le home directory SMB, è necessario aggiungere almeno un percorso di ricerca della home directory utilizzando `vserver cifs home-directory search-path add` comando.
- Condivisioni home directory specificate dal valore di `homedirectory` su `-share-properties` il parametro deve includere `%w` (Nome utente Windows) variabile dinamica nel nome della condivisione.

Il nome della condivisione può contenere anche `%d` (nome di dominio) variabile dinamica (ad esempio, `%d/%w`) o una parte statica nel nome della condivisione (ad esempio, `home1_%w`).

- Se la condivisione viene utilizzata da amministratori o utenti per connettersi alle home directory di altri utenti (utilizzando le opzioni di `vserver cifs home-directory modify` comando), il modello di nome di condivisione dinamica deve essere preceduto da una tilde (`~`).

"Gestione delle PMI" e `vserver cifs share` le pagine man contengono informazioni aggiuntive.

Creare una condivisione SMB

È necessario creare una condivisione SMB prima di poter condividere i dati da un server SMB con client SMB. Quando si crea una condivisione, è possibile impostare le proprietà della condivisione, ad esempio designarla come home directory. È inoltre possibile personalizzare la condivisione configurando le impostazioni opzionali.

Prima di iniziare

Il percorso della directory per il volume o qtree deve esistere nello spazio dei nomi SVM prima di creare la condivisione.

A proposito di questa attività

Quando si crea una condivisione, l'ACL di condivisione predefinito (autorizzazioni di condivisione predefinite) è `Everyone / Full Control`. Dopo aver testato l'accesso alla condivisione, rimuovere l'ACL della condivisione predefinita e sostituirlo con un'alternativa più sicura.

Fasi

1. Se necessario, creare la struttura del percorso di directory per la condivisione.

Il `vserver cifs share create` il comando verifica il percorso specificato in `-path` durante la

creazione della condivisione. Se il percorso specificato non esiste, il comando non riesce.

2. Creare una condivisione SMB associata alla SVM specificata:
`vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verificare che la condivisione sia stata creata:
`vserver cifs share show -share-name share_name`

Esempi

Il seguente comando crea una condivisione SMB denominata “SHARE1” su SVM `vs1.example.com`. Il percorso della directory è `/users` e viene creato con le proprietà predefinite.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

Verificare l'accesso al client SMB

Verificare di aver configurato SMB correttamente accedendo e scrivendo i dati nella condivisione. Verificare l'accesso utilizzando il nome del server SMB e gli alias NetBIOS.

Fasi

1. Accedere a un client Windows.
2. Verificare l'accesso utilizzando il nome del server SMB:
 - a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato: `\\SMB_Server_Name\Share_Name`

Se la mappatura non riesce, è possibile che la mappatura DNS non sia ancora propagata in tutta la rete. È necessario verificare l'accesso utilizzando il nome del server SMB in un secondo momento.

Se il server SMB è denominato `vs1.example.com` e la condivisione è denominata `SHARE1`, immettere quanto segue: `\\vs0.example.com\SHARE1`

- b. Sul disco appena creato, creare un file di prova, quindi eliminare il file.

L'accesso in scrittura alla condivisione è stato verificato utilizzando il nome del server SMB.

3. Ripetere il passaggio 2 per tutti gli alias NetBIOS.

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.

Prima di iniziare

È necessario decidere quali utenti o gruppi avranno accesso alla condivisione.

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.

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 di condivisione predefinito:
`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	<code>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</code>
Gruppo di Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>

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

Esempio

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

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

cluster1::> vsserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

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

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

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

cluster1::> vsserver cifs share access-control show -vsserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

Configurare le autorizzazioni per i file NTFS in una condivisione

Per consentire l'accesso ai file agli utenti o ai gruppi che hanno accesso a una condivisione, è necessario configurare le autorizzazioni dei file NTFS su file e directory in tale condivisione da un client 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

"[Gestione delle PMI](#)" La documentazione di Windows contiene informazioni su come impostare le autorizzazioni NTFS standard e avanzate.

Fasi

1. Accedere a un client Windows come amministratore.
2. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
3. Completare la casella **Map Network Drive** (Connetti unità di rete):
 - a. Selezionare una lettera **Drive**.
 - b. Nella casella **Folder** (cartella), digitare il nome del server SMB contenente la condivisione contenente i dati a cui si desidera applicare le autorizzazioni e il nome della condivisione.

Se il nome del server SMB è SMB_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB_SERVER01\SHARE1.



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

- 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.

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

La scheda Security (sicurezza) visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella Permissions for <Object> (autorizzazioni per utenti) visualizza un elenco di permessi e permessi di negazione in vigore per l'utente o il gruppo selezionato.

7. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra Permissions for <Object> (autorizzazioni per l'accesso)

8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni...
Impostare le autorizzazioni NTFS standard per un nuovo utente o gruppo	<p>a. Fare clic su Aggiungi.</p> <p>Viene visualizzata la finestra Seleziona utente, computer, account di servizio o gruppi.</p> <p>b. Nella casella inserire i nomi degli oggetti da selezionare, digitare il nome dell'utente o del gruppo a cui si desidera aggiungere l'autorizzazione NTFS.</p> <p>c. Fare clic su OK.</p>
Modificare o rimuovere le autorizzazioni NTFS standard da un utente o gruppo	Nella casella nomi gruppo o utente , selezionare l'utente o il gruppo che si desidera modificare o rimuovere.

9. Eseguire le azioni desiderate:

Se si desidera...	Effettuare le seguenti operazioni
Impostare le autorizzazioni NTFS standard per un utente o un gruppo nuovo o esistente	Nella casella Permissions for <Object> (autorizzazioni per l'accesso), selezionare le caselle Allow (Consenti) o Nega per il tipo di accesso che si desidera consentire o meno per l'utente o il gruppo selezionato.
Rimuovere un utente o un gruppo	Fare clic su Rimuovi .



Se alcune o tutte le caselle di autorizzazione standard non sono selezionabili, le autorizzazioni vengono ereditate dall'oggetto padre. La casella **permessi speciali** non è selezionabile. Se selezionata, significa che uno o più diritti avanzati granulari sono stati impostati per l'utente o il gruppo selezionato.

10. Una volta aggiunte, rimosse o modificate le autorizzazioni NTFS per l'oggetto, fare clic su **OK**.

Verificare l'accesso dell'utente

È necessario verificare che gli utenti configurati possano accedere alla condivisione SMB e ai file in essa contenuti.

Fasi

1. Su un client Windows, accedere come uno degli utenti che ora ha accesso alla condivisione.
2. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
3. Completare la casella **Map Network Drive** (Connetti unità di rete):
 - a. Selezionare una lettera **Drive**.
 - b. Nella casella **Folder** (cartella), digitare il nome della condivisione che verrà fornito agli utenti.

Se il nome del server SMB è SMB_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB_SERVER01\share1.

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.

4. Creare un file di test, verificare che esista, scriverne del testo e rimuovere il file di test.

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 d'urevoli			X	X	X	X

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
Operazioni composte			X	X	X	X
Operazioni asincrone			X	X	X	X
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
CRITTOGRA FIA SMB: AES-128-CCM	X				X	X

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
		9.0	9.1	9.2	9.3	9.4
Scale-out (richiesto dalle condivisioni CA)					X	X
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
```

Vserver	Database	Enabled	Source 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
```

Vserver	Database	Enabled	Source 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	<pre>vserver services name- service unix-user vserver services name-service unix-group</pre> <pre>vserver services name- service netgroup</pre> <pre>vserver services name- service dns hosts</pre>
nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	<pre>vserver services name- service ldap</pre>
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	<pre>vserver services name- service dns</pre>

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
```

Vserver	Database	Source	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: `vserver 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 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 ravvicinate 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	<pre>vserver cifs options modify -vserver vserver_name options</pre>
A livello di privilegi avanzati	<pre>a. set -privilege advanced b. vserver cifs options modify -vserver vserver_name options c. set -privilege admin</pre>

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	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Disattivare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

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
<code>no-restriction</code> (impostazione predefinita)	Non specifica restrizioni di accesso per utenti anonimi.
<code>no-enumeration</code>	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 qtrees](#)

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	<code>vserver cifs security show -vserver vserver_name</code>

Se si desidera visualizzare informazioni su...	Immettere il comando...
Una o più impostazioni di sicurezza specifiche sulla SVM	<code>vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]</code> È possibile immettere <code>-fields ?</code> 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	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required false</code>

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).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>L'impostazione predefinita è 5 minuti.</p>
Specificare la durata del ticket Kerberos in ore.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>L'impostazione predefinita è 10 ore.</p>
Specificare il numero massimo di giorni di rinnovo del ticket.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>L'impostazione predefinita è 7 giorni.</p>
Specificare il timeout per i socket sui KDC dopo il quale tutti i KDC sono contrassegnati come irraggiungibili.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>L'impostazione predefinita è 3 secondi.</p>

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	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Disattivato	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

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::> vsriver cifs security modify -vsriver 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::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  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	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Disattivato	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato:

```
vsriver cifs security show -vsriver vsriver_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 `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	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

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)	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>
Dettagli di una sessione firmata con un ID di sessione specifico sulla SVM	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

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
ID          ID      Workstation      Windows User      Open      Idle
-----
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	<code>`show -sample-id sample_ID -counter signed_sessions`</code>
<code>node_name [-node node_name]</code>	Sessioni firmate e sessioni stabilite
<code>`show -sample-id sample_ID -counter signed_sessions`</code>	<code>established_sessions</code>

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	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code>

- 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::> vsriver cifs security modify -vsriver vs1 -is-smb-encryption
-required true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-smb-
encryption-required
vsriver  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	<code>`vsriver cifs session show -vsriver vsriver_name {unencrypted</code>
<code>partially-encrypted</code>	<code>encrypted} -instance`</code>
L'impostazione di crittografia per un ID sessione specifico su una SVM specificata	<code>vsriver cifs session show -vsriver vsriver_name -session-id integer -instance</code>

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
<code>rejected_unencrypted_shares</code>	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	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>

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

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"](https://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"](https://technet.microsoft.com)

Al termine

Installare il certificato sulla SVM.

Informazioni correlate

["Microsoft TechNet Library"](https://technet.microsoft.com)

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\
4s                               Administrator      0
```

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"	<code>vserver cifs options modify -default -unix-user pcuser</code>
Utilizzare un altro account utente UNIX come utente predefinito	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Disattiva l'utente UNIX predefinito	<code>vserver cifs options modify -default -unix-user ""</code>

```
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	<code>vserver cifs options modify -guest -unix-user <i>unix_name</i></code>
Disattivare l'utente UNIX guest	<code>vserver cifs options modify -guest -unix-user ""</code>

```
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	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> 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	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> 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	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
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 publ -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
-----
publnode1 publ      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...
<p>Abilitare gli oplock su una condivisione durante la creazione della condivisione</p>	<p>Immettere il seguente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></p> <div data-bbox="873 615 927 667">  </div> <p>Se si desidera che la condivisione abbia solo le proprietà di condivisione predefinite, che sono <code>oplocks</code>, <code>browsable</code>, e. <code>changenotify</code> attivato, non è necessario specificare <code>-share-properties</code> Parametro durante la creazione di una condivisione SMB. Se si desidera una combinazione di proprietà di condivisione diversa da quella predefinita, è necessario specificare <code>-share-properties</code> parametro con l'elenco delle proprietà di condivisione da utilizzare per la condivisione.</p>
<p>Disattiva gli oplock su una condivisione durante la creazione della condivisione</p>	<p>Immettere il seguente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></p> <div data-bbox="873 1260 927 1312">  </div> <p>Quando si disattivano gli oplock, è necessario specificare un elenco di proprietà di condivisione durante la creazione della condivisione, ma non è necessario specificare <code>oplocks</code> proprietà.</p>

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	<code>volume qtree oplocks con -oplock-mode</code> parametro impostato su <code>enable</code>
Disattiva gli oplock sui volumi o sui qtree	<code>volume qtree oplocks con -oplock-mode</code> parametro impostato su <code>disable</code>

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	<p>Immettere il seguente comando: <code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div>  <p>È possibile specificare ulteriori proprietà di condivisione da aggiungere utilizzando un elenco delimitato da virgole.</p> </div> <p>Le nuove proprietà aggiunte vengono aggiunte all'elenco esistente di proprietà di condivisione. Tutte le proprietà di condivisione precedentemente specificate rimangono attive.</p>
Disattivare gli oplock su una condivisione modificando una condivisione esistente	<p>Immettere il seguente comando: <code>vserver cifs share properties remove -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div>  <p>È possibile specificare ulteriori proprietà di condivisione da rimuovere utilizzando un elenco delimitato da virgole.</p> </div> <p>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.</p>

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	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Disattivare gli oggetti Criteri di gruppo	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

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	<code>vserver cifs group-policy update -vserver vserver_name</code>
Tutte le impostazioni dell'oggetto Criteri di gruppo	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

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	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Applicato a una SVM (Storage Virtual Machine) abilitata per CIFS	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

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
```

```

    /voll/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	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

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: gp01
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: gp01  
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	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

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	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

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	<code>vserver cifs domain password change</code>
Reimpostare la password dell'account di dominio e non si conosce la password	<code>vserver cifs domain password reset</code>
Configurare i server SMB per la modifica automatica della password dell'account del computer	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>

Se si desidera...	Utilizzare questo comando...
Disattiva le modifiche automatiche della password dell'account del computer sui server SMB	<pre>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</pre>

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	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

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 conatterà 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 nulla non richiedono l'autenticazione, i client che richiedono l'accesso di sessione nulla 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	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
Tutti gli alias NetBIOS dall'elenco	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
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	<code>vserver cifs show -display-netbios -aliases</code>
L'elenco degli alias NetBIOS come parte delle informazioni dettagliate sul server CIFS	<code>vserver cifs show -instance</code>

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	<code>vserver cifs session show -instance</code>
Connessioni che utilizzano un alias NetBIOS specificato:	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

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	<code>`vserver cifs stop -vserver vserver_name [-foreground {true</code>
<code>false}}`</code>	Avviare il server CIFS
<code>`vserver cifs start -vserver vserver_name [-foreground {true</code>	<code>false}}`</code>

`-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	<code>vserver cifs create</code>
Visualizzare le informazioni su un server SMB	<code>vserver cifs show</code>
Modificare un server SMB	<code>vserver cifs modify</code>

Spostare un server SMB in un altro dominio	<code>vserver cifs modify</code>
Arrestare un server SMB	<code>vserver cifs stop</code>
Avviare un server SMB	<code>vserver cifs start</code>
Eliminare un server SMB	<code>vserver cifs delete</code>
Reimpostare e riscoprire i server per il server SMB	<code>vserver cifs domain discovered-servers reset-servers</code>
Modificare la password dell'account del computer del server SMB	<code>vserver cifs domain password change</code>
Reimpostare la password dell'account del computer del server SMB	<code>vserver cifs domain password change</code>
Pianificare le modifiche automatiche delle password per l'account del computer del server SMB	<code>vserver cifs domain password schedule modify</code>
Aggiungere alias NetBIOS per il server SMB	<code>vserver cifs add-netbios-aliases</code>
Rimuovere gli alias NetBIOS per il server SMB	<code>vserver cifs remove-netbios-aliases</code>

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	<code>vserver cifs session show -vserver <i>vserver_name</i> -instance</code>
IPv6 viene utilizzato per le sessioni SMB attraverso un indirizzo LIF specificato	<code>vserver cifs session show -vserver <i>vserver_name</i> -lif-address <i>LIF_IP_address</i> -instance</code> <i>LIF_IP_address</i> È l'indirizzo IPv6 del LIF dei dati.

Impostare l'accesso ai file utilizzando SMB

Configurare gli stili di sicurezza

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` II 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<code>volume create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume modify</code> e includono <code>-security-style</code> 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	<code>volume qtree create</code> e includono <code>-security -style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume qtree modify</code> e includono <code>-security -style</code> 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 vs1 -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 vs1 -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
```

Vserver	Volume	Active	Junction Path	Junction 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 vs1 -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 vs1 -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



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	<code>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</code>
Smontare un volume	<code>volume unmount -vserver svm_name -volume volume_name</code> <code>volume offline -vserver svm_name -volume volume_name</code>

