



Workflow di configurazione multiprotocollo

System Manager Classic

NetApp
April 09, 2024

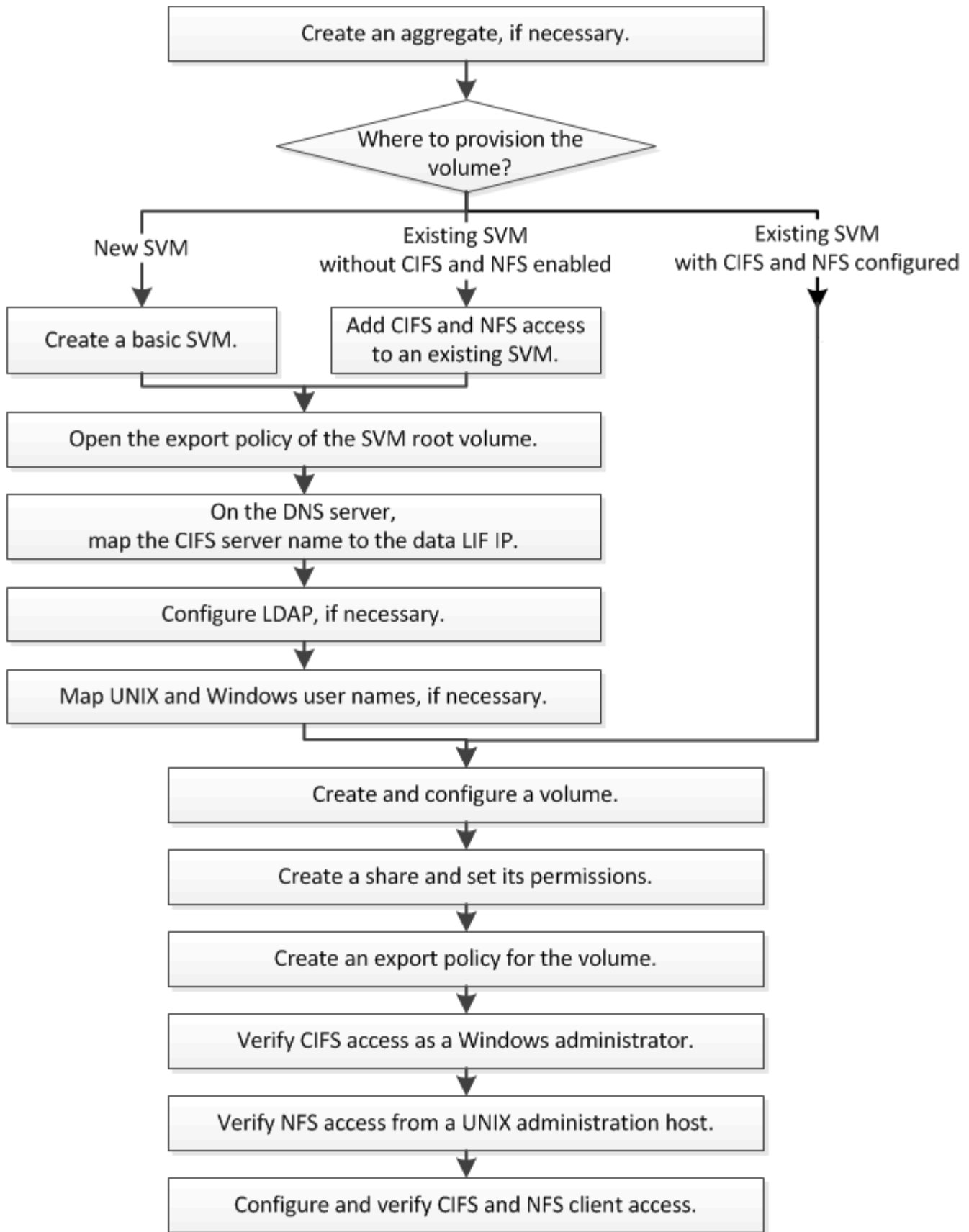
This PDF was generated from https://docs.netapp.com/it-it/ontap-sm-classic/nas-multiprotocol-config/task_creating_aggregate.html on April 09, 2024. Always check docs.netapp.com for the latest.

Sommario

- Workflow di configurazione multiprotocollo 1
 - Creare un aggregato 2
 - Decidere dove eseguire il provisioning del nuovo volume 3
 - Creare e configurare un volume 17
 - Creare una condivisione e impostarne le autorizzazioni 18
 - Creare una policy di esportazione per il volume 19
 - Verificare l'accesso al client SMB 20
 - Verificare l'accesso NFS da un host di amministrazione UNIX 21
 - Configurare e verificare l'accesso al client CIFS e NFS 22

Workflow di configurazione multiprotocollo

La configurazione di SMB/CIFS e NFS richiede la creazione opzionale di un aggregato, la creazione di una nuova SVM o la configurazione di una esistente, la creazione di un volume, la condivisione e l'esportazione e la verifica dell'accesso da host di amministrazione UNIX e Windows. È quindi possibile aprire l'accesso ai client SMB/CIFS e NFS.



Creare un aggregato

Se non si desidera utilizzare un aggregato esistente, è possibile creare un nuovo

aggregato per fornire storage fisico al volume che si sta eseguendo il provisioning.

A proposito di questa attività

Se si dispone di un aggregato esistente che si desidera utilizzare per il nuovo volume, è possibile ignorare questa procedura.

Fasi

1. Inserire l'URL `https://IP-address-of-cluster-management-LIF` In un browser Web e accedere a System Manager utilizzando la credenziale dell'amministratore del cluster.
2. Passare alla finestra **aggregati**.
3. Fare clic su **Crea**.
4. Seguire le istruzioni sullo schermo per creare l'aggregato utilizzando la configurazione RAID-DP predefinita, quindi fare clic su **Create** (Crea).

Create Aggregate

To create an aggregate, select a disk type then specify the number of disks.

Name:

Disk Type:

Number of Disks: Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP

RAID Configuration: RAID-DP; RAID group size of 16 disks [Change](#)

New Usable Capacity: 4.968 TB (Estimated)

Risultati

L'aggregato viene creato con la configurazione specificata e aggiunto all'elenco degli aggregati nella finestra aggregati.