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
```

Vserver	Volume	Active	Junction Path	Junction 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	data2_root	aggr3	8GB	online	RW	ntfs	/data2/d2_1		
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	pubs	aggr1	1GB	online	RW	unix	/publications		
vs2	images	aggr3	2TB	online	RW	ntfs	/images		
vs2	logs	aggr1	1GB	online	RW	unix	/logs		
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".
*	*	<p>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.</p> <div>  <p>Il modello è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.</p> </div>

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 riconnettersi 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	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Configurare l'utente Windows predefinito	<code>vserver nfs modify -default-win-user <i>user_name</i></code>

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	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>

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

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	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</code>

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 Unitto 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	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</code>
Rimuovere i domini attendibili dall'elenco	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</code>
Modificare l'elenco esistente	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</code>

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)	<code>vserver cifs domain name-mapping-search show</code>
Tutti i domini trusted preferiti per una SVM specificata	<code>vserver cifs domain name-mapping-search show -vserver <i>vserver_name</i></code>

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:

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

- I seguenti caratteri speciali non sono supportati quando si assegnano nomi SMB share:

◦ " / " ; | < > , ? * =

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 <i>Access Based Enumeration</i> (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	<pre>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>

Se si desidera...	Immettere il comando...
Rimuovere le proprietà di condivisione	<code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>

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	<code>vserver cifs share create</code>
Visualizzare le condivisioni SMB	<code>vserver cifs share show</code>
Modificare una condivisione SMB	<code>vserver cifs share modify</code>
Eliminare una condivisione SMB	<code>vserver cifs share delete</code>

Se si desidera...	Utilizzare questo comando...
Aggiungere le proprietà di condivisione a una condivisione esistente	<code>vserver cifs share properties add</code>
Rimuovere le proprietà di condivisione da una condivisione esistente	<code>vserver cifs share properties remove</code>
Visualizza le informazioni sulle proprietà di condivisione	<code>vserver cifs share properties show</code>

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	<code>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</code>
Gruppo di Windows	<code>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</code>
Utente UNIX	<code>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</code>
Gruppo UNIX	<code>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</code>

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

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access 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::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access 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::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

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

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	

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	<code>vsriver cifs share access-control create</code>
Visualizza ACL	<code>vsriver cifs share access-control show</code>
Modificare un ACL	<code>vsriver cifs share access-control modify</code>
Eliminare un ACL	<code>vsriver cifs share access-control delete</code>

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>.

- 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**.

- 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.

- 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**.
- Fare clic su **OK**.
- Dopo aver aggiunto, rimosso o modificato le autorizzazioni NTFS, specificare l'impostazione di ereditarietà per questo oggetto:

- Selezionare la casella **include inheritable 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.

- Fare clic su **OK** per chiudere la casella **Permissions**.
- 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](#)

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 <code>vserver security file-directory show</code> per visualizzare le informazioni sui criteri di accesso centrale applicati.
Analisi della sicurezza che include policy di accesso centralizzate	Estende <code>vserver security trace</code> 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	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

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	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Dove viene visualizzato l'output con SID di gruppo e utente	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>
Informazioni sulla sicurezza di file e directory per file e directory in cui la bit mask esadecimale viene convertita in formato testuale	<pre>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</pre>

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::> vservers export-policy rule create -vservers 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: `vservers cifs options modify -vservers vservers_name -is-exportpolicy-enabled true`
 - Disattiva policy di esportazione: `vservers cifs options modify -vservers vservers_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.

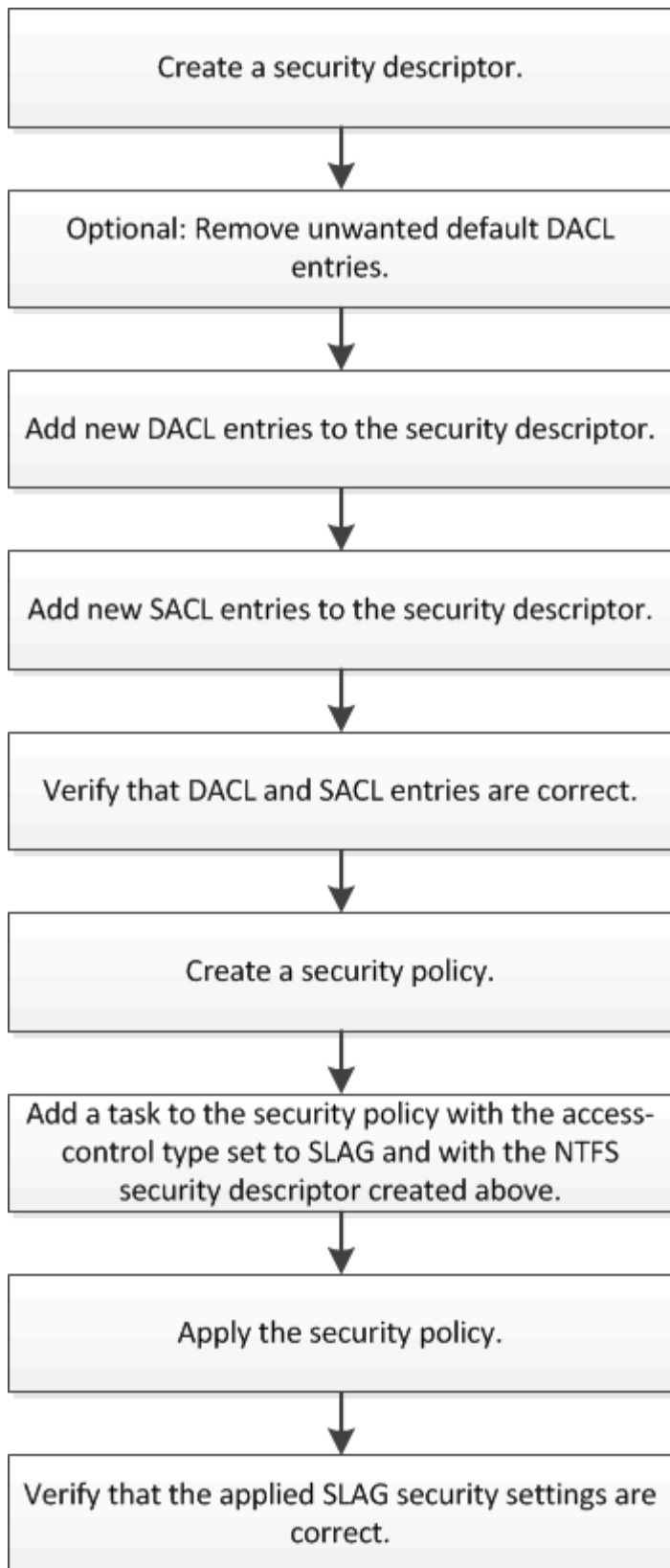
I casi di utilizzo tipici di questa funzionalità includono i seguenti scenari:

- 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 Descriptor Name	Owner 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 Type	Access Rights	Apply To
-----	-----	-----	-----
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 Type	Access Rights	Apply To
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 Type	Access Rights	Apply To
-----	-----	-----	-----
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 Type	Access Rights	Apply To
-----	-----	-----	-----
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	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

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 /datavol15 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\AdministratorsRID 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.	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
BUILTIN\Power UsersRID 547 Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo hanno le seguenti caratteristiche: <ul style="list-style-type: none"> • 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 OperatorsRID 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.	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
BUILTIN\UsersRID 545 Quando creato per la prima volta, questo gruppo non ha membri (oltre a quelli impliciti <code>Authenticated Users</code> gruppo speciale). Quando la SVM viene unita a un dominio, la <code>domain\Domain Users</code> il gruppo viene aggiunto a questo gruppo. Se SVM lascia il dominio, il <code>domain\Domain Users</code> il gruppo viene rimosso da questo gruppo.	SeChangeNotifyPrivilege
EveryoneSID 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 reimpresso 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	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</code>

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	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

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::*> vservers cifs options modify -vservers 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	<code>vservers cifs users-and-groups local-user modify -vservers vservers_name -user -name user_name -full-name text</code> Se il nome completo contiene uno spazio, deve essere racchiuso tra virgolette doppie.
Modificare la descrizione dell'utente locale	<code>vservers cifs users-and-groups local-user modify -vservers vservers_name -user -name user_name -description text</code> Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Attivare o disattivare l'account utente locale	<code>`vservers cifs users-and-groups local-user modify -vservers vservers_name -user-name user_name -is -account-disabled {true</code>
<code>false}`</code>	Rinominare l'account utente locale

Esempio

Nell'esempio seguente l'utente locale "CIFS_SERVER` sue" viene rinominata 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	<pre>vserver cifs users-and-groups local- user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account -disabled false</pre>
Disattivare l'account utente	<pre>vserver cifs users-and-groups local- user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account -disabled true</pre>

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::> vsserver cifs users-and-groups local-user set-password -user  
-name CIFS_SERVER\sue -vsserver 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)	<code>vsserver cifs users-and-groups local-user show -vsserver vsserver_name</code>
Visualizza informazioni dettagliate sull'account di un utente	<code>vsserver cifs users-and-groups local-user show -instance -vsserver vsserver_name -user-name user_name</code>

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	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Visualizza le informazioni di appartenenza dell'utente locale per il gruppo locale di cui l'utente locale è membro	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Visualizzazione delle informazioni di appartenenza degli utenti locali associati a una specifica SVM (Storage Virtual Machine)	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Visualizza informazioni dettagliate per tutti gli utenti locali su una SVM specificata	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

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

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

cluster1::> vsriver cifs users-and-groups local-user show -vsriver 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	<code>vsriver cifs users-and-groups local-group modify -vsriver vsriver_name -group-name group_name -description text</code> Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Rinominare il gruppo locale	<code>vsriver cifs users-and-groups local-group rename -vsriver vsriver_name -group-name group_name -new-group-name new_group_name</code>

Esempi

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

```

cluster1::> vsriver cifs users-and-groups local-group rename -vsriver 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::> vsriver cifs users-and-groups local-group modify -vsriver 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	<code>vsriver cifs users-and-groups local-group show</code>
Tutti i gruppi locali sulla SVM	<code>vsriver cifs users-and-groups local-group show -vsriver vsriver_name</code>

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::> vsriver cifs users-and-groups local-group show -vsriver 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	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.</p>
Rimuovere un membro da un gruppo	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.</p>

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_grpl
                                     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::> vsserver cifs users-and-groups local-group show -vsserver 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::> vsserver cifs users-and-groups local-group delete -vsserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vsserver cifs users-and-groups local-group show -vsserver 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	<code>vsserver cifs users-and-groups update-names -vsserver vsserver_name</code>

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	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Visualizzare solo gli utenti e i gruppi di dominio che non riescono ad aggiornare	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Elimina tutte le informazioni di stato relative agli aggiornamenti	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

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::*> vsserver cifs users-and-groups update-names -vsserver 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

```

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)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>
Privilegi personalizzati per un dominio o un utente e gruppo locale specifico sulla SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

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

cluster1::> vservers cifs users-and-groups privilege show -vservers vs1
Vservers    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: `vservers cifs users-and-groups privilege remove-privilege -vservers vservers_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: `vservers cifs users-and-groups privilege show -vservers vservers_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	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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

```

Synchronize1.....	=
Write Owner1.....	=
Write DAC1.....	=
Read Control1.....	=
Delete1.....	=
Write Attributes1.....	=
Read Attributes1.....	=
Delete Child1.....	=
Execute1.....	=
Write EA1.....	=
Read EA1.....	=
Append1.....	=
Write1.....	=
Read1.....	=
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0.....	=
Generic Write	.0.....	=
Generic Execute	..0.....	=
Generic All	...1.....	=
System Security0.....	=
Synchronize0.....	=
Write Owner0.....	=
Write DAC0.....	=

Read Control0..... =
Delete0..... =
Write Attributes0..... =
Read Attributes0..... =
Delete Child0..... =
Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

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](#)

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	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

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	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

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	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Come elenco dettagliato	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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 Type	Access Rights	Apply To
-----	-----	-----	-----
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 Type	Access Rights	Apply To
-----	-----	-----	-----
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_SID optional_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
	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
```

Generic Write	.0..	=
Generic Execute	..0.	=
Generic All	...0	=
System Security0	=
Synchronize1	=
Write Owner1...	=
Write DAC1..	=
Read Control1.	=
Delete1	=
Write Attributes1	=
Read Attributes1...	=
Delete Child1..	=
Execute1.	=
Write EA1	=
Read EA1...	=
Append1..	=
Write1.	=
Read1	=
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0...	=
Generic Write	.0..	=
Generic Execute	..0.	=
Generic All	...1	=

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_name optional_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 sac1 add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sac1 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 sac1 show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sac1 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 SAACL 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
            SAACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DAACL - 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	<code>vserver security file-directory ntfs create</code>
Modificare i descrittori di protezione NTFS esistenti	<code>vserver security file-directory ntfs modify</code>
Visualizza informazioni sui descrittori di protezione NTFS esistenti	<code>vserver security file-directory ntfs show</code>
Eliminare i descrittori di protezione NTFS	<code>vserver security file-directory ntfs delete</code>

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	<code>vserver security file-directory ntfs dacl add</code>
Modificare gli ACE esistenti nei DACL NTFS	<code>vserver security file-directory ntfs dacl modify</code>
Visualizza le informazioni sugli ACE esistenti nei DACL NTFS	<code>vserver security file-directory ntfs dacl show</code>
Rimuovere gli ACE esistenti dai DACL NTFS	<code>vserver security file-directory ntfs dacl remove</code>

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	<code>vserver security file-directory ntfs sacl add</code>
Modificare gli ACE esistenti nei SACL NTFS	<code>vserver security file-directory ntfs sacl modify</code>
Visualizza le informazioni sugli ACE esistenti nei SACL NTFS	<code>vserver security file-directory ntfs sacl show</code>
Rimuovere gli ACE esistenti dai SACL NTFS	<code>vserver security file-directory ntfs sacl remove</code>

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	<code>vserver security file-directory policy create</code>
Visualizzare informazioni sulle policy di sicurezza	<code>vserver security file-directory policy show</code>
Eliminare le policy di sicurezza	<code>vserver security file-directory policy delete</code>

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	<code>vserver security file-directory policy task add</code>
Modificare le attività dei criteri di protezione	<code>vserver security file-directory policy task modify</code>
Visualizza informazioni sulle attività dei criteri di protezione	<code>vserver security file-directory policy task show</code>
Rimuovere le attività dei criteri di protezione	<code>vserver security file-directory policy task remove</code>

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	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
Riprendere i processi di policy di sicurezza	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>

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

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	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code>

Se si desidera...	Immettere il comando...
Abilitare il caching dei metadati SMB su una condivisione esistente	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</pre>

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	<pre>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</pre>
Modificare una condivisione esistente	<pre>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</pre>

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	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
L'ID blocco	<code>vserver locks break -lockid UUID</code>

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	<code>vserver cifs session show -vserver vserver_name</code>
Su un ID di connessione specificato	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
Da un indirizzo IP della workstation specificato	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
Su un indirizzo IP LIF specificato	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
Su un nodo specificato	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
local}`	Da un utente Windows specificato
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	Con un meccanismo di autenticazione specificato
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
Con una versione del protocollo specificata	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
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	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>
Yes	<code>Partial}`</code> [NOTE] ===== <p>Se lo stato di disponibilità continua è <code>Partial</code>, 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 <code>vserver cifs sessions file show</code> comando per determinare quali file della sessione stabilita non sono aperti con una protezione continuamente disponibile.</p> =====
Con uno stato di sessione SMB Signing specificato	<code>`vserver cifs session show -vserver vserver_name -is-session-signed {true</code>

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
ID          ID      Workstation      Windows User      Open      Idle
-----
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	<code>vserver cifs session file show -vserver vserver_name</code>
Su un nodo specificato	<code>`vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	Su un ID file specificato
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	Su un ID connessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	Su un ID sessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	Sull'aggregato di hosting specificato
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	Sul volume specificato
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	Sulla condivisione SMB specificata

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	Sul percorso SMB specificato
<code>vserver cifs session file show -vserver vserver_name -path path</code>	Con il livello specificato di protezione a disponibilità continua
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	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	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

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::> vsriver cifs session file show -vsriver 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	<code>statistics catalog object show</code>
Oggetti specifici disponibili	<code>statistics catalog object show object object_name</code>
Quali contatori sono disponibili	<code>statistics catalog counter show object object_name</code>

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	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x e SMB 3.0	<code>statistics show -object smb2</code>
Sottosistema CIFS del nodo	<code>statistics show -object nblade_cifs</code>
Audit multiprotocollo	<code>statistics show -object audit_ng</code>
Servizio hash BranchCache	<code>statistics show -object hashd</code>
DNS dinamico	<code>statistics show -object ddns_update</code>

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
<code>none</code>	Non consente ai client Windows di memorizzare nella cache i file presenti in questa condivisione.
<code>manual</code>	Consente agli utenti sui client Windows di selezionare manualmente i file da memorizzare nella cache.
<code>documents</code>	Consente ai client Windows di memorizzare nella cache i documenti utente utilizzati dall'utente per l'accesso offline.
<code>programs</code>	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	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	Una condivisione SMB esistente
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	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::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver 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"](https://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::> vsserver cifs share show
Vserver  Share  Path      Properties      Comment  ACL
-----
vs1      eng    /eng      oplocks         -        Everyone / Full Control
          chngenotify
          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 vservers -name -volume volume-name -fields vservers,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
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::> vsriver cifs share create -vsriver vs1 -share-name %w -path %w  
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vsriver cifs share show -vsriver vs1
```

Vsriver	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::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver 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::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver 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::> vservice cifs share create -vservice vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vservice cifs share show -vservice vs1 -share-name %u
```

```

                Vservice: 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::> vservice cifs home-directory search-path add -vservice vs1 -path
/home1
```

```
cluster::> vservice cifs home-directory search-path show -vservice vs1
```

```
Vservice      Position Path
-----
vs1           1         /home1
```

```
cluster::> vservice name-mapping create -vservice vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vservice name-mapping show -pattern user1
```

```
Vservice      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	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\win_username che indica all'utente /vol1/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\win_username che indica all'utente /vol1/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\unix_username che indica all'utente /vol1/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

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	<code>vserver cifs home-directory search-path add</code>
Visualizzare i percorsi di ricerca	<code>vserver cifs home-directory search-path show</code>

Se si desidera...	Utilizzare questo comando...
Modificare l'ordine dei percorsi di ricerca	<code>vserver cifs home-directory search-path reorder</code>
Rimuovere un percorso di ricerca	<code>vserver cifs home-directory search-path remove</code>

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	<code>net use * \\IPAddress\~domain~user/u:credentials</code>

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)	<ol style="list-style-type: none"> 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
<code>read_only</code> (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.
<code>hide</code> (OBSOLETO*)	Specifica che ai client SMB viene impedito di visualizzare i collegamenti simbolici.
<code>no-strict-security</code>	Specifica che i client seguono collegamenti simbolici al di fuori dei limiti di condivisione.
<code>symlinks</code>	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 <code>is-advertise-dfs-enabled</code> è impostato su <code>true</code> . Questa è l'impostazione predefinita.
<code>symlinks-and-widelinks</code>	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 widelink anche se l'opzione CIFS <code>is-advertise-dfs-enabled</code> è impostato su <code>false</code> .
<code>disable</code>	Specifica che i collegamenti simbolici e i collegamenti widelink sono disattivati. Gli annunci DFS non vengono generati anche se l'opzione CIFS <code>is-advertise-dfs-enabled</code> è impostato su <code>true</code> .
<code>""</code> (nullo, non impostato)	Disattiva i collegamenti simbolici sulla condivisione.
<code>-</code> (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	<code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code>
<code>hide</code>	<code>read-only</code>

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 widelink.

```
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	<code>vserver cifs symlink create</code>
Visualizza informazioni sulle mappature dei collegamenti simbolici	<code>vserver cifs symlink show</code>
Modificare un mapping di collegamento simbolico	<code>vserver cifs symlink modify</code>
Eliminare un mapping di collegamento simbolico	<code>vserver cifs symlink delete</code>

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](#)

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
<i>Nome SVM</i>	BranchCache viene configurato per SVM. Specificare su quale SVM CIFS-Enabled si desidera configurare il servizio BranchCache.

Parametri richiesti	Descrizione
<i>Percorso all'archivio hash</i>	<p>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.</p> <p>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.</p> <p>Il percorso hash può contenere spazi vuoti e qualsiasi carattere di nome file valido.</p>

È possibile specificare i seguenti parametri:

Parametri opzionali	Descrizione
<i>Versioni supportate</i>	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.
<i>Dimensione massima dell'archivio hash</i>	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
<i>Chiave server</i>	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.
<i>Modalità operativa</i>	<p>Per impostazione predefinita, BranchCache viene attivato in base alle condivisioni.</p> <ul style="list-style-type: none"> • Per creare una configurazione BranchCache in cui abilitare BranchCache in base alle condivisioni, non è possibile specificare questo parametro facoltativo oppure è possibile specificarlo <code>per-share</code>. • Per attivare automaticamente BranchCache su tutte le condivisioni, è necessario impostare la modalità operativa su <code>all-shares</code>.

Fasi

1. Abilitazione di SMB 2.1 e 3.0 in base alle esigenze:

- Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
- Controllare le impostazioni SMB SVM configurate per determinare se tutte le versioni richieste di SMB sono abilitate: `vserver cifs options show -vserver vserver_name`
- 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.

- Se necessario, abilitare SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
- 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,notify

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
                  notify
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::> vsserver cifs share show -vsserver 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::> vsserver cifs share properties add -vsserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vsserver cifs share show -vsserver 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

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	<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</code>
MB	GB
TB	PB]}`
Aumentare le dimensioni del volume che contiene l'archivio hash	<code>`volume size -vserver vserver_name -volume volume_name -new-size new_size[k</code>
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...
<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</code>	<p><code>false}`</code> 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.</p> <p>Il percorso hash di BranchCache può contenere spazi vuoti e qualsiasi carattere valido per il nome del file.</p> <p>Se si modifica il percorso hash, <code>-flush-hashes</code> 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 <code>-flush-hashes</code> parametro:</p> <p>Se si specifica <code>true</code>, 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.</p> <p>Se si specifica <code>false</code>, gli hash non vengono spazzati via.</p> <p>+</p> <p>In questo caso, è possibile scegliere di riutilizzare gli hash esistenti in un secondo momento modificando il percorso dell'archivio hash nella posizione originale.</p>
Modificare la modalità operativa	<code>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</code>
all-shares	<p><code>disable}`</code></p> <p>Quando si modifica la modalità operativa, tenere presente quanto segue:</p> <p>ONTAP annuncia il supporto di BranchCache per una condivisione quando viene impostata la sessione SMB.</p> <p>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.</p>
Modificare il supporto della versione di BranchCache	<code>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</code>
v2-enable	<code>enable-all}`</code>

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	<code>vserver cifs branchcache show</code>
Informazioni dettagliate sulla configurazione di una SVM specifica	<code>vserver cifs branchcache show -vserver <i>vserver_name</i></code>

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	<code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</code>
In modo ricorrente su tutti i file di una struttura di directory	<code>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</code>

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

```

It attempting to read existing hash data.
data 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
to be Total number of bytes of data that had
that read by the client because the hash for
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	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</pre>
Attiva BranchCache per share	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</pre>
Abilitare BranchCache per tutte le condivisioni	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</pre>

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	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code>
Eliminare la configurazione BranchCache ma mantenere gli hash esistenti	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code>

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.

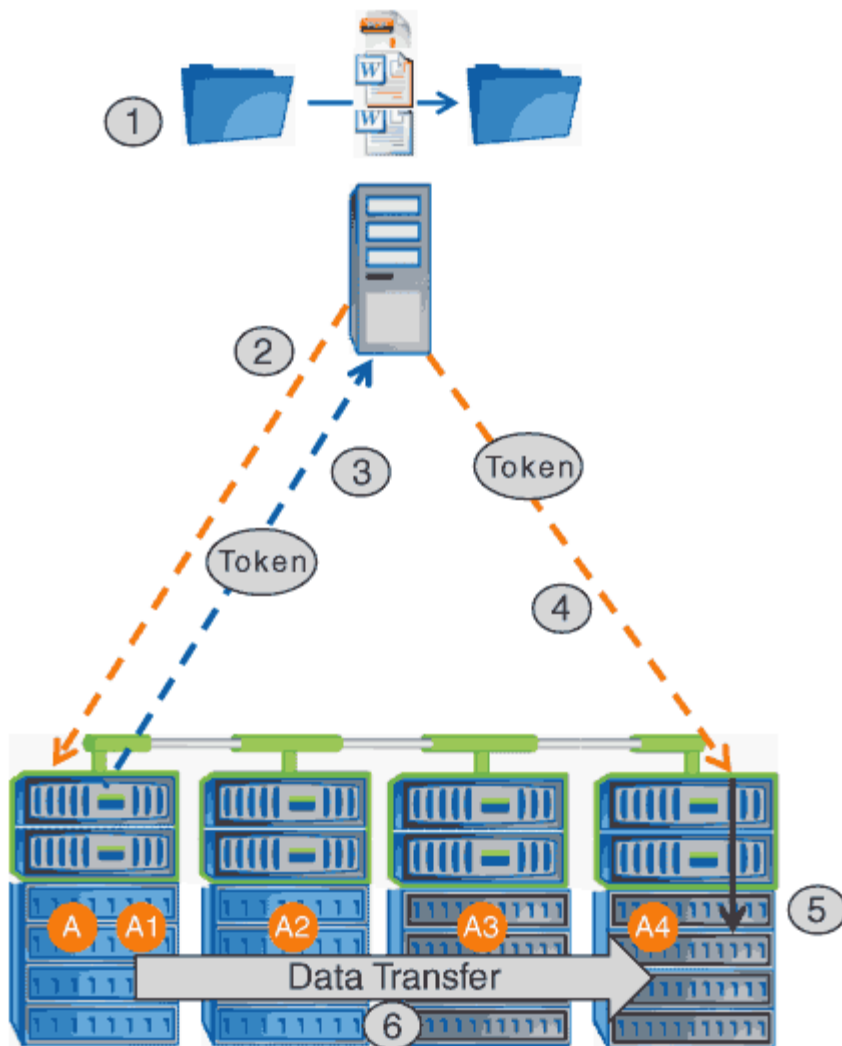


L'origine e la destinazione possono trovarsi sulla stessa SVM (Storage Virtual Machine) o su SVM diverse, a seconda dell'ambito dell'operazione di copia.

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	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

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 disgiunto. 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	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code>

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/"](http://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	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> 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 <code>vserver cifs share create</code> comando.
Abilitare ABE su una condivisione esistente	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> 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	<code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> 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` il 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 `test.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
0x22	"	Virgoletta

Carattere Unicode	Carattere stampato	Descrizione
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	<code>vserver cifs character-mapping create</code>
Visualizza le informazioni sulle mappature dei caratteri del file	<code>vserver cifs character-mapping show</code>
Modificare le mappature dei caratteri del file esistente	<code>vserver cifs character-mapping modify</code>

Se si desidera...	Utilizzare questo comando...
Eliminare le mappature dei caratteri del file	<code>vserver cifs character-mapping delete</code>

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](#)

Fornire l'accesso del client S3 ai dati NAS

Panoramica sul multiprotocollo S3

A partire da ONTAP 9.12.1, è possibile consentire ai client che eseguono il protocollo S3 di accedere agli stessi dati forniti ai client che utilizzano i protocolli NFS e SMB senza riformattare. Questa funzionalità consente ai dati NAS di continuare a essere serviti ai client NAS, presentando al contempo i dati a oggetti ai client S3 che eseguono applicazioni S3 (come data mining e intelligenza artificiale).

La funzionalità multiprotocollo S3 consente di gestire due casi di utilizzo:

1. Accesso ai dati NAS esistenti mediante client S3

Se i dati esistenti sono stati creati utilizzando client NAS tradizionali (NFS o SMB) e si trovano su volumi NAS (volumi FlexVol o FlexGroup), è ora possibile utilizzare strumenti analitici sui client S3 per accedere a questi dati.

2. Storage back-end per client moderni in grado di eseguire i/o utilizzando protocolli NAS e S3

È ora possibile fornire un accesso integrato ad applicazioni come Spark e Kafka in grado di leggere e scrivere gli stessi dati utilizzando i protocolli NAS e S3.

Funzionamento del multiprotocollo S3

Il multiprotocollo ONTAP consente di presentare lo stesso set di dati come una gerarchia di file o come oggetti in un bucket. A tale scopo, ONTAP crea "bucket S3 NAS" che consentono ai client S3 di creare, leggere, eliminare ed enumerare i file nello storage NAS utilizzando le richieste a oggetti S3. Questa mappatura è conforme alla configurazione di sicurezza NAS, osservando le autorizzazioni di accesso a file e directory e scrivendo nel registro di controllo della sicurezza secondo necessità.

Questa mappatura viene eseguita presentando una gerarchia di directory NAS specificata come bucket S3. Ogni file nella gerarchia di directory è rappresentato come un oggetto S3 il cui nome è relativo dalla directory mappata verso il basso, con i limiti di directory rappresentati dal carattere barra ('/').

Gli utenti S3 definiti da ONTAP normali possono accedere a questo storage, in base alle policy bucket definite per il bucket che esegue la mappatura alla directory NAS. Affinché ciò sia possibile, è necessario definire le mappature tra gli utenti S3 e gli utenti SMB/NFS. Le credenziali dell'utente SMB/NFS verranno utilizzate per il controllo delle autorizzazioni NAS e incluse nei record di audit risultanti da tali accessi.

Quando viene creato da client SMB o NFS, un file viene immediatamente inserito in una directory e quindi visibile ai client, prima che i dati vengano scritti in essa. I client S3 si aspettano semantica diversa, in cui il

nuovo oggetto non è visibile nello spazio dei nomi fino a quando non sono stati scritti tutti i dati. Questa mappatura di S3 allo storage NAS crea file utilizzando la semantica S3, mantenendo i file invisibili esternamente fino al completamento del comando di creazione S3.

Protezione dei dati per i bucket S3 NAS

I "bucket" S3 NAS sono semplicemente mappature di dati NAS per i client S3, non sono bucket S3 standard. Pertanto, non è necessario proteggere i bucket S3 NAS utilizzando la funzionalità SnapMirror di NetApp S3. È invece possibile proteggere volumi contenenti bucket S3 NAS utilizzando la replica del volume asincrona SnapMirror. Il disaster recovery di SnapMirror Synchronous e SVM non è supportato.

A partire da ONTAP 9.14.1, i bucket S3 NAS sono supportati in aggregati con mirroring e senza mirror per le configurazioni MetroCluster IP e FC.

Scopri di più ["SnapMirror asincrono"](#).

Audit per i bucket S3 NAS

Poiché i bucket S3 NAS non sono bucket S3 convenzionali, l'audit S3 non può essere configurato per controllare l'accesso su di essi. Scopri di più ["Verifica S3"](#).

Tuttavia, i file e le directory NAS mappati nei bucket S3 NAS possono essere controllati per gli eventi di accesso utilizzando le procedure di audit ONTAP convenzionali. Le operazioni S3 possono quindi attivare eventi di audit NAS, con le seguenti eccezioni:

- Se l'accesso al client S3 viene negato dalla configurazione del criterio S3 (policy di gruppo o bucket), l'audit NAS per l'evento non viene avviato. Questo perché le autorizzazioni S3 vengono controllate prima di poter eseguire i controlli di audit SVM.
- Se il file di destinazione di una richiesta S3 GET è di dimensione 0, il contenuto 0 viene restituito alla richiesta GET e l'accesso in lettura non viene registrato.
- Se il file di destinazione di una richiesta S3 GET si trova in una cartella per la quale l'utente non dispone dell'autorizzazione di attraversamento, il tentativo di accesso non riesce e l'evento non viene registrato.

Scopri di più ["Controllo degli eventi NAS su SVM"](#).

Interoperabilità S3 e NAS

I bucket NAS ONTAP S3 supportano le funzionalità NAS e S3 standard, ad eccezione di quelle elencate di seguito.

Funzionalità NAS attualmente non supportata dai bucket S3 NAS

Tier di capacità FabricPool

I bucket S3 NAS non possono essere configurati come Tier di capacità per FabricPool.

La funzionalità S3 non è attualmente supportata dai bucket S3 NAS

Metadati utente AWS

- Le coppie di valori chiave ricevute come parte dei metadati utente S3 non vengono memorizzate su disco insieme ai dati oggetto nella release corrente.
- Le intestazioni delle richieste con il prefisso "x-amz-meta" vengono ignorate.

Tag AWS

- All'avvio delle richieste PUT object e Multipart, le intestazioni con il prefisso "x-amz-tagging" vengono ignorate.
- Le richieste di aggiornamento dei tag su un file esistente (ad esempio, richieste put, GET ed Delete con la stringa di query ?tagging) vengono rifiutate con un errore.

Versione

Non è possibile specificare la versione nella configurazione di mappatura bucket.

- Le richieste che includono specifiche di versione non null (versionID=stringa di query xyz) ricevono risposte di errore.
- Le richieste che influiscono sullo stato di versione di un bucket vengono rifiutate con errori.

Operazioni multiparte

Le seguenti operazioni non sono supportate:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Requisiti dei dati NAS per l'accesso al client S3

È importante comprendere che ci sono alcune incompatibilità intrinseche quando si mappano file e directory NAS per l'accesso S3. Potrebbe essere necessario regolare le gerarchie dei file NAS prima di servirle utilizzando i bucket S3 NAS.

Un bucket S3 NAS fornisce l'accesso S3 a una directory NAS mappando tale directory utilizzando la sintassi del bucket S3 e i file nell'albero delle directory vengono visualizzati come oggetti. I nomi degli oggetti sono i percorsi delimitati dalla barra dei file relativi alla directory specificata nella configurazione del bucket S3.

Questa mappatura impone alcuni requisiti quando i file e le directory vengono serviti utilizzando i bucket NAS S3:

- I nomi S3 sono limitati a 1024 byte, pertanto i file con percorsi più lunghi non sono accessibili utilizzando S3.
- I nomi di file e directory sono limitati a 255 caratteri, pertanto il nome di un oggetto non può contenere più di 255 caratteri consecutivi non slash ('/')
- Un nome percorso SMB delimitato da caratteri backslash ("\") viene visualizzato in s3 come nome di oggetto contenente caratteri '/' (barra rovesciata).
- Alcune coppie di nomi di oggetti S3 legali non possono coesistere nell'albero di directory NAS mappato. Ad esempio, i nomi degli oggetti S3 legali "part1/part2" e "part1/part2/part3" corrispondono a file che non possono esistere contemporaneamente nell'albero delle directory NAS, in quanto "part1/part2" è un file nel nome e una directory nell'altro.
 - Se "part1/part2" è un file esistente, la creazione S3 di "part1/part2/part3" non riesce.
 - Se "part1/part2/part3" è un file esistente, la creazione o l'eliminazione S3 di "part1/part2" non avrà esito positivo.
 - La creazione di un oggetto S3 che corrisponde al nome di un oggetto esistente sostituisce l'oggetto

pre-esistente (nei bucket senza versione), che contiene in NAS ma richiede una corrispondenza esatta. Gli esempi precedenti non causeranno la rimozione dell'oggetto esistente perché, mentre i nomi si scontrano, non corrispondono.

Sebbene un archivio di oggetti sia progettato per supportare un numero molto elevato di nomi arbitrari, una struttura di directory NAS può riscontrare problemi di performance se un numero molto elevato di nomi viene inserito in una directory. In particolare, i nomi che non contengono caratteri slash (/) verranno tutti inseriti nella directory principale della mappatura NAS. Le applicazioni che utilizzano in modo esteso nomi non compatibili con NAS potrebbero essere ospitate meglio su un bucket di archivio di oggetti effettivo piuttosto che su una mappatura NAS.

Abilitare l'accesso del protocollo S3 ai dati NAS

L'abilitazione dell'accesso al protocollo S3 consiste nel garantire che una SVM abilitata NAS soddisfi gli stessi requisiti di un server abilitato S3, tra cui l'aggiunta di un server di archiviazione a oggetti e la verifica dei requisiti di rete e autenticazione.