Decidere dove eseguire il provisioning del nuovo volume

Prima di creare un nuovo volume multiprotocollo, è necessario decidere se collocare il volume in una macchina virtuale di storage (SVM) esistente e, in tal caso, la quantità di configurazione richiesta da SVM. Questa decisione determina il tuo flusso di lavoro.

Procedura

- Se si desidera eseguire il provisioning di un volume su una nuova SVM, creare una SVM di base.

"Creazione di una SVM di base"

Scegliere questa opzione se CIFS e NFS non sono già abilitati su una SVM esistente.

- Se si desidera eseguire il provisioning di un volume su una SVM esistente con CIFS e NFS attivati ma non configurati, aggiungere l'accesso CIFS e NFS alla SVM esistente.

"Aggiunta di accesso CIFS e NFS su una SVM esistente"

- Se si desidera eseguire il provisioning di un volume su una SVM esistente completamente configurata per l'accesso multiprotocollo CIFS e NFS, è possibile creare e configurare direttamente il volume.

"Creazione e configurazione di un volume"

Creare una SVM di base

È possibile utilizzare una procedura guidata che guida l'utente nel processo di creazione di una nuova SVM (Storage Virtual Machine), configurazione del DNS (Domain Name System), creazione di un'interfaccia logica dati (LIF), configurazione di un server CIFS, abilitazione di NFS e, facoltativamente, configurazione di NIS.

Prima di iniziare

- La rete deve essere configurata e le relative porte fisiche devono essere collegate alla rete.
- È necessario sapere quali dei seguenti componenti di rete verranno utilizzati da SVM:
 - Il nodo e la porta specifica su quel nodo in cui verrà creata l'interfaccia logica dati (LIF)
 - La subnet da cui verrà fornito l'indirizzo IP del LIF dei dati o, facoltativamente, l'indirizzo IP specifico che si desidera assegnare al LIF dei dati
 - Dominio Active Directory (ad) a cui si aggiungerà questa SVM, insieme alle credenziali richieste per aggiungervi la SVM
 - Informazioni NIS, se il sito utilizza NIS per i servizi di nome o la mappatura dei nomi
- La subnet deve essere instradabile a tutti i server esterni richiesti per servizi come NIS (Network Information Service), LDAP (Lightweight Directory Access Protocol), ad (Active Directory) e DNS.
- Tutti i firewall esterni devono essere configurati in modo appropriato per consentire l'accesso ai servizi di rete.
- L'ora dei controller di dominio ad, dei client e di SVM deve essere sincronizzata entro cinque minuti l'una dall'altra.

A proposito di questa attività

Quando si crea una SVM per l'accesso multiprotocollo, non utilizzare le sezioni di provisioning della finestra di installazione di Storage Virtual Machine (SVM), che crea due volumi, non un singolo volume con accesso multiprotocollo. È possibile eseguire il provisioning del volume in un secondo momento nel flusso di lavoro.

Fasi

1. Accedere alla finestra **SVM**.
2. Fare clic su **Crea**.
3. Nella finestra di dialogo **Storage Virtual Machine (SVM) Setup**, creare il campo SVM:
 - a. Specificare un nome univoco per la SVM.

Il nome deve essere un FQDN (Fully Qualified Domain Name) o seguire un'altra convenzione che garantisca nomi univoci in un cluster.

- b. Selezionare tutti i protocolli per i quali si dispone di licenze e che verranno utilizzati sulla SVM, anche se non si desidera configurare immediatamente tutti i protocolli.

- c. Mantenere l'impostazione predefinita della lingua, C.UTF-8.



Se si supporta la visualizzazione internazionale dei caratteri nei client NFS e SMB/CIFS, si consiglia di utilizzare il codice lingua **UTF8MB4**, disponibile a partire da ONTAP 9.5.

- d. **Opzionale:** Assicurarsi che lo stile di sicurezza sia impostato in base alle proprie preferenze.

Selezionando il protocollo CIFS, lo stile di protezione viene impostato su NTFS per impostazione predefinita.

- e. **Opzionale:** Selezionare l'aggregato root per contenere il volume root SVM.

L'aggregato selezionato per il volume root non determina la posizione del volume di dati. L'aggregato per il volume di dati viene selezionato separatamente in una fase successiva.

Storage Virtual Machine (SVM) Setup

1 Enter SVM basic details

SVM Details

? Specify a unique name and the data protocols for the SVM

SVM Name:

? IPspace:

? Data Protocols: ☒ CIFS ☒ NFS ☒ iSCSI ☒ FC/FCoE ☐ NVMe

? Default Language:

The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.

? Security Style:

Root Aggregate:

- f. **Opzionale:** Nella sezione **Configurazione DNS**, assicurarsi che il dominio di ricerca DNS e i server dei nomi predefiniti siano quelli che si desidera utilizzare per questa SVM.

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

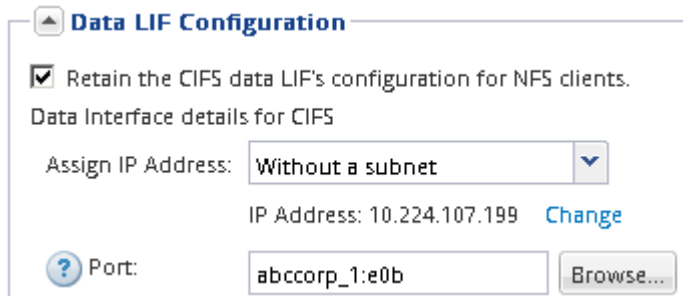
? Search Domains:

? Name Servers:

g. Fare clic su **Invia e continua**.

La SVM viene creata, ma i protocolli non sono ancora configurati.

4. Nella sezione **Data LIF Configuration** della pagina **Configure CIFS/NFS Protocol** (Configura protocollo CIFS/NFS), specificare i dettagli della LIF che i client utilizzeranno per accedere ai dati:
 - a. Assegnare automaticamente un indirizzo IP alla LIF da una subnet specificata o immetterlo manualmente.
 - b. Fare clic su **Browse** (Sfoglia) e selezionare un nodo e una porta da associare alla LIF.



Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

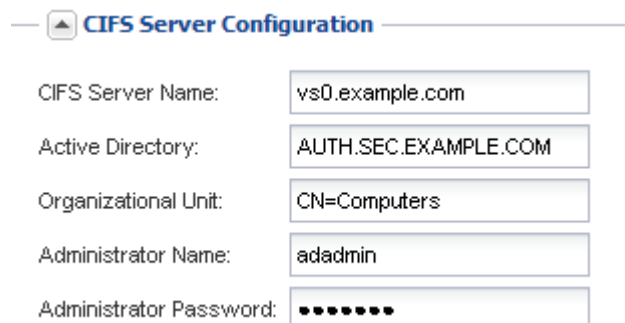
Data Interface details for CIFS

Assign IP Address: Without a subnet ▼

IP Address: 10.224.107.199 [Change](#)

? Port: abccorp_1:e0b Browse...

5. Nella sezione **CIFS Server Configuration**, definire il server CIFS e configurarlo per accedere al dominio ad:
 - a. Specificare un nome per il server CIFS univoco nel dominio ad.
 - b. Specificare l'FQDN del dominio ad a cui il server CIFS può accedere.
 - c. Se si desidera associare un'unità organizzativa (OU) all'interno del dominio ad diversa da CN=Computers, immettere l'unità organizzativa.
 - d. Specificare il nome e la password di un account amministrativo con privilegi sufficienti per aggiungere il server CIFS all'unità organizzativa.
 - e. Se si desidera evitare l'accesso non autorizzato a tutte le condivisioni su questa SVM, selezionare l'opzione per crittografare i dati utilizzando SMB 3.0.



CIFS Server Configuration

CIFS Server Name: vs0.example.com


Active Directory: AUTH.SEC.EXAMPLE.COM

Organizational Unit: CN=Computers

Administrator Name: adadmin

Administrator Password: ••••••••


6. Ignorare l'area **Provision a volume for CIFS Storage** (Esegui provisioning di un volume per lo storage CIFS), in quanto fornisce un volume solo per l'accesso CIFS, non per l'accesso multiprotocollo.
7. Se l'area **NIS Configuration** (Configurazione NIS) è compressa, espanderla.
8. Se il sito utilizza NIS per la mappatura dei nomi o dei nomi, specificare il dominio e gli indirizzi IP dei server NIS.

—  **NIS Configuration {Optional}** —

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:

IP Addresses:

 Database Type: ☒ group ☒ passwd ☒ netgroup

9. Ignorare l'area **Provision a volume for NFS Storage** (Esegui provisioning di un volume per NFS Storage*), in quanto fornisce un volume solo per l'accesso NFS, non per l'accesso multiprotocollo.

10. Fare clic su **Invia e continua**.

Vengono creati i seguenti oggetti:

- Una LIF di dati denominata dopo la SVM con il suffisso “_cifs_nfs_lif1”
- Un server CIFS che fa parte del dominio ad
- Un server NFS

11. Per tutte le altre pagine di configurazione del protocollo visualizzate, fare clic su **Skip** (Ignora) e configurare il protocollo in un secondo momento.

12. Quando viene visualizzata la pagina **SVM Administration** (Amministrazione SVM), configurare o rinviare la configurazione di un amministratore separato per questa SVM:

- Fare clic su **Ignora** e configurare un amministratore in un secondo momento, se necessario.
- Inserire le informazioni richieste, quindi fare clic su **Submit & Continue** (Invia e continua).

13. Esaminare la pagina **Riepilogo**, annotare le informazioni eventualmente necessarie in un secondo momento, quindi fare clic su **OK**.

L'amministratore DNS deve conoscere il nome del server CIFS e l'indirizzo IP del file LIF dei dati. I client Windows devono conoscere il nome del server CIFS. I client NFS devono conoscere l'indirizzo IP del file LIF dei dati.

Risultati

Viene creata una nuova SVM con un server CIFS e un server NFS accessibili attraverso lo stesso LIF di dati.

Cosa fare in seguito

A questo punto, è necessario aprire la policy di esportazione del volume root SVM.

Informazioni correlate

[Apertura della policy di esportazione del volume root SVM \(creazione di una nuova SVM abilitata per NFS\)](#)

Aggiungere l'accesso CIFS e NFS a una SVM esistente

L'aggiunta dell'accesso CIFS/SMB e NFS a una SVM esistente implica la creazione di una LIF dati, la configurazione di un server CIFS, l'abilitazione di NFS e, facoltativamente, la configurazione di NIS.

Prima di iniziare

- È necessario sapere quali dei seguenti componenti di rete verranno utilizzati da SVM:
 - Il nodo e la porta specifica su quel nodo in cui verrà creata l'interfaccia logica dati (LIF)
 - La subnet da cui verrà fornito l'indirizzo IP del LIF dei dati o, facoltativamente, l'indirizzo IP specifico che si desidera assegnare al LIF dei dati
 - Il dominio Active Directory (ad) a cui si unisce questa SVM, insieme alle credenziali richieste per aggiungervi la SVM
 - Informazioni NIS se il sito utilizza NIS per i servizi di nome o la mappatura dei nomi
- Tutti i firewall esterni devono essere configurati in modo appropriato per consentire l'accesso ai servizi di rete.
- L'ora dei domain controller, dei client e della SVM di ad deve essere sincronizzata entro cinque minuti l'uno dall'altro.
- I protocolli CIFS e NFS devono essere consentiti su SVM.

Questo è il caso se non si è seguita questa procedura per creare SVM durante la configurazione di un protocollo diverso.

A proposito di questa attività

L'ordine di configurazione di CIFS e NFS influisce sulle finestre di dialogo visualizzate. In questa procedura, è necessario configurare prima CIFS e poi NFS.

Fasi

1. Accedere all'area in cui è possibile configurare i protocolli di SVM:
 - a. Selezionare la SVM che si desidera configurare.
 - b. Nel riquadro **Dettagli**, accanto a **protocolli**, fare clic su **CIFS**.