Per le nuove installazioni ONTAP, si consiglia di abilitare l'accesso al protocollo S3 a una SVM dopo averla configurato per fornire i dati NAS ai client. Per ulteriori informazioni sulla configurazione del protocollo NAS, consultare:

- ["Configurazione NFS"](#)
- ["Configurazione SMB"](#)

Prima di iniziare

Prima di attivare il protocollo S3, è necessario configurare quanto segue:

- Il protocollo S3 e i protocolli NAS desiderati (NFS, SMB o entrambi) sono concessi in licenza.
- Viene configurata una SVM per i protocolli NAS desiderati.
- Esistono server NFS e/o SMB.
- Il DNS e gli altri servizi richiesti sono configurati.
- I dati NAS vengono esportati o condivisi nei sistemi client.

A proposito di questa attività


Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority). È possibile utilizzare certificati CA provenienti da tre origini:

- Un nuovo certificato autofirmato ONTAP sulla SVM.
- Un certificato autofirmato ONTAP esistente su SVM.
- Un certificato di terze parti.

Per il bucket S3/NAS è possibile utilizzare le stesse LIF di dati utilizzate per la fornitura dei dati NAS. Se sono richiesti indirizzi IP specifici, vedere ["Creazione di LIF di dati"](#). Per attivare il traffico dati S3 su LIF è necessaria una policy dei dati del servizio S3; è possibile modificare la policy di servizio esistente di SVM in modo da includere S3.

Quando si crea il server a oggetti S3, si dovrebbe essere pronti a inserire il nome del server S3 come FQDN (Fully Qualified Domain Name), che i client utilizzeranno per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

System Manager

1. Abilitare S3 su una VM di storage con protocolli NAS configurati.
 - a. Fare clic su **Storage > Storage VM**, selezionare una VM storage pronta per NAS, fare clic su Settings (Impostazioni), quindi fare clic su  Sotto S3.
 - b. Selezionare il tipo di certificato. Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.
 - c. Inserire le interfacce di rete.
2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.
 - La chiave segreta non viene visualizzata di nuovo.
 - Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

CLI

1. Verificare che il protocollo S3 sia consentito su SVM:
`vserver show -fields allowed-protocols`
2. Registrare il certificato della chiave pubblica per questa SVM. + se è necessario un nuovo certificato autofirmato ONTAP, vedere ["Creare e installare un certificato CA sulla SVM"](#).
3. Aggiornare la policy dei dati del servizio
 - a. Visualizzare la policy dei dati di servizio per SVM
`network interface service-policy show -vserver svm_name`
 - b. Aggiungere il data-core e data-s3-server services se non sono presenti.
`network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Verificare che i dati LIF presenti su SVM soddisfino i requisiti:
`network interface show -vserver svm_name`
5. Creare il server S3:
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con l'opzione `-Secure-listener-port`. + quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.
- HTTP è disattivato per impostazione predefinita; se attivato, il server è in attesa sulla porta 80. Puoi abilitarlo con l'opzione `-is-http-enabled` o modificare il numero di porta con l'opzione `-listener-port`. + quando HTTP è attivato, tutte le richieste e le risposte vengono inviate in rete in testo non crittografato.

1. Verificare che S3 sia configurato come desiderato:
`vserver object-store-server show`

Esempio + il seguente comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

Creare un bucket S3 NAS

Un bucket S3 NAS è una mappatura tra un nome di bucket S3 e un percorso NAS. I bucket NAS S3 consentono di fornire l'accesso S3 a qualsiasi parte di uno spazio dei nomi SVM con volumi e struttura di directory esistenti.

Prima di iniziare

- Un server a oggetti S3 è configurato in una SVM contenente dati NAS.
- I dati NAS sono conformi a ["Requisiti per l'accesso al client S3"](#).

A proposito di questa attività

È possibile configurare i bucket S3 NAS per specificare qualsiasi set di file e directory all'interno della directory root di SVM.

È inoltre possibile impostare policy bucket che consentono o non consentono l'accesso ai dati NAS in base a qualsiasi combinazione di questi parametri:

- File e directory
- Autorizzazioni utente e gruppo
- Operazioni S3

Ad esempio, potrebbero essere necessarie policy di bucket separate che concedano l'accesso ai dati di sola lettura a un gruppo di utenti di grandi dimensioni e un'altra che consenta a un gruppo limitato di eseguire operazioni su un sottoinsieme di tali dati.

Poiché i "bucket" S3 NAS sono mappature e non bucket S3, le seguenti proprietà dei bucket S3 standard non si applicano ai bucket S3 NAS.

- **Aggr-list/aggr-list-moltiplicer/storage-service-level/volume/size/exclude-aggr-list/qos-policy-group** + Nessun volume o qtree viene creato durante la configurazione dei bucket S3 NAS.
- **Il ruolo è -protetto/è -Protected-on-ontap/è -Protected-on-cloud** + i bucket NAS S3 non sono protetti o mirrorati utilizzando S3 SnapMirror, ma utilizzeranno invece la protezione SnapMirror regolare disponibile alla granularità del volume.

- **Versioning-state** + i volumi NAS dispongono solitamente della tecnologia Snapshot per salvare versioni diverse. Tuttavia, la versione non è attualmente disponibile nei bucket S3 NAS.
- I comandi del volume consentono di accedere alle statistiche utilizzate in modo logico/object-count* + equivalenti per i volumi NAS.

System Manager

Aggiungere un nuovo bucket S3 NAS su una VM di storage abilitata per NAS.

1. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
2. Inserire un nome per il bucket S3 NAS e selezionare la VM di storage, non inserire una dimensione, quindi fare clic su **altre opzioni**.
3. Immettere un nome di percorso valido o fare clic su Browse (Sfogliare) per effettuare una selezione da un elenco di nomi di percorso validi. + quando si immette un nome di percorso valido, le opzioni non rilevanti per la configurazione S3 NAS vengono nascoste.
4. Se gli utenti S3 sono già stati mappati agli utenti NAS e sono stati creati dei gruppi, è possibile configurarne le autorizzazioni, quindi fare clic su **Save** (Salva). + prima di configurare le autorizzazioni in questa fase, è necessario aver già mappato gli utenti S3 agli utenti NAS.

Altrimenti, fare clic su **Save** (Salva) per completare la configurazione del bucket S3 NAS.

CLI

Creare un bucket S3 NAS in una SVM contenente i filesystem NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Esempio:

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

Abilitare gli utenti del client S3

Per consentire agli utenti del client S3 di accedere ai dati NAS, è necessario mappare i nomi utente S3 agli utenti NAS corrispondenti, quindi concedere loro l'autorizzazione ad accedere ai dati NAS utilizzando i criteri di servizio bucket.

Prima di iniziare

I nomi utente per l'accesso al client (utenti LINUX/UNIX, Windows e S3) devono già esistere.

A proposito di questa attività

La mappatura di un nome utente S3 a un utente LINUX/UNIX o Windows corrispondente consente di onorare i controlli di autorizzazione sui file NAS quando tali file sono accessibili dai client S3. Le mappature da S3 a NAS vengono specificate fornendo un nome utente S3 *Pattern*, che può essere espresso come un singolo nome o un'espressione regolare POSIX, e un nome utente LINUX/UNIX o Windows *Replacement*.

Se non è presente alcuna mappatura dei nomi, viene utilizzata la mappatura dei nomi predefinita, in cui il nome utente S3 stesso verrà utilizzato come nome utente UNIX e nome utente Windows. È possibile modificare le mappature predefinite dei nomi utente UNIX e Windows con `vserver object-store-server modify` comando.

È supportata solo la configurazione di mappatura dei nomi locali; LDAP non è supportato.

Una volta mappati gli utenti S3 agli utenti NAS, è possibile concedere autorizzazioni agli utenti specificando le risorse (directory e file) a cui hanno accesso e le azioni che possono eseguire o meno.

System Manager

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).
 - a. Fare clic su **Storage > Bucket**, quindi selezionare la VM di storage abilitata per S3/NAS.
 - b. Selezionare **Impostazioni**, quindi fare clic su ➔ In **Name Mapping** (sotto **host Users and Groups**).
 - c. Nei riquadri **S3 to Windows** o **S3 to UNIX** (o entrambi), fare clic su **Add** (Aggiungi), quindi immettere i nomi utente desiderati **Pattern** (S3) e **Replacement** (NAS).
2. Creare una policy bucket per fornire l'accesso al client.
 - a. Fare clic su **Storage > Bucket**, quindi su ⓘ Accanto al bucket S3 desiderato, quindi fare clic su **Edit** (Modifica).
 - b. Fare clic su **Add** (Aggiungi) e fornire i valori desiderati.
 - **Principal** - specificare i nomi utente S3 o utilizzare il valore predefinito (tutti gli utenti).
 - **Effetto** - selezionare **Consenti** o **Nega**.
 - **Azioni** - inserire azioni per questi utenti e risorse. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` e `ListBucketVersions`. I caratteri jolly sono accettati per questo parametro.
 - **Risorse** - inserire i percorsi di cartella o file in cui le azioni sono consentite o rifiutate, oppure utilizzare le impostazioni predefinite (directory principale del bucket).

CLI

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).

```
vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}
-position integer -pattern s3_user_name -replacement nas_user_name
```

 - `-position` - numero di priorità per la valutazione della mappatura; inserire 1 o 2.
 - `-pattern` - Un nome utente S3 o un'espressione regolare
 - `-replacement` - un nome utente windows o unix

Esempi

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Creare una policy bucket per fornire l'accesso al client.

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal
list_of_users_or_groups -resource [-sid alphanumeric_text]
```

 - `-effect {deny|allow}` - specifica se l'accesso è consentito o negato quando un utente richiede un'azione.
 - `-action <Action>, ...` - specifica le operazioni di risorsa consentite o negate. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`,

PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning e ListBucketVersions. I caratteri jolly sono accettati per questo parametro.

- `-principal <Objectstore Principal>, ...` - convalida l'utente che richiede l'accesso in base agli utenti o ai gruppi del server dell'archivio di oggetti specificati in questo parametro.
 - Per specificare un gruppo di server di archiviazione oggetti, aggiungere un gruppo di prefissi/ al nome del gruppo.
 - `-principal -` (il trattino) consente l'accesso a tutti gli utenti.
- `-resource <text>, ...` - specifica il bucket, la cartella o l'oggetto per il quale sono impostate le autorizzazioni allow/deny. I caratteri jolly sono accettati per questo parametro.
- `[-sid <SID>]` - specifica un commento di testo facoltativo per l'istruzione del criterio bucket del server archivio oggetti.

Esempi

```
cluster1::> vservers object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* -sid "FullAccessForUser1"

cluster1::> vservers object-store-server bucket policy statement create
-vservers vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configurazione SMB per Microsoft Hyper-V e SQL Server

Panoramica della configurazione SMB per Microsoft Hyper-V e SQL Server

Le funzionalità di ONTAP consentono di eseguire operazioni senza interruzioni per due applicazioni Microsoft tramite il protocollo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Utilizzare queste procedure se si desidera implementare operazioni SMB senza interruzioni nei seguenti casi:

- È stato configurato l'accesso al file del protocollo SMB di base.
- Si desidera abilitare le condivisioni di file SMB 3.0 o versioni successive che risiedono in SVM per memorizzare i seguenti oggetti:
 - File di macchine virtuali Hyper-V.
 - Database di sistema di SQL Server

Informazioni correlate

Per ulteriori informazioni sulla tecnologia ONTAP e sull'interazione con i servizi esterni, consultare i seguenti report tecnici: ["Report tecnico NetApp 4172: Best practice Microsoft Hyper-V su SMB 3.0 con ONTAP"](#) ["Report tecnico NetApp 4369: Best practice per Microsoft SQL Server e SnapManager 7.2 per SQL Server con Clustered Data ONTAP"](#)

Configurare ONTAP per le soluzioni Microsoft Hyper-V e SQL Server su SMB

È possibile utilizzare le condivisioni di file SMB 3.0 e versioni successive disponibili in modo continuo per memorizzare i file delle macchine virtuali Hyper-V o i database di sistema SQL Server e i database degli utenti su volumi residenti in SVM, fornendo al contempo operazioni senza interruzioni (NDOS) per eventi pianificati e non pianificati.

Microsoft Hyper-V su SMB

Per creare una soluzione Hyper-V su SMB, devi prima configurare ONTAP per fornire servizi di storage per i server Microsoft Hyper-V. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster), i server Hyper-V, le connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS e, facoltativamente, i servizi di backup per proteggere i file delle macchine virtuali memorizzati nei volumi SVM.



I server Hyper-V devono essere configurati su Windows 2012 Server o versioni successive. Sono supportate le configurazioni dei server Hyper-V in cluster e standalone.

- Per informazioni sulla creazione di cluster Microsoft e server Hyper-V, visitare il sito Web Microsoft.
- SnapManager per Hyper-V è un'applicazione basata su host che semplifica i servizi di backup rapidi basati su copia Snapshot, progettati per l'integrazione con le configurazioni Hyper-V su SMB.

Per informazioni sull'utilizzo di SnapManager con configurazioni Hyper-V su SMB, consultare la [_Guida all'installazione e all'amministrazione di SnapManager per Hyper-V](#).

Microsoft SQL Server su SMB

Per creare una soluzione SQL Server su SMB, è necessario prima configurare ONTAP per fornire servizi di storage per l'applicazione Microsoft SQL Server. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster). Installare e configurare SQL Server sui server Windows e creare connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS. Facoltativamente, è possibile configurare i servizi di backup per proteggere i file di database memorizzati nei volumi SVM.



SQL Server deve essere installato e configurato su Windows 2012 Server o versione successiva. Sono supportate sia le configurazioni standalone che quelle in cluster.

- Per informazioni sulla creazione di cluster Microsoft e sull'installazione e configurazione di SQL Server, visitare il sito Web Microsoft.
- Il plug-in SnapCenter per Microsoft SQL Server è un'applicazione basata su host che semplifica i servizi di backup rapidi basati su copia Snapshot, progettati per l'integrazione con le configurazioni SQL Server su SMB.

Per informazioni sull'utilizzo del plug-in SnapCenter per Microsoft SQL Server, vedere ["Plug-in SnapCenter per Microsoft SQL Server"](#) documento.

Operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Che cosa significa operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB si riferiscono alla

combinazione di funzionalità che consentono ai server di applicazioni e alle macchine virtuali o ai database contenuti di rimanere online e di garantire una disponibilità continua durante molte attività amministrative. Ciò include downtime pianificati e non pianificati dell'infrastruttura storage.

Le operazioni senza interruzioni supportate per i server di applicazioni su SMB includono:

- Acquisizione e giveback pianificati
- Takeover non pianificato
- Eseguire l'upgrade
- Delocalizzazione pianificata degli aggregati (ARL)
- Migrazione LIF e failover
- Spostamento pianificato del volume

Protocolli che consentono operazioni senza interruzioni su SMB

Insieme al rilascio di SMB 3.0, Microsoft ha rilasciato nuovi protocolli per fornire le funzionalità necessarie per supportare operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

ONTAP utilizza questi protocolli quando fornisce operazioni senza interruzioni per server di applicazioni su PMI:

- SMB 3.0
- Testimone

Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Prima di configurare la soluzione Hyper-V o SQL Server su SMB, è necessario comprendere alcuni concetti relativi alle operazioni senza interruzioni (NDOS).

• Quota a disponibilità continua

Una condivisione SMB 3.0 con la proprietà di condivisione continuamente disponibile impostata. I client che si connettono attraverso condivisioni continuamente disponibili possono sopravvivere a eventi di interruzione come takeover, giveback e trasferimento aggregato.

• Nodo *

Un singolo controller che è membro di un cluster. Per distinguere i due nodi di una coppia SFO, un nodo viene talvolta chiamato *nodo locale* e l'altro nodo viene talvolta chiamato *nodo partner* o *nodo remoto*. Il principale proprietario dello storage è il nodo locale. Il proprietario secondario, che assume il controllo dello storage in caso di guasto del proprietario primario, è il nodo partner. Ciascun nodo è il principale proprietario dello storage e il proprietario secondario dello storage del partner.

• Trasferimento aggregato senza interruzioni

Possibilità di spostare un aggregato tra nodi partner all'interno di una coppia SFO in un cluster senza interrompere le applicazioni client.

- **Failover senza interruzioni**

Vedi *Takeover*.

- **Migrazione LIF senza interruzioni**

La possibilità di eseguire una migrazione LIF senza interrompere le applicazioni client connesse al cluster attraverso tale LIF. Per le connessioni SMB, ciò è possibile solo per i client che si connettono utilizzando SMB 2.0 o versioni successive.

- **Operazioni senza interruzioni**

La capacità di eseguire importanti operazioni di gestione e aggiornamento di ONTAP e di resistere agli errori dei nodi senza interrompere le applicazioni client. Questo termine si riferisce alla raccolta di funzionalità di Takeover senza interruzioni, upgrade senza interruzioni e migrazione senza interruzioni nel loro complesso.

- **Upgrade senza interruzioni**

Possibilità di aggiornare l'hardware o il software del nodo senza interruzioni dell'applicazione.

- **Spostamento del volume senza interruzioni**

Possibilità di spostare liberamente un volume nel cluster senza interrompere le applicazioni che utilizzano il volume. Per le connessioni SMB, tutte le versioni di SMB supportano spostamenti di volume senza interruzioni.

- **Handle persistenti**

Proprietà di SMB 3.0 che consente alle connessioni continuamente disponibili di riconnettersi in modo trasparente al server CIFS in caso di disconnessione. In modo analogo ai gestori a lunga durata, i gestori persistenti vengono mantenuti dal server CIFS per un periodo di tempo successivo alla perdita della comunicazione con il client di connessione. Tuttavia, le maniglie persistenti hanno una maggiore resilienza rispetto alle maniglie resistenti. Oltre a dare al client la possibilità di recuperare l'handle in una finestra di 60 secondi dopo la riconnessione, il server CIFS nega l'accesso a tutti gli altri client che richiedono l'accesso al file durante la finestra di 60 secondi.