Protocols: NFS CIFS FC/FCoE

2. Nella sezione **Data LIF Configuration** della finestra di dialogo **Configure CIFS Protocol** (Configura protocollo CIFS), creare una LIF dati per SVM:
 - a. Assegnare automaticamente un indirizzo IP alla LIF da una subnet specificata o immetterlo manualmente.
 - b. Fare clic su **Browse** (Sfogliare) e selezionare un nodo e una porta da associare alla LIF.

Data LIF Configuration

☒ Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

? Port: abccorp_1:e0b [Browse...](#)

3. Nella sezione **CIFS Server Configuration**, definire il server CIFS e configurarlo per accedere al dominio ad:
 - a. Specificare un nome per il server CIFS univoco nel dominio ad.

- b. Specificare l'FQDN del dominio ad a cui il server CIFS può accedere.
- c. Se si desidera associare un'unità organizzativa (OU) all'interno del dominio ad diversa da CN=Computers, immettere l'unità organizzativa.
- d. Specificare il nome e la password di un account amministrativo con privilegi sufficienti per aggiungere il server CIFS all'unità organizzativa.
- e. Se si desidera evitare l'accesso non autorizzato a tutte le condivisioni su questa SVM, selezionare l'opzione per crittografare i dati utilizzando SMB 3.0.

▲ **CIFS Server Configuration**

CIFS Server Name:	<input type="text" value="vs0.example.com"/>
Active Directory:	<input type="text" value="AUTH.SEC.EXAMPLE.COM"/>
Organizational Unit:	<input type="text" value="CN=Computers"/>
Administrator Name:	<input type="text" value="adadmin"/>
Administrator Password:	<input type="password" value="••••••"/>

4. Creare un volume per l'accesso CIFS/SMB ed eseguire il provisioning di una condivisione:
 - a. Assegnare un nome alla condivisione utilizzata dai client CIFS/SMB per accedere al volume.

Il nome immesso per la condivisione verrà utilizzato anche come nome del volume.

- b. Specificare una dimensione per il volume.

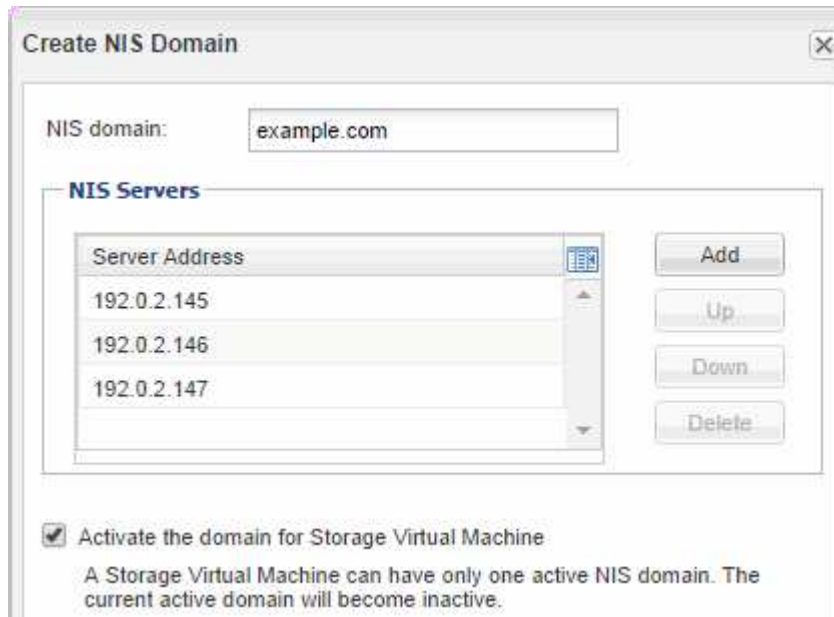
Provision a volume for CIFS storage (Optional).

Share Name:	<input type="text" value="Eng"/>
Size:	<input type="text" value="10"/> <input type="text" value="GB"/> ▼
Permission:	<input type="text" value="Administrators - Full Control"/> Change

Non è necessario specificare l'aggregato per il volume perché viene posizionato automaticamente sull'aggregato con lo spazio più disponibile.

5. Ignorare l'area **Provision a volume for CIFS Storage** (Esegui provisioning di un volume per lo storage CIFS), in quanto fornisce un volume solo per l'accesso CIFS, non per l'accesso multiprotocollo.
6. Fare clic su **Submit & Close**, quindi su **OK**.
7. Abilitare NFS:
 - a. Dalla scheda SVM, selezionare la SVM per cui si desidera attivare NFS e fare clic su **Manage** (Gestisci).
 - b. Nel riquadro **Protocols** (protocolli), fare clic su **NFS**, quindi su **Enable** (attiva).
8. Se il sito utilizza NIS per la mappatura dei nomi o per i servizi dei nomi, configurare NIS:
 - a. Nella finestra **servizi**, fare clic su **NIS**.
 - b. Nella finestra **NIS**, fare clic su **Create** (Crea).
 - c. Specificare il dominio dei server NIS.

- d. Aggiungere gli indirizzi IP dei server NIS.
- e. Selezionare **Activate the domain for Storage Virtual Machine** (attiva dominio per Storage Virtual Machine*), quindi fare clic su **Create** (Crea).



Cosa fare in seguito

Aprire la policy di esportazione del volume root SVM.

Aprire la policy di esportazione del volume root SVM (creare una nuova SVM abilitata per NFS)

È necessario aggiungere una regola al criterio di esportazione predefinito per consentire l'accesso a tutti i client tramite NFSv3. Senza tale regola, a tutti i client NFS viene negato l'accesso alla macchina virtuale di storage (SVM) e ai relativi volumi.

A proposito di questa attività

Specificare tutti gli accessi NFS come policy di esportazione predefinita e in seguito limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per i singoli volumi.

Fasi

1. Accedere alla finestra **SVM**.
2. Fare clic sulla scheda **Impostazioni SVM**.
3. Nel riquadro **Policies**, fare clic su **Export Policies** (Esporta policy).
4. Selezionare il criterio di esportazione denominato **default**, che viene applicato al volume root SVM.
5. Nel riquadro inferiore, fare clic su **Aggiungi**.
6. Nella finestra di dialogo **Create Export Rule** (Crea regola di esportazione), creare una regola che apra l'accesso a tutti i client per i client NFS:
 - a. Nel campo **Client Specification**, immettere `0.0.0.0/0` in modo che la regola si applichi a tutti i client.
 - b. Mantenere il valore predefinito **1** per l'indice della regola.

- c. Selezionare **NFSv3**.
- d. Deselezionare tutte le caselle di controllo ad eccezione della casella di controllo **UNIX** in **sola lettura**.
- e. Fare clic su **OK**.

Create Export Rule

Client Specification: 0.0.0.0/0

Rule Index: 1

Access Protocols: ☒ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☒ Read-Only ☐ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

Risultati

I client NFSv3 possono ora accedere a qualsiasi volume creato su SVM.

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 LDAP (creare una nuova SVM abilitata per NFS)

Se si desidera che la macchina virtuale di storage (SVM) ottenga le informazioni utente dal protocollo LDAP (Lightweight Directory Access Protocol) basato su Active Directory, è necessario creare un client LDAP, attivarlo per la SVM e assegnare la priorità LDAP ad altre fonti di informazioni utente.

Prima di iniziare

- La configurazione LDAP deve utilizzare Active Directory (ad).

Se si utilizza un altro tipo di LDAP, è necessario utilizzare l'interfaccia della riga di comando (CLI) e altra documentazione per configurare LDAP.

["Report tecnico NetApp 4067: NFS in NetApp ONTAP"](#)

["Report tecnico NetApp 4616: NFS Kerberos in ONTAP con Microsoft Active Directory"](#)

["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)

- È necessario conoscere il dominio e i server di ad, nonché le seguenti informazioni di binding: Il livello di autenticazione, l'utente e la password di binding, il DN di base e la porta LDAP.

Fasi

1. Accedere alla finestra **SVM**.
2. Selezionare la SVM richiesta
3. Fare clic sulla scheda **Impostazioni SVM**.
4. Impostare un client LDAP per SVM da utilizzare:
 - a. Nel riquadro **servizi**, fare clic su **Client LDAP**.
 - b. Nella finestra **LDAP Client Configuration** (Configurazione client LDAP), fare clic su **Add** (Aggiungi).
 - c. Nella scheda **Generale** della finestra **Crea client LDAP**, digitare il nome della configurazione del client LDAP, ad esempio `vs0client1`.
 - d. Aggiungere il dominio ad o i server ad.

Create LDAP Client

General | Binding

LDAP Client Configuration:

Servers

☒ Active Directory Domain

Preferred Active Directory Servers

Server
192.0.2.145

Add Delete Up Down

☐ Active Directory Servers

- e. Fare clic su **binding** e specificare il livello di autenticazione, l'utente e la password di binding, il DN di base e la porta.

Edit LDAP Client

General | **Binding**

Authentication level: ▼

Bind DN (User):

Bind user password:

Base DN:

Tcp port:

i The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.

- f. Fare clic su **Save and Close** (Salva e chiudi).

Viene creato un nuovo client che può essere utilizzato da SVM.

5. Abilitare il nuovo client LDAP per SVM:

- Nel riquadro di navigazione, fare clic su **Configurazione LDAP**.
- Fare clic su **Edit** (Modifica).
- Assicurarsi che il client appena creato sia selezionato in **Nome client LDAP**.
- Selezionare **Enable LDAP client** (attiva client LDAP) e fare clic su **OK**.

Active LDAP Client

LDAP client name:

☒ Enable LDAP client

Active Directory Domain:

Servers

SVM utilizza il nuovo client LDAP.

6. Assegnare la priorità LDAP ad altre fonti di informazioni utente, ad esempio NIS (Network Information Service) e utenti e gruppi locali:
 - a. Accedere alla finestra **SVM**.
 - b. Selezionare la SVM e fare clic su **Edit** (Modifica).
 - c. Fare clic sulla scheda **servizi**.
 - d. In **Name Service Switch**, specificare **LDAP** come origine preferita dello switch name service per i tipi di database.
 - e. Fare clic su **Save and Close** (Salva e chiudi).

Edit Storage Virtual Machine

Details Resource Allocation **Services**

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	<input type="text" value="files"/>	<input type="text" value="dns"/>	
namemap:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	
group:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>
netgroup:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>
passwd:	<input type="text" value="ldap"/>	<input type="text" value="files"/>	<input type="text" value="nis"/>

LDAP è la fonte principale delle informazioni utente per i servizi di nome e la mappatura dei nomi su questa SVM.

Mappare i nomi utente UNIX e Windows

Se il sito dispone di account utente Windows e UNIX, è necessario utilizzare la mappatura dei nomi per garantire che gli utenti Windows possano accedere ai file con

autorizzazioni UNIX e per garantire che gli utenti UNIX possano accedere ai file con autorizzazioni NTFS. La mappatura dei nomi può comprendere qualsiasi combinazione di mappatura implicita, regole di conversione e utenti predefiniti.

A proposito di questa attività

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 operazione può essere eseguita utilizzando NIS, LDAP o utenti locali. Se si dispone di due set di utenti che non corrispondono, è necessario configurare la mappatura dei nomi.

Fasi

1. Decidere un metodo di mappatura dei nomi: Regole di conversione della mappatura dei nomi, mappature utente predefinite o entrambi, tenendo conto dei seguenti fattori:
 - Le regole di conversione utilizzano espressioni regolari per convertire un nome utente in un altro, il che è utile se si desidera controllare o tenere traccia dell'accesso a un singolo livello.

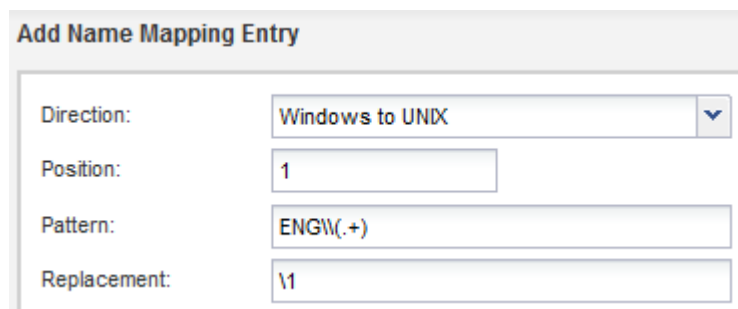
Ad esempio, è possibile mappare gli utenti UNIX agli utenti Windows di un dominio e viceversa.