Le informazioni sugli handle persistenti vengono mirrorate sullo storage persistente del partner SFO, che consente ai client con handle persistenti disconnessi di recuperare gli handle durevoli dopo un evento in cui il partner SFO assume la proprietà dello storage del nodo. Oltre a fornire operazioni senza interruzioni in caso di spostamenti LIF (che supportano la gestione durevole), le maniglie persistenti forniscono operazioni senza interruzioni per il takeover, il giveback e il trasferimento di aggregati.

- **Giveback SFO**

Restituzione degli aggregati nelle sedi domestiche durante il ripristino da un evento di Takeover.

- **Coppia SFO**

Coppia di nodi i cui controller sono configurati per fornire dati l'uno per l'altro se uno dei due nodi smette di funzionare. A seconda del modello di sistema, entrambi i controller possono trovarsi in un unico chassis o in uno chassis separato. Nota come coppia ha in un cluster a due nodi.

- **Takeover**

Il processo mediante il quale il partner assume il controllo dello storage in caso di guasto del proprietario

principale dello storage. Nel contesto di SFO, il failover e il takeover sono sinonimi.

In che modo la funzionalità SMB 3.0 supporta operazioni senza interruzioni sulle condivisioni SMB

SMB 3.0 offre funzionalità cruciali che consentono il supporto per operazioni senza interruzioni per Hyper-V e SQL Server su condivisioni SMB. Ciò include `continuously-available` Condividere la proprietà e un tipo di handle di file noto come *handle persistente* che consentono ai client SMB di recuperare lo stato di apertura del file e ristabilire in modo trasparente le connessioni SMB.

Gli handle persistenti possono essere concessi ai client SMB 3.0 che si connettono a una condivisione con il set di proprietà di condivisione continuamente disponibile. Se la sessione SMB viene disconnessa, il server CIFS conserva le informazioni sullo stato di handle persistente. Il server CIFS blocca le altre richieste client durante il periodo di 60 secondi in cui il client può riconnettersi, consentendo così al client con l'handle persistente di recuperare l'handle dopo una disconnessione dalla rete. I client con handle persistenti possono riconnettersi utilizzando una delle LIF di dati sulla macchina virtuale di storage (SVM), riconnettendosi attraverso lo stesso LIF o attraverso un LIF diverso.

Il trasferimento, il takeover e il giveback degli aggregati avvengono tra coppie SFO. Per gestire senza problemi la disconnessione e la riconnessione delle sessioni con file con handle persistenti, il nodo partner conserva una copia di tutte le informazioni persistenti sul blocco degli handle. Sia che l'evento sia pianificato o non pianificato, il partner SFO può gestire senza interruzioni le riconnesse persistenti dell'handle. Con questa nuova funzionalità, le connessioni SMB 3.0 al server CIFS possono eseguire il failover trasparente e senza interruzioni su un altro LIF di dati assegnato a SVM in eventi che tradizionalmente hanno subito interruzioni.

Sebbene l'utilizzo di handle persistenti consenta al server CIFS di eseguire il failover in modo trasparente sulle connessioni SMB 3.0, se un errore causa il failover dell'applicazione Hyper-V su un altro nodo nel cluster di Windows Server, il client non ha alcun modo per recuperare gli handle di file di questi handle disconnessi. In questo scenario, gli handle di file in stato disconnesso possono potenzialmente bloccare l'accesso all'applicazione Hyper-V se viene riavviata su un nodo diverso. "failover Clustering" fa parte di SMB 3.0 che risolve questo scenario fornendo un meccanismo per invalidare handle obsoleti e in conflitto. Grazie a questo meccanismo, un cluster Hyper-V può essere ripristinato rapidamente in caso di guasto dei nodi del cluster Hyper-V.

Cosa fa il protocollo Witness per migliorare il failover trasparente

Il protocollo Witness offre funzionalità di failover client avanzate per le condivisioni SMB 3.0 a disponibilità continua (condivisioni CA). La funzione Witness facilita un failover più rapido perché evita il periodo di failover di LIF. Notifica agli application server quando un nodo non è disponibile senza dover attendere il timeout della connessione SMB 3.0.

Il failover è perfetto, con le applicazioni in esecuzione sul client che non sono a conoscenza del failover. Se il server di controllo del mirroring non è disponibile, le operazioni di failover continuano a essere eseguite correttamente, ma il failover senza server di controllo del mirroring è meno efficiente.

Il failover avanzato di Witness è possibile quando vengono soddisfatti i seguenti requisiti:

- Può essere utilizzato solo con server CIFS con funzionalità SMB 3.0 e SMB 3.0 abilitati.
- Le condivisioni devono utilizzare SMB 3.0 con la proprietà di condivisione a disponibilità continua impostata.
- Il partner SFO del nodo a cui sono connessi i server applicazioni deve avere almeno una LIF di dati

operativi assegnata alla macchina virtuale di storage (SVM) che ospita i dati per i server applicazioni.



Il protocollo Witness opera tra coppie SFO. Poiché i LIF possono migrare a qualsiasi nodo all'interno del cluster, qualsiasi nodo potrebbe dover essere il testimone per il partner SFO. Il protocollo Witness non è in grado di fornire un failover rapido delle connessioni SMB su un dato nodo se la SVM che ospita i dati per gli application server non dispone di una LIF di dati attiva sul nodo partner. Pertanto, ogni nodo del cluster deve disporre di almeno una LIF di dati per ogni SVM che ospita una di queste configurazioni.

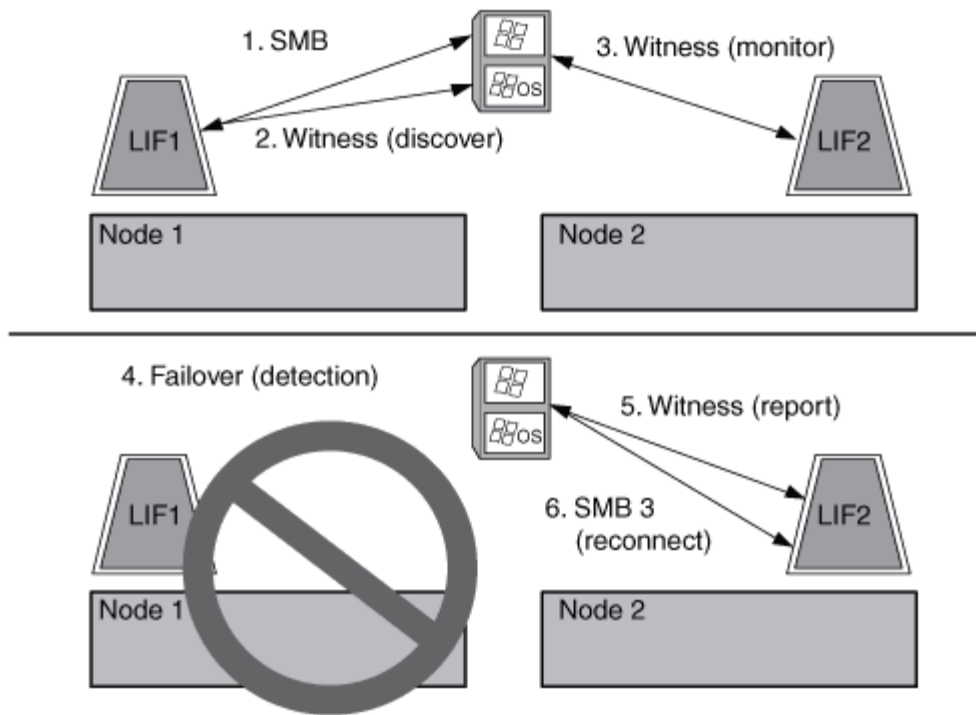
- I server applicazioni devono connettersi al server CIFS utilizzando il nome del server CIFS memorizzato in DNS invece di utilizzare singoli indirizzi IP LIF.

Funzionamento del protocollo Witness

ONTAP implementa il protocollo Witness utilizzando il partner SFO di un nodo come Witness. In caso di guasto, il partner rileva rapidamente il guasto e notifica il client SMB.

Il protocollo Witness offre un failover avanzato utilizzando il seguente processo:

1. Quando l'application server stabilisce una connessione SMB continuamente disponibile al Node1, il server CIFS informa l'application server che il server di controllo è disponibile.
2. Il server applicazioni richiede gli indirizzi IP del server di controllo del mirroring dal Node1 e riceve un elenco di indirizzi IP LIF dei dati Node2 (il partner SFO) assegnati alla macchina virtuale di storage (SVM).
3. Il server applicazioni sceglie uno degli indirizzi IP, crea una connessione testimone a Node2 e registra per ricevere una notifica se la connessione continuamente disponibile su Node1 deve spostarsi.
4. Se si verifica un evento di failover su Node1, Witness facilita gli eventi di failover, ma non è coinvolto nel giveback.
5. Il server di controllo del mirroring rileva l'evento di failover e notifica al server applicazioni tramite la connessione di controllo del mirroring che la connessione SMB deve spostarsi su Node2.
6. L'application server sposta la sessione SMB su Node2 e ripristina la connessione senza interrompere l'accesso al client.



Backup basati su condivisione con Remote VSS

Backup basati su condivisione con panoramica di Remote VSS

È possibile utilizzare Remote VSS per eseguire backup basati su condivisioni di file di macchine virtuali Hyper-V memorizzati su un server CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) è un'estensione dell'infrastruttura Microsoft VSS esistente. Con Remote VSS, Microsoft ha esteso l'infrastruttura VSS per supportare la copia shadow delle condivisioni SMB. Inoltre, le applicazioni server come Hyper-V possono memorizzare i file VHD nelle condivisioni di file SMB. Con queste estensioni, è possibile creare copie shadow coerenti con le applicazioni per le macchine virtuali che memorizzano i file di dati e di configurazione su condivisioni.

Concetti VSS remoti

È necessario conoscere alcuni concetti necessari per comprendere in che modo i servizi di backup con configurazioni Hyper-V su SMB utilizzano il servizio Remote VSS (Volume Shadow Copy Service).

- **VSS (Volume Shadow Copy Service)**

Tecnologia Microsoft utilizzata per eseguire copie di backup o snapshot di dati su un volume specifico in un determinato momento. Il sistema VSS coordina tra server di dati, applicazioni di backup e software di gestione dello storage per supportare la creazione e la gestione di backup coerenti.

- **VSS remoto (Remote Volume Shadow Copy Service)**

Tecnologia Microsoft utilizzata per eseguire copie di backup basate su condivisione dei dati in uno stato coerente con i dati in un momento specifico in cui si accede ai dati tramite le condivisioni SMB 3.0. Noto anche come *Volume Shadow Copy Service*.

- **Copia shadow**

Un insieme duplicato di dati contenuti nella condivisione in un istante di tempo ben definito. Le copie shadow vengono utilizzate per creare backup point-in-time coerenti dei dati, consentendo al sistema o alle applicazioni di continuare ad aggiornare i dati sui volumi originali.

- **Set di copie shadow**

Una raccolta di una o più copie shadow, con ciascuna copia shadow corrispondente a una condivisione. Le copie shadow all'interno di un set di copie shadow rappresentano tutte le condivisioni di cui è necessario eseguire il backup nella stessa operazione. Il client VSS nell'applicazione abilitata per VSS identifica le copie shadow da includere nel set.

- **Recupero automatico del set di copie shadow**

Parte del processo di backup per le applicazioni di backup remote abilitate per VSS in cui la directory di replica contenente le copie shadow viene resa coerente point-in-time. All'inizio del backup, il client VSS sull'applicazione attiva l'applicazione per prendere punti di controllo software sui dati pianificati per il backup (i file della macchina virtuale nel caso di Hyper-V). Il client VSS consente quindi alle applicazioni di continuare. Una volta creato il set di copie shadow, Remote VSS rende il set di copie shadow scrivibile ed espone la copia scrivibile alle applicazioni. L'applicazione prepara il set di copie shadow per il backup eseguendo un ripristino automatico utilizzando il checkpoint del software preso in precedenza. Il ripristino automatico porta le copie shadow in uno stato coerente srotolando le modifiche apportate ai file e alle directory dalla creazione del checkpoint. Il ripristino automatico è un passaggio opzionale per i backup abilitati per VSS.

- **ID copia shadow**

GUID che identifica in modo univoco una copia shadow.

- **ID set copia shadow**

GUID che identifica in modo univoco una raccolta di ID di copia shadow sullo stesso server.

- **SnapManager per Hyper-V**

Il software che automatizza e semplifica le operazioni di backup e ripristino per Microsoft Windows Server 2012 Hyper-V. SnapManager per Hyper-V utilizza VSS remoto con recovery automatico per eseguire il backup dei file Hyper-V sulle condivisioni SMB.

Informazioni correlate

[Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB](#)

[Backup basati su condivisione con Remote VSS](#)

Esempio di struttura di directory utilizzata da Remote VSS

Il VSS remoto attraversa la struttura di directory che memorizza i file delle macchine virtuali Hyper-V durante la creazione di copie shadow. È importante capire quale sia la struttura di directory appropriata, in modo da poter creare correttamente i backup dei file delle macchine virtuali.

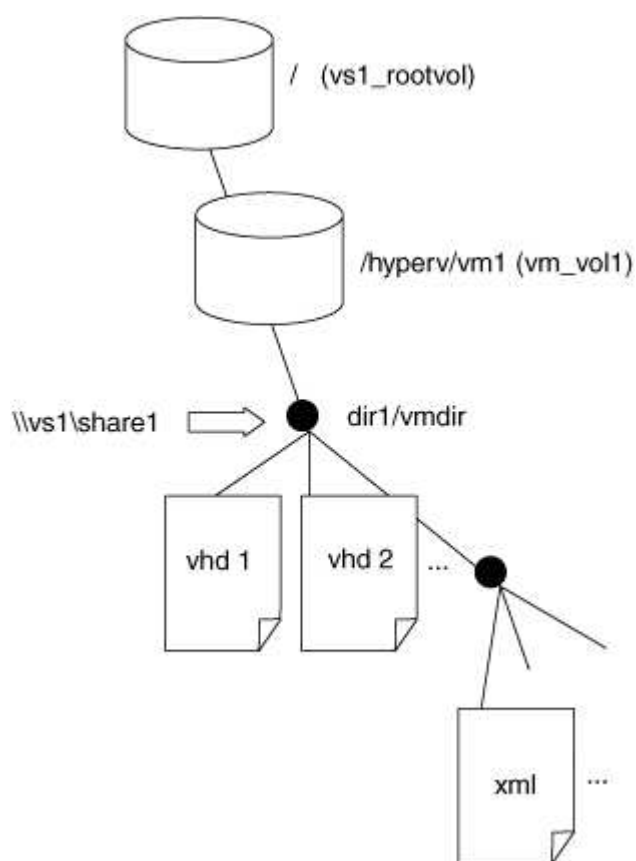
Una struttura di directory supportata per la creazione di copie shadow è conforme ai seguenti requisiti:

- Solo le directory e i file regolari sono presenti all'interno della struttura di directory utilizzata per memorizzare i file delle macchine virtuali.

La struttura di directory non contiene giunzioni, collegamenti o file non regolari.

- Tutti i file di una macchina virtuale risiedono all'interno di una singola condivisione.
- La struttura di directory utilizzata per memorizzare i file delle macchine virtuali non supera la profondità configurata della directory di copia shadow.
- La directory principale della condivisione contiene solo i file o le directory delle macchine virtuali.

Nella seguente illustrazione, il volume denominato `vm_vol1` viene creato con un punto di giunzione in `/hyperv/vm1` Su storage virtual machine (SVM) `vs1`. Le sottodirectory che contengono i file della macchina virtuale vengono create sotto il punto di giunzione. Ai file della macchina virtuale del server Hyper-V si accede tramite `share1` che ha il percorso `/hyperv/vm1/dir1/vmdir`. Il servizio di copia shadow crea copie shadow di tutti i file della macchina virtuale contenuti nella struttura di directory sotto `share1` (fino alla profondità configurata della directory di copia shadow).



In che modo SnapManager per Hyper-V gestisce backup remoti basati su VSS per Hyper-V su SMB

È possibile utilizzare SnapManager per Hyper-V per gestire i servizi di backup basati su VSS remoto. L'utilizzo del servizio di backup gestito di SnapManager per Hyper-V offre vantaggi per creare set di backup efficienti in termini di spazio.

Le ottimizzazioni di SnapManager per i backup gestiti da Hyper-V includono quanto segue:

- L'integrazione di SnapDrive con ONTAP offre l'ottimizzazione delle performance quando si scopre la posizione di condivisione delle PMI.

ONTAP fornisce a SnapDrive il nome del volume in cui risiede la condivisione.

- SnapManager per Hyper-V specifica l'elenco dei file delle macchine virtuali nelle condivisioni SMB che il servizio di copia shadow deve copiare.

Fornendo un elenco mirato di file di macchine virtuali, il servizio di copia shadow non deve creare copie shadow di tutti i file nella condivisione.

- La macchina virtuale per lo storage (SVM) conserva le copie Snapshot per SnapManager per Hyper-V da utilizzare per i ripristini.

Non esiste alcuna fase di backup. Il backup è la copia Snapshot efficiente in termini di spazio.