- Gli utenti predefiniti consentono di assegnare un nome utente a tutti gli utenti che non sono mappati da mappature implicite o regole di conversione della mappatura dei nomi.

Ogni SVM ha un utente UNIX predefinito chiamato "pcuser" ma non ha un utente Windows predefinito.

2. Accedere alla finestra **SVM**.
3. Selezionare la SVM che si desidera configurare.
4. Fare clic sulla scheda **Impostazioni SVM**.
5. **Opzionale:** Creare una mappatura dei nomi che converte gli account utente UNIX in account utente Windows e viceversa:
 - a. Nel riquadro **host Users and Groups** (utenti e gruppi host), fare clic su **Name Mapping** (mappatura nome).
 - b. Fare clic su **Aggiungi**, mantenere la direzione predefinita **da Windows a UNIX**, quindi creare un'espressione regolare che produca una credenziale UNIX quando un utente Windows tenta di accedere a un file che utilizza le autorizzazioni per i file UNIX.

Utilizzare la seguente voce per convertire qualsiasi utente Windows nel dominio ENG in un utente UNIX con lo stesso nome. Il modello `ENG\\ (.+)` Trova qualsiasi nome utente Windows con il prefisso `ENG\\` e la sostituzione `\\1` Crea la versione UNIX rimuovendo tutto tranne il nome utente.



Add Name Mapping Entry

Direction:	Windows to UNIX
Position:	1
Pattern:	ENG\\(.+)
Replacement:	\\1

- c. Fare clic su **Aggiungi**, selezionare la direzione **da UNIX a Windows**, quindi creare il mapping corrispondente che produce una credenziale Windows quando un utente UNIX tenta di accedere a un file che dispone delle autorizzazioni per i file NTFS.

Utilizzare la seguente voce per convertire ogni utente UNIX in un utente Windows con lo stesso nome nel dominio ENG. Il modello (.+) Trova qualsiasi nome UNIX e la sostituzione ENG\\1 Crea la versione di Windows inserendo ENG\\ prima del nome utente.

Add Name Mapping Entry

Direction:	UNIX to Windows
Position:	2
Pattern:	(.+)
Replacement:	ENG\\1

- a. Poiché la posizione di ciascuna regola determina l'ordine di applicazione delle regole, è necessario esaminare il risultato e confermare che l'ordine corrisponde alle proprie aspettative.

Name Mapping

Add Edit Delete Swap Refresh		
Position	Pattern	Replacement
UNIX to Windows		
2	(.+)	ENG\\1
Windows to UNIX		
1	ENG\\(.+)	\\1

- b. Ripetere i passaggi da 5b a 5d per mappare tutti i domini e i nomi sulla SVM.

6. Opzionale: Creare un utente Windows predefinito:

- a. Creare un account utente Windows in LDAP, NIS o gli utenti locali di SVM.

Se si utilizzano utenti locali, è possibile creare un account in **Windows** nel riquadro host Users and Groups (utenti e gruppi host).

- b. Impostare l'utente Windows predefinito selezionando **NFS > Edit** nel pannello **Protocols** e immettendo il nome utente.

È possibile creare un utente Windows locale denominato "unixusers" e impostarlo come utente Windows predefinito.

7. Opzionale: Configurare l'utente UNIX predefinito se si desidera un utente diverso dal valore predefinito, ovvero l'utente "pcuser".

- a. Creare un account utente UNIX in LDAP, NIS o gli utenti locali di SVM.

Se si utilizzano utenti locali, è possibile creare un account in **UNIX** nel pannello host Users and Groups (utenti e gruppi host).

- b. Impostare l'utente UNIX predefinito selezionando **CIFS > Opzioni** nel riquadro **protocolli** e immettendo il nome utente.

È possibile creare un utente UNIX locale denominato "winusers" e impostarlo come utente UNIX

predefinito.

Cosa fare in seguito

Se sono stati configurati utenti predefiniti, quando si configurano le autorizzazioni dei file in un secondo momento nel flusso di lavoro, è necessario impostare le autorizzazioni per l'utente Windows predefinito e per l'utente UNIX predefinito.

Creare e configurare un volume

È necessario creare un volume FlexVol per contenere i dati. È possibile modificare lo stile di protezione predefinito del volume, ereditato dallo stile di protezione del volume root. È anche possibile modificare la posizione predefinita del volume nello spazio dei nomi, che si trova nel volume root della macchina virtuale di storage (SVM).

Fasi

1. Accedere alla finestra **Volumes**.
2. Fare clic su **Crea > Crea FlexVol**.

Viene visualizzata la finestra di dialogo Create Volume (Crea volume).

3. Se si desidera modificare il nome predefinito, che termina con un indicatore di data e ora, specificare un nuovo nome, ad esempio `vol1`.
4. Selezionare un aggregato per il volume.
5. Specificare le dimensioni del volume.
6. Fare clic su **Create** (Crea).

Qualsiasi nuovo volume creato in System Manager viene montato per impostazione predefinita sul volume root utilizzando il nome del volume come nome della giunzione. Quando si configurano le condivisioni CIFS, si utilizzano il percorso di giunzione e il nome della giunzione, mentre i client NFS utilizzano il percorso di giunzione e il nome della giunzione per il montaggio del volume.

7. **Opzionale:** Se non si desidera che il volume si trovi nella directory principale di SVM, modificare la posizione del nuovo volume nello spazio dei nomi esistente:

- a. Accedere alla finestra **namespace**.
- b. Selezionare **SVM** dal menu a discesa.
- c. Fare clic su **Mount**.
- d. Nella finestra di dialogo **Mount Volume**, specificare il volume, il nome del percorso di giunzione e il percorso di giunzione su cui si desidera montare il volume.
- e. Verificare il nuovo percorso di giunzione nella finestra **namespace**.

Se si desidera organizzare alcuni volumi in un volume principale denominato "data", è possibile spostare il nuovo volume "vol1" dal volume root al volume "data".