SnapManager per Hyper-V offre funzionalità di backup e ripristino per HyperV su SMB utilizzando il seguente processo:

1. Preparazione per l'operazione di copia shadow

Il client VSS di SnapManager per l'applicazione Hyper-V imposta il set di copie shadow. Il client VSS raccoglie informazioni sulle condivisioni da includere nel set di copie shadow e fornisce queste informazioni a ONTAP. Un set potrebbe contenere una o più copie shadow e una copia shadow corrisponde a una condivisione.

2. Creazione del set di copie shadow (se viene utilizzato il ripristino automatico)

Per ogni condivisione inclusa nel set di copie shadow, ONTAP crea una copia shadow e la rende scrivibile.

3. Esposizione del set di copie shadow

Dopo che ONTAP ha creato le copie shadow, queste vengono esposte a SnapManager per Hyper-V in modo che i writer VSS dell'applicazione possano eseguire il ripristino automatico.

4. Ripristino automatico del set di copie shadow

Durante la creazione del set di copie shadow, vi è un periodo di tempo in cui si verificano modifiche attive ai file inclusi nel set di backup. I writer VSS dell'applicazione devono aggiornare le copie shadow per assicurarsi che si trovino in uno stato completamente coerente prima del backup.



Il modo in cui viene eseguito il ripristino automatico è specifico dell'applicazione. Il VSS remoto non è coinvolto in questa fase.

5. Completamento e pulizia del set di copie shadow

Il client VSS notifica a ONTAP una volta completato il ripristino automatico. Il set di copie shadow viene reso di sola lettura e quindi pronto per il backup. Quando si utilizza SnapManager per Hyper-V per il backup, i file in una copia Snapshot diventano il backup; pertanto, per la fase di backup, viene creata una copia Snapshot per ogni volume contenente condivisioni nel set di backup. Una volta completato il backup, il set di copie shadow viene rimosso dal server CIFS.

Come viene utilizzato l'offload delle copie ODX con Hyper-V e SQL Server su condivisioni SMB

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. L'offload delle copie ODX di ONTAP offre vantaggi in termini di performance quando si eseguono operazioni di copia sul server applicativo rispetto all'installazione SMB.

Nei trasferimenti di file non ODX, i dati vengono letti dal server CIFS di origine e trasferiti attraverso la rete al computer client. Il computer client trasferisce di nuovo i dati sulla rete al server CIFS di 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.

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.
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.

- Tra volumi, stesso nodo, stessa SVM (Storage Virtual Machine)

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.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni Hyper-V includono:

- 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.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni SQL Server includono:

- È possibile utilizzare l'offload delle copie di ODX per esportare e importare i database SQL Server tra le condivisioni SMB mappate o tra le condivisioni SMB e le LUN iSCSI connesse all'interno dello stesso cluster.
- L'offload delle copie ODX viene utilizzato per le esportazioni e le importazioni dei database se lo storage di origine e di destinazione si trova nello stesso cluster.

Requisiti di configurazione e considerazioni

ONTAP e requisiti di licenza

Quando si creano soluzioni SQL Server o Hyper-V su PMI, è necessario conoscere alcuni requisiti di licenza e ONTAP per operazioni senza interruzioni su SVM.

Requisiti di versione di ONTAP

- Hyper-V su SMB

ONTAP supporta operazioni senza interruzioni sulle condivisioni SMB per Hyper-V in esecuzione su Windows 2012 o versioni successive.

- SQL Server su SMB

ONTAP supporta operazioni senza interruzioni su condivisioni SMB per SQL Server 2012 o versioni successive in esecuzione su Windows 2012 o versioni successive.

Per informazioni aggiornate sulle versioni supportate di ONTAP, Windows Server e SQL Server per operazioni senza interruzioni sulle condivisioni SMB, consulta la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

Requisiti di licenza

Sono necessarie le seguenti licenze:

- CIFS
- FlexClone (solo per Hyper-V su SMB)

Questa licenza è necessaria se si utilizza VSS remoto per i backup. Il servizio di copia shadow utilizza FlexClone per creare copie point-in-time dei file che vengono poi utilizzate durante la creazione di un backup.

Una licenza FlexClone è opzionale se si utilizza un metodo di backup che non utilizza Remote VSS.

La licenza FlexClone è inclusa in "ONTAP uno". Se non si dispone di ONTAP ONE, è necessario ["verificare che le licenze richieste siano installate"](#), e, se necessario, ["installarli"](#).

Requisiti LIF di rete e dati

Quando si creano configurazioni SQL Server o Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti LIF di rete e dati).

Requisiti del protocollo di rete

- Sono supportate le reti IPv4 e IPv6.
- È richiesto SMB 3.0 o versione successiva.

SMB 3.0 offre le funzionalità necessarie per creare le connessioni SMB continuamente disponibili necessarie per offrire operazioni senza interruzioni.

- I server DNS devono contenere voci che associano il nome del server CIFS agli indirizzi IP assegnati ai file LIF dei dati sulla macchina virtuale di storage (SVM).

I server applicativi Hyper-V o SQL Server in genere effettuano più connessioni su più file di dati LIF quando accedono a macchine virtuali o file di database. Per una corretta funzionalità, i server applicazioni devono stabilire connessioni SMB multiple utilizzando il nome del server CIFS invece di effettuare connessioni multiple a più indirizzi IP univoci.

Il server Witness richiede inoltre l'utilizzo del nome DNS del server CIFS invece di singoli indirizzi IP LIF.

A partire da ONTAP 9.4, è possibile migliorare il throughput e la tolleranza agli errori per Hyper-V e SQL Server sulle configurazioni SMB attivando SMB multicanale. A tale scopo, è necessario implementare più NIC 1G, 10G o superiori nel cluster e nei client.

Requisiti Data LIF

- La SVM che ospita l'application server sulla soluzione SMB deve avere almeno un LIF di dati operativi su ogni nodo del cluster.

Le LIF dei dati SVM possono eseguire il failover su altre porte dati all'interno del cluster, inclusi i nodi che attualmente non ospitano dati a cui accedono i server applicazioni. Inoltre, poiché il nodo di controllo è sempre il partner SFO di un nodo a cui è connesso l'application server, ogni nodo del cluster è un potenziale nodo di controllo.

- I file LIF dei dati non devono essere configurati per il ripristino automatico.

Dopo un takeover o un evento di giveback, è necessario ripristinare manualmente le LIF dei dati alle porte home.

- Tutti gli indirizzi IP LIF dei dati devono avere una voce nel DNS e tutte le voci devono essere risolte nel nome del server CIFS.

I server applicazioni devono connettersi alle condivisioni SMB utilizzando il nome del server CIFS. Non è necessario configurare i server applicazioni per effettuare connessioni utilizzando gli indirizzi IP LIF.

- Se il nome del server CIFS è diverso dal nome SVM, le voci DNS devono essere risolte nel nome del server CIFS.

Requisiti di volume e server SMB per Hyper-V su SMB

Quando si creano configurazioni Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti di volume e server SMB.

Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

Questa opzione è attivata per impostazione predefinita.

- L'opzione predefinita del server CIFS dell'utente UNIX deve essere configurata con un account utente UNIX valido.

I server applicazioni utilizzano l'account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l'utente Windows si logga correttamente a un account utente UNIX o all'account utente UNIX predefinito, ONTAP deve essere in grado di mappare l'account del computer dell'applicazione server all'account utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

Se si desidera utilizzare riferimenti automatici ai nodi per l'accesso a dati diversi dai file macchina Hyper-V, è necessario creare una SVM separata per tali dati.

- L'autenticazione Kerberos e NTLM deve essere consentita nel dominio a cui appartiene il server SMB.

ONTAP non annuncia il servizio Kerberos per il VSS remoto; pertanto, il dominio deve essere impostato su Consenti NTLM.

- La funzionalità di copia shadow deve essere attivata.

Questa funzionalità è attivata per impostazione predefinita.

- L'account di dominio Windows utilizzato dal servizio di copia shadow per la creazione delle copie shadow deve essere membro del gruppo BUILTIN/Administrators locale del server SMB o del gruppo BUILTIN/Backup Operators.

Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e

successivamente modificati in stile di sicurezza NTFS.

- Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume.

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo requisito si applica solo alle copie shadow con ripristino automatico.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti di volume e server SMB per SQL Server su SMB

Quando si creano configurazioni SQL Server su SMB per operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti di volume e server SMB.

Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

Questa opzione è attivata per impostazione predefinita.

- L'opzione predefinita del server CIFS dell'utente UNIX deve essere configurata con un account utente UNIX valido.

I server applicazioni utilizzano l'account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l'utente Windows si logga correttamente a un account utente UNIX o all'account utente UNIX predefinito, ONTAP deve essere in grado di mappare l'account del computer dell'applicazione server all'account utente UNIX predefinito.

Inoltre, SQL Server utilizza un utente di dominio come account del servizio SQL Server. L'account di servizio deve anche essere associato all'utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

Se si desidera utilizzare riferimenti automatici ai nodi per l'accesso a dati diversi dai file di database di SQL Server, è necessario creare una SVM separata per tali dati.

- All'account utente Windows utilizzato per l'installazione di SQL Server su ONTAP deve essere assegnato il privilegio SeSecurityPrivilege.

Questo privilegio viene assegnato al gruppo BUILTIN/Administrators locale del server SMB.

Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume

misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni di backup del plug-in SnapCenter per SQL Server, è necessario disporre di spazio disponibile sufficiente sul volume.

Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti e considerazioni di condivisione continuamente disponibili per Hyper-V su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni Hyper-V su SMB che supportano operazioni senza interruzioni, è necessario essere consapevoli di determinati requisiti e considerazioni.

Condividere i requisiti

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà Continuously Available (disponibilità continua).

Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS, non è possibile inserire i file Hyper-V in condivisioni che contengono giunzioni.

In caso di ripristino automatico, la creazione della copia shadow non riesce se viene rilevata una giunzione durante l'attraversamento della condivisione. In caso di non ripristino automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS con il ripristino automatico, non è possibile inserire i file Hyper-V in condivisioni contenenti quanto segue:

- Symlink, hardlink o widelink
- File non regolari

La creazione della copia shadow non riesce se nella copia shadow sono presenti collegamenti o file non regolari. Questo requisito si applica solo alle copie shadow con ripristino automatico.

- Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume (solo per Hyper-V su SMB).

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo

requisito si applica solo alle copie shadow con ripristino automatico.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
 - Home directory
 - Caching degli attributi
 - BranchCache

Considerazioni

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni Hyper-V su SMB:
 - Controllo
 - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` parametro impostato su `Yes`.

Requisiti e considerazioni di condivisione continuamente disponibili per SQL Server su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni SQL Server su SMB che supportano operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti e considerazioni.

Condividere i requisiti

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire operazioni senza interruzioni per i server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per operazioni senza interruzioni sulle condivisioni SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per operazioni senza interruzioni sulle condivisioni SMB, è necessario posizionare manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà `Continuously Available` (disponibilità continua).

Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni del plug-in SnapCenter per SQL Server, è necessario disporre di

spazio disponibile sufficiente sul volume.

Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
 - Home directory
 - Caching degli attributi
 - BranchCache

Condividere le considerazioni

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni SQL Server su SMB:
 - Controllo
 - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` condividere il set di proprietà.

Considerazioni sul VSS remoto per le configurazioni Hyper-V su SMB

Quando si utilizzano soluzioni di backup abilitate per VSS remoto per configurazioni Hyper-V su SMB, è necessario tenere presenti alcune considerazioni.

Considerazioni generali su Remote VSS

- È possibile configurare un massimo di 64 condivisioni per server applicazioni Microsoft.

L'operazione di copia shadow non riesce se sono presenti più di 64 condivisioni in un set di copie shadow. Si tratta di un requisito Microsoft.
- È consentito un solo set di copie shadow attive per server CIFS.

Un'operazione di copia shadow non riesce se è in corso un'operazione di copia shadow sullo stesso server CIFS. Si tratta di un requisito Microsoft.
- Non sono consentite giunzioni all'interno della struttura di directory in cui Remote VSS crea una copia shadow.
 - In caso di ripristino automatico, la creazione della copia shadow non riesce se si incontra una giunzione durante l'attraversamento della condivisione.
 - Nel caso di recovery non automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

Considerazioni sul VSS remoto valide solo per le copie shadow con ripristino automatico

Alcuni limiti si applicano solo alle copie shadow con ripristino automatico.

- Per la creazione delle copie shadow è consentita una profondità massima di directory di cinque sottodirectory.

Questa è la profondità della directory in cui il servizio di copia shadow crea un set di backup delle copie shadow. La creazione della copia shadow non riesce se le directory contenenti il file della macchina virtuale sono nidificate più in profondità di cinque livelli. Questa opzione consente di limitare l'attraversamento della directory durante la clonazione della condivisione. È possibile modificare la profondità massima della directory utilizzando un'opzione del server CIFS.

- La quantità di spazio disponibile sul volume deve essere adeguata.

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow.

- Non sono consentiti collegamenti o file non regolari all'interno della struttura di directory in cui Remote VSS crea una copia shadow.

La creazione della copia shadow non riesce se nella condivisione sono presenti collegamenti o file non regolari alla copia shadow. Il processo di clonazione non li supporta.

- Non sono consentiti ACL NFSv4 nelle directory.

Sebbene la creazione delle copie shadow conservi gli ACL NFSv4 nei file, gli ACL NFSv4 nelle directory vengono persi.

- È consentito creare un set di copie shadow per un massimo di 60 secondi.

Le specifiche Microsoft consentono di creare il set di copie shadow per un massimo di 60 secondi. Se il client VSS non riesce a creare il set di copie shadow entro questo intervallo di tempo, l'operazione di copia shadow non riesce; pertanto, questo limita il numero di file in un set di copie shadow. Il numero effettivo di file o macchine virtuali che possono essere inclusi in un set di backup varia; tale numero dipende da molti fattori e deve essere determinato per ogni ambiente del cliente.

Requisiti di offload delle copie ODX per SQL Server e Hyper-V su SMB

L'offload delle copie ODX deve essere attivato se si desidera migrare i file delle macchine virtuali o esportare e importare i file di database direttamente dall'origine alla posizione di storage di destinazione senza inviare dati attraverso i server applicazioni. È necessario comprendere alcuni requisiti sull'utilizzo dell'offload delle copie ODX con SQL Server e Hyper-V su soluzioni SMB.

L'utilizzo dell'offload delle copie di ODX offre un significativo vantaggio in termini di performance. Questa opzione del server CIFS è attivata per impostazione predefinita.

- SMB 3.0 deve essere abilitato per utilizzare l'offload delle copie ODX.
- I volumi di origine devono essere di almeno 1.25 GB.
- La deduplica deve essere attivata sui volumi utilizzati con l'offload delle copie.
- 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

- Per utilizzare l'offload delle copie di ODX per migrare i guest Hyper-V all'interno e tra i dischi, i server Hyper-V devono essere configurati per l'utilizzo di dischi SCSI.

L'impostazione predefinita prevede la configurazione dei dischi IDE, ma l'offload delle copie ODX non funziona quando i guest vengono migrati se i dischi vengono creati utilizzando dischi IDE.

Raccomandazioni per le configurazioni SQL Server e Hyper-V su SMB

Per essere sicuri che le configurazioni di SQL Server e Hyper-V su SMB siano solide e operative, è necessario conoscere le Best practice consigliate per la configurazione delle soluzioni.

Raccomandazioni generali

- Separare i file del server applicazioni dai dati generali dell'utente.

Se possibile, dedicare un'intera macchina virtuale di storage (SVM) e il relativo storage ai dati dell'application server.

- Per ottenere performance ottimali, non abilitare la firma SMB sulle SVM utilizzate per memorizzare i dati dell'application server.
- Per ottenere le migliori performance e una maggiore tolleranza agli errori, abilitare SMB multicanale per fornire più connessioni tra ONTAP e client in una singola sessione SMB.
- Non creare condivisioni continuamente disponibili su condivisioni diverse da quelle utilizzate nella configurazione Hyper-V o SQL Server su SMB.
- Disattiva la notifica delle modifiche sulle condivisioni utilizzate per la disponibilità continua.
- Non eseguire uno spostamento del volume contemporaneamente al trasferimento dell'aggregato (ARL) perché ARL ha fasi che interrompono alcune operazioni.
- Per le soluzioni Hyper-V su SMB, utilizzare dischi iSCSI in-guest durante la creazione di macchine virtuali in cluster. Condiviso .VHDX I file non sono supportati per Hyper-V su SMB nelle condivisioni SMB ONTAP.

Pianificare la configurazione di Hyper-V o SQL Server su SMB

Completare il foglio di lavoro per la configurazione del volume

Il foglio di lavoro offre un modo semplice per registrare i valori necessari per la creazione di volumi per le configurazioni SQL Server e Hyper-V su SMB.

Per ciascun volume, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

Il nome SVM è lo stesso per tutti i volumi.

- Nome del volume
- Nome dell'aggregato

È possibile creare volumi su aggregati situati su qualsiasi nodo del cluster.

- Dimensione
- Percorso di giunzione

Quando si creano volumi utilizzati per memorizzare i dati dell'application server, tenere presente quanto segue:

- Se il volume root non dispone di uno stile di protezione NTFS, è necessario specificare lo stile di protezione come NTFS quando si crea il volume.

Per impostazione predefinita, i volumi ereditano lo stile di sicurezza del volume root SVM.

- I volumi devono essere configurati con la garanzia di spazio del volume predefinita.
- Facoltativamente, è possibile configurare l'impostazione di gestione automatica dello spazio.
- Impostare l'opzione che determina la riserva di spazio di copia Snapshot su 0.
- Il criterio Snapshot applicato al volume deve essere disattivato.

Se il criterio Snapshot SVM è disattivato, non è necessario specificare un criterio Snapshot per i volumi. I volumi ereditano la policy Snapshot per SVM. Se il criterio Snapshot per SVM non è disattivato ed è configurato per creare copie Snapshot, è necessario specificare un criterio Snapshot a livello di volume e tale criterio deve essere disattivato. I backup abilitati al servizio di copia shadow e i backup di SQL Server gestiscono la creazione e l'eliminazione delle copie Snapshot.

- Non è possibile configurare i mirror di condivisione del carico per i volumi.

I percorsi di giunzione su cui si intende creare le condivisioni utilizzate dai server applicazioni devono essere scelti in modo che non vi siano volumi congiunti al di sotto del punto di ingresso della condivisione.

Ad esempio, se si desidera memorizzare i file delle macchine virtuali su quattro volumi denominati "vol1", "vol2", "vol3" e "vol4", è possibile creare lo spazio dei nomi mostrato nell'esempio. È quindi possibile creare condivisioni per i server applicazioni nei seguenti percorsi: /data1/vol1, /data1/vol2, /data2/vol3, e, /data2/vol4.

Vserver	Volume	Junction		Junction	
		Active	Junction Path	Path	Source
vs1	data1	true	/data1	RW_volume	
vs1	vol1	true	/data1/vol1	RW_volume	
vs1	vol2	true	/data1/vol2	RW_volume	
vs1	data2	true	/data2	RW_volume	
vs1	vol3	true	/data2/vol3	RW_volume	
vs1	vol4	true	/data2/vol4	RW_volume	

Tipi di informazioni	Valori
Volume 1: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 2: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 3: Nome del volume, aggregato, dimensione, percorso di giunzione	

Tipi di informazioni	Valori
<i>Volume 4: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 5: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 6: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volumi aggiuntivi: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	

Completare il foglio di lavoro per la configurazione della condivisione SMB

Utilizzare questo foglio di lavoro per registrare i valori necessari per la creazione di condivisioni SMB continuamente disponibili per le configurazioni SQL Server e Hyper-V su SMB.

Informazioni sulle proprietà delle condivisioni SMB e sulle impostazioni di configurazione

Per ciascuna condivisione, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

Il nome SVM è lo stesso per tutte le condivisioni

- Nome di condivisione
- Percorso
- Condividere le proprietà

È necessario configurare le seguenti due proprietà di condivisione:

- `oplocks`
- `continuously-available`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
 - I collegamenti simbolici devono essere disattivati (il valore per `-symlink-properties` il parametro deve essere nullo [""]).

Informazioni sui percorsi di condivisione

Se si utilizza il VSS remoto per eseguire il backup dei file Hyper-V, è importante scegliere i percorsi di condivisione da utilizzare per le connessioni SMB dai server Hyper-V alle posizioni di storage in cui sono

memorizzati i file delle macchine virtuali. Sebbene sia possibile creare condivisioni in qualsiasi punto dello spazio dei nomi, i percorsi per le condivisioni utilizzati dai server Hyper-V non devono contenere volumi congiunti. Le operazioni di copia shadow non possono essere eseguite su percorsi di condivisione che contengono punti di giunzione.

SQL Server non è in grado di incrociare le giunzioni durante la creazione della struttura di directory del database. Non creare percorsi di condivisione per SQL Server che contengono punti di giunzione.

Ad esempio, dato lo spazio dei nomi mostrato, se si desidera memorizzare i file di macchine virtuali o i file di database sui volumi “vol1”, “vol2”, “vol3” e “vol4”, è necessario creare condivisioni per i server applicazioni nei seguenti percorsi: /data1/vol1, /data1/vol2, /data2/vol3, e. /data2/vol4.

Vserver	Volume	Junction		Junction Path Source
		Active	Junction Path	
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume



Sebbene sia possibile creare condivisioni su /data1 e. /data2 percorsi per la gestione amministrativa, non è necessario configurare i server applicazioni per utilizzare tali condivisioni per memorizzare i dati.

Foglio di lavoro per la pianificazione

Tipi di informazioni	Valori
Volume 1: Nome e percorso della condivisione SMB	
Volume 2: Nome e percorso della condivisione SMB	
Volume 3: Nome e percorso della condivisione SMB	
Volume 4: Nome e percorso della condivisione SMB	
Volume 5: Nome e percorso della condivisione SMB	
Volume 6: Nome e percorso della condivisione SMB	
Volume 7: Nome e percorso della condivisione SMB	
Volumi aggiuntivi: Nomi e percorsi di condivisione SMB	

Creazione di configurazioni ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB

Crea configurazioni ONTAP per operazioni senza interruzioni con la panoramica di Hyper-V e SQL Server su SMB

Per preparare le installazioni di ONTAP e Hyper-V, è necessario eseguire diverse operazioni di configurazione di SQL Server che forniscono operazioni senza interruzioni su SMB.

Prima di creare la configurazione ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB, è necessario completare le seguenti attività:

- I servizi Time devono essere impostati sul cluster.
- È necessario configurare la rete per SVM.
- È necessario creare la SVM.
- Le interfacce Data LIF devono essere configurate su SVM.
- Il DNS deve essere configurato sulla SVM.
- I servizi Names desiderati devono essere impostati per la SVM.
- È necessario creare il server SMB.

Informazioni correlate

[Pianificare la configurazione di Hyper-V o SQL Server su SMB](#)

[Requisiti di configurazione e considerazioni](#)

Verificare che sia consentita l'autenticazione Kerberos e NTLMv2 (Hyper-V su condivisioni SMB)

Le operazioni senza interruzioni per Hyper-V su SMB richiedono che il server CIFS su una SVM dati e il server Hyper-V consentano l'autenticazione Kerberos e NTLMv2. È necessario verificare le impostazioni sul server CIFS e sui server Hyper-V che controllano i metodi di autenticazione consentiti.

A proposito di questa attività

L'autenticazione Kerberos è necessaria quando si effettua una connessione di condivisione continuamente disponibile. Parte del processo VSS remoto utilizza l'autenticazione NTLMv2. Pertanto, le connessioni che utilizzano entrambi i metodi di autenticazione devono essere supportate per le configurazioni Hyper-V su SMB.

È necessario configurare le seguenti impostazioni per consentire l'autenticazione Kerberos e NTLMv2:

- I criteri di esportazione per SMB devono essere disattivati sulla macchina virtuale di storage (SVM).

L'autenticazione Kerberos e NTLMv2 è sempre abilitata sulle SVM, ma è possibile utilizzare i criteri di esportazione per limitare l'accesso in base al metodo di autenticazione.

I criteri di esportazione per SMB sono opzionali e sono disattivati per impostazione predefinita. Se i criteri di esportazione sono disattivati, l'autenticazione Kerberos e NTLMv2 è consentita per impostazione predefinita su un server CIFS.

- Il dominio a cui appartengono il server CIFS e i server Hyper-V deve consentire l'autenticazione Kerberos

e NTLMv2.

L'autenticazione Kerberos è attivata per impostazione predefinita nei domini Active Directory. Tuttavia, l'autenticazione NTLMv2 può essere non consentita, utilizzando le impostazioni dei criteri di protezione o i criteri di gruppo.

Fasi

1. Eseguire le seguenti operazioni per verificare che i criteri di esportazione siano disattivati su SVM:

- a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Verificare che il `-is-exportpolicy-enabled` L'opzione del server CIFS è impostata su `false`:

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. Tornare al livello di privilegio admin:

```
set -privilege admin
```

2. Se i criteri di esportazione per SMB non sono disattivati, disabilitarli:

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. Verificare che l'autenticazione NTLMv2 e Kerberos sia consentita nel dominio.

Per informazioni sulla determinazione dei metodi di autenticazione consentiti nel dominio, consultare la Microsoft TechNet Library.

4. Se il dominio non consente l'autenticazione NTMLv2, attivare l'autenticazione NTLMv2 utilizzando uno dei metodi descritti nella documentazione Microsoft.

Esempio

I seguenti comandi verificano che i criteri di esportazione per SMB siano disattivati 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 vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-----  -
vs1      false

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

Verificare che gli account di dominio siano associati all'utente UNIX predefinito

Hyper-V e SQL Server utilizzano gli account di dominio per creare connessioni SMB alle condivisioni continuamente disponibili. Per creare correttamente la connessione, l'account del computer deve essere mappato correttamente a un utente UNIX. Il modo più conveniente per eseguire questa operazione consiste nel mappare l'account del computer all'utente UNIX predefinito.

A proposito di questa attività

Hyper-V e SQL Server utilizzano gli account dei computer di dominio per creare connessioni SMB. Inoltre, SQL Server utilizza un account utente di dominio come account di servizio che effettua anche connessioni SMB.

Quando si crea una macchina virtuale per lo storage (SVM), ONTAP crea automaticamente l'utente predefinito "pcuser" (con un UID di 65534) e il gruppo denominato "pcuser" (con un GID di 65534) e aggiunge l'utente predefinito al gruppo "pcuser". Se si configura una soluzione Hyper-V su SMB su una SVM esistente prima dell'aggiornamento del cluster a Data ONTAP 8.2, l'utente e il gruppo predefiniti potrebbero non esistere. In caso contrario, è necessario crearli prima di configurare l'utente UNIX predefinito del server CIFS.

Fasi

1. Determinare se esiste un utente UNIX predefinito:

```
vserver cifs options show -vserver vserver_name
```

2. Se l'opzione utente predefinita non è impostata, determinare se esiste un utente UNIX che può essere designato come utente UNIX predefinito:

```
vserver services unix-user show -vserver vserver_name
```

3. Se l'opzione utente predefinita non è impostata e non esiste un utente UNIX che può essere designato come utente UNIX predefinito, creare l'utente UNIX predefinito e il gruppo predefinito, quindi aggiungere l'utente predefinito al gruppo.

In genere, all'utente predefinito viene assegnato il nome utente "pcuser" e deve essere assegnato l'UID di 65534. Al gruppo predefinito viene generalmente assegnato il nome "pcuser". Il GID assegnato al gruppo deve essere 65534.

- a. Creare il gruppo predefinito:

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. Creare l'utente predefinito e aggiungerlo al gruppo predefinito:

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. Verificare che l'utente e il gruppo predefinito siano configurati correttamente:

```
vserver services unix-user show -vserver vserver_name+  
vserver services unix-group show -vserver vserver_name -members
```

4. Se l'utente predefinito del server CIFS non è configurato, eseguire le seguenti operazioni:

- a. Configurare l'utente predefinito:

```
vserver cifs options modify -vserver *vserver_name -default-unix-user
```

pcuser*

- b. Verificare che l'utente UNIX predefinito sia configurato correttamente:

vserver cifs options show -vserver vserver_name

5. Per verificare che l'account del computer del server applicazioni sia associato correttamente all'utente predefinito, mappare un'unità a una condivisione che risiede sulla SVM e confermare l'associazione dell'utente Windows all'utente UNIX utilizzando `vserver cifs session show` comando.

Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Esempio

I seguenti comandi determinano che l'utente predefinito del server CIFS non è impostato, ma determinano l'esistenza dell'utente "pcuser" e del gruppo "pcuser". L'utente "pcuser" viene assegnato come utente predefinito del server CIFS su SVM vs1.

```
cluster1::> vserver cifs options show
```

```
Vserver: vs1
```

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

```
cluster1::> vserver services unix-user show
```

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

```
cluster1::> vserver services unix-group show -members
```

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0

```
Users: -
```

```
cluster1::> vsserver cifs options modify -vsserver vs1 -default-unix-user pcuser
```

```
cluster1::> vsserver cifs options show
```

```
Vserver: vs1
```

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

Verificare che lo stile di protezione del volume root SVM sia impostato su NTFS

Per garantire il successo delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB, i volumi devono essere creati con lo stile di sicurezza NTFS. Poiché lo stile di sicurezza del volume root viene applicato per impostazione predefinita ai volumi creati sulla macchina virtuale di storage (SVM), lo stile di sicurezza del volume root deve essere impostato su NTFS.

A proposito di questa attività

- È possibile specificare lo stile di sicurezza del volume root al momento della creazione di SVM.
- Se SVM non viene creato con il volume root impostato sullo stile di protezione NTFS, è possibile modificare lo stile di protezione in un secondo momento utilizzando `volume modify` comando.

Fasi

1. Determinare lo stile di sicurezza corrente del volume root SVM:

```
volume show -vsserver vsserver_name -fields vsserver,volume,security-style
```

2. Se il volume root non è un volume di sicurezza NTFS, impostare lo stile di protezione su NTFS:

```
volume modify -vsserver vsserver_name -volume root_volume_name -security-style ntfs
```

3. Verificare che il volume root SVM sia impostato sullo stile di protezione NTFS:

```
volume show -vsserver vsserver_name -fields vsserver,volume,security-style
```

Esempio

I seguenti comandi verificano che lo stile di protezione del volume root sia NTFS su SVM vs1:


```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     ntfs
```

Verificare che le opzioni del server CIFS richieste siano configurate

È necessario verificare che le opzioni del server CIFS richieste siano attivate e configurate in base ai requisiti delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

A proposito di questa attività

- SMB 2.x e SMB 3.0 devono essere abilitati.
- L'offload delle copie di ODX deve essere abilitato per utilizzare l'offload delle copie che migliora le performance.
- I servizi di copia shadow di VSS devono essere attivati se la soluzione Hyper-V su SMB utilizza servizi di backup abilitati per VSS remoto (solo Hyper-V).

Fasi

1. Verificare che le opzioni del server CIFS richieste siano attivate sulla macchina virtuale di storage (SVM):
 - a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Immettere il seguente comando:

```
vserver cifs options show -vserver vserver_name
```

Le seguenti opzioni devono essere impostate su `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Solo Hyper-V)

2. Se una delle opzioni non è impostata su `true`, eseguire le seguenti operazioni:
 - a. Impostarli su `true` utilizzando `vserver cifs options modify` comando.

- b. Verificare che le opzioni siano impostate su true utilizzando `vserver cifs options show` comando.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

I seguenti comandi verificano che le opzioni richieste per la configurazione Hyper-V su SMB siano attivate su SVM vs1. Nell'esempio, l'offload delle copie ODX deve essere abilitato per soddisfare i requisiti delle opzioni.

```
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,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

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

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 per Hyper-V e SQL Server rispetto alle configurazioni SMB.

Di cosa hai bisogno

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 options show
```

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\
4s                                     Administrator
0
```

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: -
```

Creare volumi di dati NTFS

È necessario creare volumi di dati NTFS sulla macchina virtuale di storage (SVM) prima di poter configurare condivisioni continuamente disponibili per l'utilizzo con Hyper-V o

SQL Server su server applicazioni SMB. Utilizzare il foglio di lavoro per la configurazione del volume per creare i volumi di dati.

A proposito di questa attività

Per personalizzare un volume di dati, è possibile utilizzare parametri opzionali. Per ulteriori informazioni sulla personalizzazione dei volumi, vedere xref:./smb-hyper-v-sql/"Gestione dello storage logico".

Durante la creazione dei volumi di dati, non è necessario creare punti di giunzione all'interno di un volume contenente quanto segue:

- File Hyper-V per i quali ONTAP crea copie shadow
- File di database di SQL Server di cui viene eseguito il backup mediante SQL Server



Se si crea inavvertitamente un volume che utilizza uno stile di sicurezza misto o UNIX, non è possibile modificare il volume in un volume di sicurezza NTFS e utilizzarlo direttamente per creare condivisioni continuamente disponibili per operazioni senza interruzioni. Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB non funzionano correttamente, a meno che i volumi utilizzati nella configurazione non vengano creati come volumi di sicurezza NTFS. È necessario eliminare il volume e ricrearlo con lo stile di protezione NTFS. In alternativa, è possibile mappare il volume su un host Windows e applicare un ACL nella parte superiore del volume e propagare l'ACL a tutti i file e cartelle del volume.

Fasi

1. Creare il volume di dati immettendo il comando appropriato:

Se si desidera creare un volume in una SVM in cui lo stile di sicurezza del volume root è...	Immettere il comando...
NTFS	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
Non NTFS	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. Verificare che la configurazione del volume sia corretta:

```
volume show -vserver vservice_name -volume volume_name
```

Creare condivisioni SMB continuamente disponibili

Dopo aver creato i volumi di dati, è possibile creare le condivisioni continuamente disponibili utilizzate dai server applicazioni per accedere alla macchina virtuale Hyper-V, ai file di configurazione e ai file di database di SQL Server. È necessario utilizzare il foglio di lavoro di configurazione della condivisione per creare le condivisioni SMB.

Fasi

1. Visualizzare informazioni sui volumi di dati esistenti e sui relativi percorsi di giunzione:

```
volume show -vserver vserver_name -junction
```

2. Creare una condivisione SMB sempre disponibile:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- È possibile aggiungere un commento alla configurazione della condivisione.
 - Per impostazione predefinita, la proprietà di condivisione dei file offline è configurata sulla condivisione ed è impostata su `manual`.
 - ONTAP crea la condivisione con l'autorizzazione di condivisione predefinita di `Everyone / Full Control`.
3. Ripetere il passaggio precedente per tutte le condivisioni nel foglio di lavoro di configurazione della condivisione.
 4. Verificare che la configurazione sia corretta utilizzando `vserver cifs share show` comando.
 5. Configurare le autorizzazioni dei file NTFS sulle condivisioni continuamente disponibili mappando un disco a ciascuna condivisione e configurando le autorizzazioni dei file utilizzando la finestra **Proprietà di Windows**.