Path ▾	Storage Object
▲ + /	vs0examplecom_root
+ data	data
+ vol1	vol1

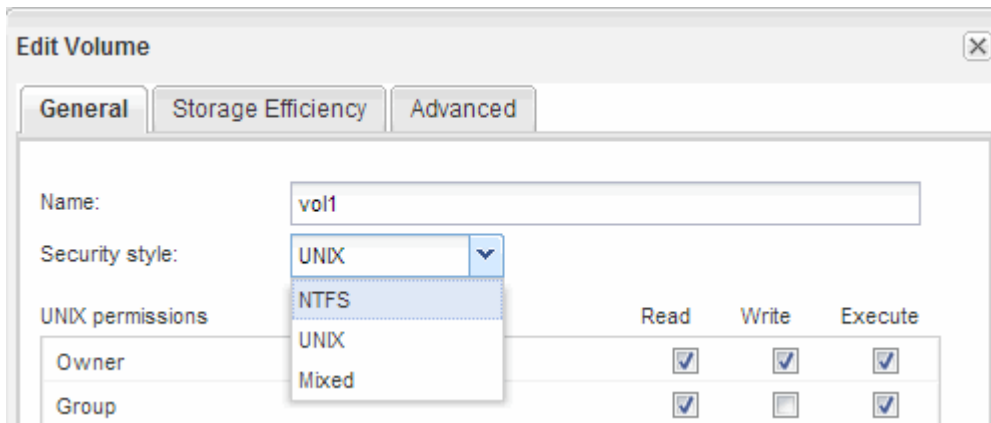
Path ▾	Storage Object
▲ + /	vs0examplecom_root
▲ + data	data
+ vol1	vol1

8. Esaminare lo stile di sicurezza del volume e modificarlo, se necessario:

- Nella finestra **Volume**, selezionare il volume appena creato e fare clic su **Edit** (Modifica).

Viene visualizzata la finestra di dialogo Edit Volume (Modifica volume), che mostra lo stile di protezione corrente del volume, ereditato dallo stile di protezione del volume root SVM.

- Selezionare lo stile di sicurezza desiderato e fare clic su **Salva e chiudi**.



Creare una condivisione e impostarne le autorizzazioni

Prima che gli utenti Windows possano accedere a un volume, è necessario creare una condivisione CIFS sul volume e limitare l'accesso alla condivisione modificando l'elenco di controllo di accesso (ACL) per la condivisione.

A proposito di questa attività

A scopo di test, è necessario consentire l'accesso solo agli amministratori. In seguito, dopo aver verificato che il volume è accessibile, è possibile consentire l'accesso a più client.

Fasi

- Accedere alla finestra **Shares**.
- Creare una condivisione in modo che i client SMB possano accedere al volume:
 - Fare clic su **Create Share** (Crea condivisione).
 - Nella finestra di dialogo **Crea condivisione**, fare clic su **Sfoggia**, espandere la gerarchia dello spazio dei nomi, quindi selezionare il volume creato in precedenza.
 - Se si desidera che il nome della condivisione sia diverso dal nome del volume, modificare il nome della condivisione.
 - Fare clic su **Create** (Crea).

La condivisione viene creata con un ACL predefinito impostato su controllo completo per il gruppo Everyone.

3. Limitare l'accesso alla condivisione modificando l'ACL della condivisione:

- a. Selezionare la condivisione, quindi fare clic su **Modifica**.
- b. Nella scheda **Permissions**, selezionare il gruppo **Everyone**, quindi fare clic su **Remove**.
- c. Fare clic su **Aggiungi**, quindi immettere il nome di un gruppo di amministratori definito nel dominio Active Directory di Windows che include SVM.
- d. Dopo aver selezionato il nuovo gruppo di amministratori, selezionare tutte le autorizzazioni.
- e. Fare clic su **Save and Close** (Salva e chiudi).

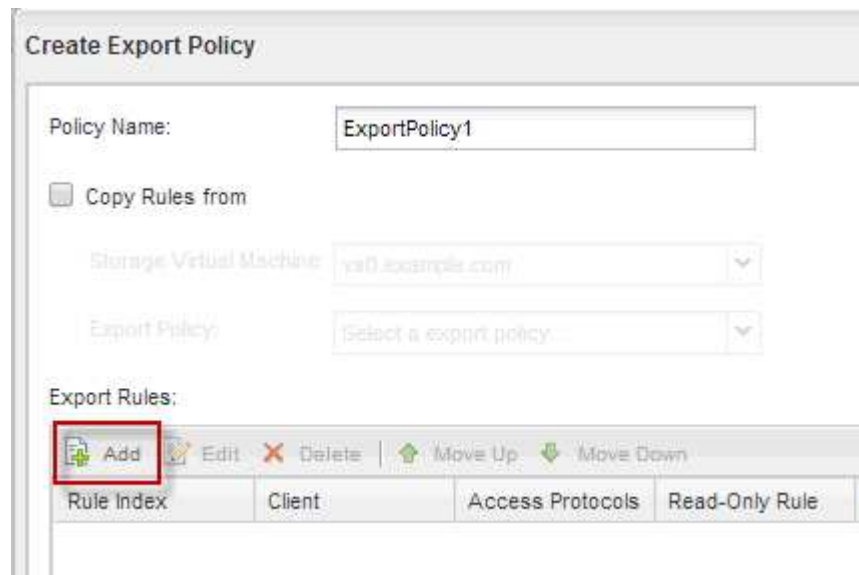
Le autorizzazioni di accesso alla condivisione aggiornate sono elencate nel pannello Share Access Control (controllo accesso alla condivisione).

Creare una policy di esportazione per il volume

Prima che qualsiasi client NFS possa accedere a un volume, è necessario creare un criterio di esportazione per il volume, aggiungere una regola che consenta l'accesso da parte di un host di amministrazione e applicare il nuovo criterio di esportazione al volume.