Esempio

I seguenti comandi creano una condivisione continuamente disponibile denominata "data2" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. I collegamenti simbolici vengono disattivati impostando `-symlink` parametro a. "":

```

cluster1::> volume show -vserver vs1 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
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

```

Aggiungere il privilegio SeSecurityPrivilege all'account utente (per SQL Server delle condivisioni SMB)

All'account utente di dominio utilizzato per l'installazione del server SQL deve essere assegnato il privilegio "SeSecurityPrivilege" per eseguire determinate azioni sul server CIFS che richiedono privilegi non assegnati per impostazione predefinita agli utenti di dominio.

Di cosa hai bisogno

L'account di dominio utilizzato per l'installazione di SQL Server deve già esistere.

A proposito di questa attività

Quando si aggiunge il privilegio all'account del programma di installazione di SQL Server, ONTAP potrebbe validare l'account contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Aggiungere il privilegio "SeSecurityPrivilege":

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name  
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

Il valore di `-user-or-group-name` Parameter è il nome dell'account utente di dominio utilizzato per l'installazione di SQL Server.

2. Verificare che il privilegio sia applicato all'account:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-  
group-name account_name
```

Esempio

Il seguente comando aggiunge il privilegio "SeSecurityPrivilege" all'account del programma di installazione di SQL Server nel dominio DI ESEMPIO per la macchina virtuale di storage (SVM) vs1:

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

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\SQLinstaller	SeSecurityPrivilege

Configurare la profondità della directory della copia shadow VSS (per Hyper-V su condivisioni SMB)

Facoltativamente, è possibile configurare la profondità massima delle directory all'interno delle condivisioni SMB su cui creare le copie shadow. Questo parametro è utile se si desidera controllare manualmente il livello massimo di sottodirectory in cui ONTAP deve creare copie shadow.

Di cosa hai bisogno

La funzione di copia shadow del VSS deve essere attivata.

A proposito di questa attività

L'impostazione predefinita prevede la creazione di copie shadow per un massimo di cinque sottodirectory. Se il valore è impostato su 0, ONTAP crea copie shadow per tutte le sottodirectory.



Sebbene sia possibile specificare che la profondità della directory shadow set copy includa più di cinque sottodirectory o tutte le sottodirectory, Microsoft richiede che la creazione del set di copie shadow venga completata entro 60 secondi. La creazione del set di copie shadow non riesce se non può essere completata entro questo intervallo di tempo. La profondità della directory di copia shadow scelta non deve far superare il tempo di creazione.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):


```
set -privilege advanced
```

2. Impostare la profondità della directory della copia shadow del VSS al livello desiderato:

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth  
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Gestire le configurazioni Hyper-V e SQL Server su SMB

Configurare le condivisioni esistenti per la disponibilità continua

È possibile modificare le condivisioni esistenti per diventare condivisioni continuamente disponibili utilizzate dai server applicativi Hyper-V e SQL Server per accedere senza interruzioni ai file di configurazione e alla macchina virtuale Hyper-V e ai file di database SQL Server.

A proposito di questa attività

Non è possibile utilizzare una condivisione esistente come condivisione continuamente disponibile per operazioni senza interruzioni con server applicazioni su SMB se la condivisione ha le seguenti caratteristiche:

- Se il `homedirectory` la proprietà share viene impostata su tale condivisione
- Se la condivisione contiene link simbolici o `widelink` abilitati
- Se la condivisione contiene volumi congiunti al di sotto della radice della condivisione

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:

- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

È necessario configurare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate. Se sono presenti nell'elenco delle proprietà di condivisione correnti, devono essere rimosse dalla condivisione continuamente disponibile:

- `attributecache`
- `branchcache`

Fasi

1. Visualizza le impostazioni correnti dei parametri di condivisione e l'elenco corrente delle proprietà di condivisione configurate:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. Se necessario, modificare i parametri di condivisione per disattivare i collegamenti simbolici e impostare i file offline su manuale utilizzando `vserver cifs share properties modify` comando.

È possibile disattivare i collegamenti simbolici impostando il valore di `-symlink` parametro a `""`.

- È possibile disattivare i collegamenti simbolici impostando il valore di `-symlink` parametro a `""`.
- È possibile impostare `-offline-files` impostare correttamente il parametro specificando `manual`.

3. Aggiungere il `continuously-available` condividere la proprietà e, se necessario, il `oplocks` proprietà di condivisione:

```
vserver cifs share properties add -vserver vserver_name -share-name share_name  
-share-properties continuously-available[,oplock]
```

Se il `oplocks` la proprietà di condivisione non è già impostata, è necessario aggiungerla con `continuously-available` condividere la proprietà.

4. Rimuovere eventuali proprietà di condivisione non supportate nelle condivisioni a disponibilità continua:

```
vserver cifs share properties remove -vserver vserver_name -share-name  
share_name -share-properties properties[,...]
```

È possibile rimuovere una o più proprietà di condivisione specificando le proprietà di condivisione con un elenco delimitato da virgole.

5. Verificare che il `-symlink` e `-offline-files` i parametri sono impostati correttamente:

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields  
symlink-properties,offline-files
```

6. Verificare che l'elenco delle proprietà di condivisione configurate sia corretto:

```
vserver cifs shares properties show -vserver vserver_name -share-name  
share_name
```

Esempi

L'esempio seguente mostra come configurare una condivisione esistente denominata "hare1 `s`" su una macchina virtuale di storage (SVM) vs1 per NDOS con un server applicativo su SMB:

- I collegamenti simbolici vengono disattivati nella condivisione impostando `-symlink` parametro su `""`.
- Il `-offline-file` il parametro viene modificato e impostato su `manual`.
- Il `continuously-available` la proprietà share viene aggiunta alla condivisione.
- Il `oplocks` la proprietà di condivisione è già presente nell'elenco delle proprietà di condivisione, pertanto non è necessario aggiungerla.
- Il `attributecache` la proprietà share viene rimossa dalla condivisione.
- Il `browsable` La proprietà Share è opzionale per una condivisione a disponibilità continua utilizzata per NDOS con server applicazioni su SMB e viene conservata come una delle proprietà di condivisione.

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
CIFS Server NetBIOS Name: vs1
        Path: /data
        Share Properties: oplocks
                        browsable
                        attributecache
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsriver cifs share modify -vsriver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
-fields symlink-properties,offline-files
vsriver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                browsable
                continuously-available
```

Abilitare o disabilitare le copie shadow VSS per i backup Hyper-V su SMB

Se si utilizza un'applicazione di backup VSS-aware per eseguire il backup dei file di macchine virtuali Hyper-V memorizzati nelle condivisioni SMB, è necessario attivare la copia shadow VSS. Se non si utilizzano applicazioni di backup compatibili con VSS, è possibile disattivare la copia shadow del VSS. L'impostazione predefinita prevede l'attivazione della copia shadow del VSS.

A proposito di questa attività

È possibile attivare o disattivare le copie shadow VSS in qualsiasi momento.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera che le copie shadow di VSS siano...	Immettere il comando...
Attivato	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</pre>
Disattivato	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

I seguenti comandi abilitano le copie shadow VSS 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 -shadowcopy-enabled
true

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

Utilizza le statistiche per monitorare l'attività di Hyper-V e SQL Server su 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 <i>object_name</i>
Quali contatori sono disponibili	statistics catalog counter show object <i>object_name</i>

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

[...]

Visualizzare le statistiche SMB

È possibile visualizzare varie statistiche SMB per monitorare le performance e

diagnosticare i problemi.

Fasi

1. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati.
2. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le statistiche per...	Immettere il seguente comando...
Tutte le versioni di SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x e SMB 3.0	<code>statistics show -object smb2</code>
Sottosistema SMB del nodo	<code>statistics show -object nblade_cifs</code>

Scopri di più su `statistics` comandi:

- ["vengono visualizzate le statistiche"](#)
- ["le statistiche iniziano"](#)
- ["le statistiche si interrompono"](#)

Verificare che la configurazione sia in grado di eseguire operazioni senza interruzioni

Utilizzare il monitoraggio dello stato di salute per determinare se lo stato delle operazioni senza interruzioni è integro

Il monitoraggio dello stato di salute fornisce informazioni sullo stato di salute del sistema nel cluster. Il monitor dello stato di salute monitora le configurazioni di Hyper-V e SQL Server su SMB per garantire operazioni senza interruzioni (NDOS) per gli application server. Se lo stato è degradato, è possibile visualizzare i dettagli del problema, incluse la probabile causa e le azioni di ripristino consigliate.

Sono disponibili diversi monitor di stato. ONTAP monitora sia lo stato generale del sistema che lo stato di salute dei singoli monitor. Il monitor di stato della connettività del nodo contiene il sottosistema CIFS-NDO. Il monitor dispone di una serie di policy di salute che attivano avvisi se determinate condizioni fisiche possono causare interruzioni e, se esiste una condizione di interruzione, genera avvisi e fornisce informazioni sulle azioni correttive. Per le configurazioni NDO su SMB, vengono generati avvisi per le due seguenti condizioni:

ID avviso	Severità	Condizione
HaNotReadyCifsNdo_Alert	Maggiore	Uno o più file ospitati da un volume in un aggregato sul nodo sono stati aperti attraverso una condivisione SMB continuamente disponibile con la promessa di persistenza in caso di guasto; tuttavia, la relazione ha con il partner non è configurata o non è integro.
NoStandbyLifCifsNdo_Alert	Minore	La macchina virtuale di storage (SVM) sta fornendo attivamente i dati tramite SMB attraverso un nodo e ci sono file SMB aperti in modo persistente su condivisioni continuamente disponibili; tuttavia, il nodo partner non sta esponendo alcun LIF di dati attivo per SVM.

Visualizzazione dello stato delle operazioni senza interruzioni mediante il monitoraggio dello stato di salute del sistema

È possibile utilizzare `system health` Comandi per visualizzare informazioni sullo stato generale del sistema del cluster e sullo stato del sottosistema CIFS-NDO, per rispondere agli avvisi, per configurare gli avvisi futuri e per visualizzare informazioni sulla configurazione del monitoraggio dello stato di salute.

Fasi

1. Monitorare lo stato di salute eseguendo l'azione appropriata:

Se si desidera visualizzare...	Immettere il comando...
Lo stato di salute del sistema, che riflette lo stato generale dei singoli monitor di salute	system health status show
Informazioni sullo stato di salute del sottosistema CIFS-NDO	system health subsystem show -subsystem CIFS-NDO -instance

2. Visualizzare le informazioni sulla configurazione del monitoraggio degli avvisi CIFS-NDO eseguendo le azioni appropriate:

Se si desidera visualizzare informazioni su...	Immettere il comando...
La configurazione e lo stato del monitor di stato per il sottosistema CIFS-NDO, ad esempio i nodi monitorati, lo stato di inizializzazione e lo stato	system health config show -subsystem CIFS-NDO

Se si desidera visualizzare informazioni su...	Immettere il comando...
CIFS-NDO avvisa che un monitor di stato può potenzialmente generare	system health alert definition show -subsystem CIFS-NDO
Criteri di monitoraggio dello stato CIFS-NDO, che determinano quando vengono generati gli avvisi	system health policy definition show -monitor node-connect



Utilizzare `-instance` per visualizzare informazioni dettagliate.

Esempi

Il seguente output mostra informazioni sullo stato di salute generale del cluster e del sottosistema CIFS-NDO:

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
  Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

Il seguente output mostra informazioni dettagliate sulla configurazione e lo stato del monitor di stato del sottosistema CIFS-NDO:

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

Verificare la configurazione della condivisione SMB continuamente disponibile

Per supportare operazioni senza interruzioni, le condivisioni SMB di Hyper-V e SQL Server devono essere configurate come condivisioni a disponibilità continua. Inoltre, è necessario controllare alcune altre impostazioni di condivisione. È necessario verificare che le condivisioni siano configurate correttamente per fornire operazioni senza interruzioni per i server di applicazioni in caso di eventi di interruzione pianificati o non pianificati.

A proposito di questa attività

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:

- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

Per operazioni corrette senza interruzioni, è necessario impostare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Fasi

1. Verificare che i file offline siano impostati su `manual` oppure `disabled` e che i link simbolici sono disabilitati:

```
vserver cifs shares show -vserver vserver_name
```

2. Verificare che le condivisioni SMB siano configurate per la disponibilità continua:

```
vserver cifs shares properties show -vserver vserver_name
```

Esempi

Nell'esempio seguente viene visualizzata l'impostazione di condivisione per una condivisione denominata "share1" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) `vs1`. I file offline sono impostati su `manual` i collegamenti simbolici e sono disattivati (indicati da un trattino in `Symlink Properties` output di campo):

```

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
          Vserver: vs1
          Share: share1
    CIFS Server NetBIOS Name: VS1
          Path: /data/share1
    Share Properties: oplocks
                    continuously-available
    Symlink Properties: -
    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 seguente vengono visualizzate le proprietà di condivisione di una condivisione denominata "share1" su SVM vs1:

```

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1    oplocks
                    continuously-available

```

Verificare lo stato LIF

Anche se si configurano le macchine virtuali di storage (SVM) con configurazioni Hyper-V e SQL Server su SMB in modo che dispongano di LIF su ciascun nodo di un cluster, durante le operazioni quotidiane, alcune LIF potrebbero spostarsi sulle porte di un altro nodo. È necessario verificare lo stato LIF e intraprendere le azioni correttive necessarie.

A proposito di questa attività

Per fornire un supporto operativo senza interruzioni, ciascun nodo di un cluster deve disporre di almeno una LIF per la SVM e tutte le LIF devono essere associate a una porta home. Se alcune delle LIF configurate non sono attualmente associate alla porta home, è necessario risolvere eventuali problemi di porta e ripristinare le LIF alla porta home.

Fasi

1. Visualizzare le informazioni sui LIF configurati per SVM:

```
network interface show -vserver vserver_name
```

In questo esempio, "lif1" non si trova sulla porta home.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
vs1	lif1	up/up	10.0.0.128/24	node2	e0d
false	lif2	up/up	10.0.0.129/24	node2	e0d
true					

2. Se alcune delle LIF non si trovano sulle porte home, attenersi alla seguente procedura:

a. Per ogni LIF, determinare quale sia la porta home di LIF:

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

vserver	lif	home-node	home-port
-----	----	-----	-----
vs1	lif1	node1	e0d

b. Per ciascun LIF, determinare se la porta home del LIF è attiva:

```
network port show -node node1 -port e0d -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

node	port	link
-----	----	----
node1	e0d	up

+
In questo esempio, “lif1” deve essere nuovamente migrato alla porta home, node1:e0d.

3. Se una delle interfacce di rete della porta home a cui devono essere associate le LIF non si trovano in up risolvere il problema in modo che queste interfacce siano in funzione.
4. Se necessario, ripristinare le LIF alle porte home:

```
network interface revert -vserver vs1 -lif lif1
```

```
network interface revert -vserver vs1 -lif lif1
```

5. Verificare che ciascun nodo del cluster disponga di una LIF attiva per SVM:

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----

vs1						
	lif1	up/up	10.0.0.128/24	node1	e0d	
true						
	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

Determinare se le sessioni SMB sono continuamente disponibili

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.

Fasi

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 <i>vserver_name</i>
Su un ID di connessione specificato	vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer
Da un indirizzo IP della workstation specificato	vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i>
Su un indirizzo IP LIF specificato	vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i>
Su un nodo specificato	<i>**vserver cifs session show -vserver vserver_name -node {node_name</i>
local}**	Da un utente Windows specificato
vserver cifs session show -vserver <i>vserver_name</i> -windows-user <i>user_name</i> Il formato per <i>user_name</i> è [domain]\user.	Con un meccanismo di autenticazione specificato

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
<pre>vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mec hanism</pre> <p>Il valore per <code>-auth</code> <code>-mechanism</code> può essere uno dei seguenti:</p> <ul style="list-style-type: none"> • NTLMv1 • NTLMv2 • Kerberos • Anonymous 	Con una versione del protocollo specificata

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
<pre>vserver cifs session show -vserver vserver_name -protocol-version protocol_version</pre> <p>Il valore per <code>-protocol-version</code> può essere uno dei seguenti:</p> <ul style="list-style-type: none"> • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 	Con un livello specifico di protezione a disponibilità continua

Se si desidera visualizzare le informazioni sulla sessione SMB...

Immettere il seguente comando...

```
vserver cifs  
session show  
-vserver  
vserver_name  
-continuously  
-available  
continuously_avail  
able_protection_le  
vel
```

Con uno stato di sessione SMB Signing specificato

Il valore per
-continuously
-available può essere
uno dei seguenti:

- No
- Yes
- Partial

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
ID          ID          Workstation      Windows User      Open      Idle
-----
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
```

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 inoltre 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.

Fasi

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	<code>vserver cifs session file show -vserver vserver_name</code>
Su un nodo specificato	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*`</code>	Su un ID file specificato
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	Su un ID connessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	Su un ID sessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	Sull'aggregato di hosting specificato
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	Sul volume specificato
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	Sulla condivisione SMB specificata
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	Sul percorso SMB specificato

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
vserver cifs session file show -vserver <i>vserver_name</i> -path <i>path</i>	Con il livello specificato di protezione a disponibilità continua
vserver cifs session file show -vserver <i>vserver_name</i> -continuously -available <i>continuously_available_status</i> Il valore per <code>-continuously-available</code> può essere uno dei seguenti: <ul style="list-style-type: none"> • No • Yes <div style="display: flex; align-items: center; margin-top: 20px;">  <div> <p>Se lo stato di disponibilità continua è <code>No</code>, 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.</p> </div> </div>	Con lo stato di riconnessione specificato

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 sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.