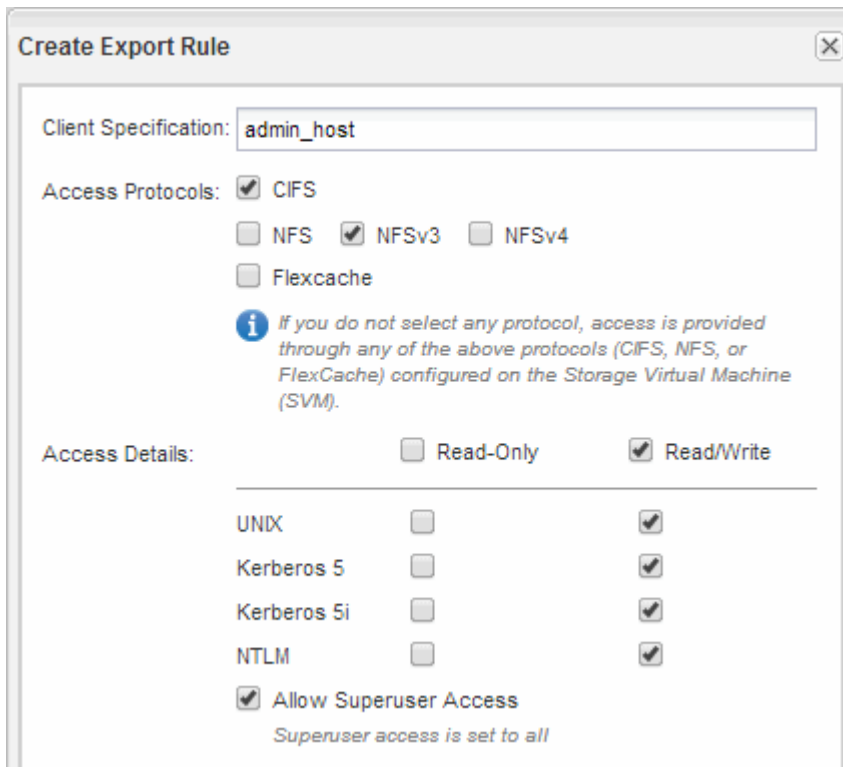
Fasi

1. Accedere alla finestra **SVM**.
2. Fare clic sulla scheda **Impostazioni SVM**.
3. Creare una nuova policy di esportazione:
 - a. Nel riquadro **Policies**, fare clic su **Export Policies** (Esporta policy), quindi su **Create** (Crea).
 - b. Nella finestra **Crea policy di esportazione**, specificare un nome di policy.
 - c. In **Esporta regole**, fare clic su **Aggiungi** per aggiungere una regola al nuovo criterio.



4. Nella finestra di dialogo **Create Export Rule** (Crea regola di esportazione), creare una regola che consenta a un amministratore di accedere all'esportazione attraverso tutti i protocolli:
 - a. Specificare l'indirizzo IP o il nome del client, ad esempio admin_host, da cui verrà amministrato il volume esportato.

- b. Selezionare **CIFS** e **NFSv3**.
- c. Assicurarsi che siano selezionati tutti i dettagli di accesso **Read/Write**, nonché **Allow Superuser Access**.



Create Export Rule

Client Specification:

Access Protocols:

- ☒ CIFS
- ☐ NFS ☒ NFSv3 ☐ NFSv4
- ☐ Flexcache

Information icon: If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Allow Superuser Access		
<i>Superuser access is set to all</i>		

- d. Fare clic su **OK**, quindi su **Crea**.

Viene creata la nuova policy di esportazione, insieme alla nuova regola.

5. Applicare il nuovo criterio di esportazione al nuovo volume in modo che l'host dell'amministratore possa accedere al volume:
 - a. Accedere alla finestra **namespace**.
 - b. Selezionare il volume e fare clic su **Change Export Policy** (Modifica policy di esportazione).
 - c. Selezionare il nuovo criterio e fare clic su **Cambia**.

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.

Verificare l'accesso NFS da un host di amministrazione UNIX

Dopo aver configurato l'accesso NFS alla macchina virtuale di storage (SVM), è necessario verificare la configurazione accedendo a un host di amministrazione NFS e leggendo i dati da e scrivendo i dati su SVM.

Prima di iniziare

- 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. Accedere come utente root al sistema client.
2. Invio `cd /mnt/` per modificare la directory nella cartella mount.
3. Creare e montare una nuova cartella utilizzando l'indirizzo IP di SVM:
 - a. Invio `mkdir /mnt/folder` per creare una nuova cartella.
 - b. Invio `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` per montare il volume in questa nuova directory.
 - c. Invio `cd folder` per modificare la directory nella nuova cartella.

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 nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Creare un nuovo file, verificarne l'esistenza e scriverne del testo:
 - a. Invio `touch filename` per creare un file di test.
 - b. Invio `ls -l filename` per verificare l'esistenza del file.
 - c. Invio `cat >filename`, Digitare del testo, quindi premere Ctrl+D per scrivere il testo nel file di prova.
 - d. Invio `cat filename` per visualizzare il contenuto del file di test.
 - e. Invio `rm filename` per rimuovere il file di test.

f. Invio `cd ..` per tornare alla directory principale.

```
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 ..
```

Risultati

Hai confermato di aver attivato l'accesso NFS a SVM.

Configurare e verificare l'accesso al client CIFS e NFS

Una volta pronti, è possibile configurare l'accesso client impostando le autorizzazioni per i file UNIX o NTFS, modificando l'ACL di condivisione e aggiungendo una regola di esportazione. Quindi, verificare che gli utenti o i gruppi interessati possano accedere al volume.

Fasi

1. Decidere quali client e utenti o gruppi avranno accesso alla condivisione.
2. Impostare le autorizzazioni del file utilizzando un metodo che corrisponde allo stile di protezione del volume:

Se lo stile di sicurezza del volume è questo...	Eseguire questa operazione...
NTFS	<ol style="list-style-type: none">a. Accedere a un client Windows come amministratore con diritti amministrativi sufficienti per gestire le autorizzazioni NTFS.b. In Esplora risorse, fare clic con il pulsante destro del mouse sull'unità, quindi selezionare Proprietà.c. Selezionare la scheda Security (sicurezza) e regolare le impostazioni di protezione per i gruppi e gli utenti in base alle esigenze.
UNIX	Su un host di amministrazione UNIX, utilizzare l'utente root per impostare la proprietà e le autorizzazioni UNIX sul volume.

3. In System Manager, modificare l'ACL della condivisione per consentire agli utenti o ai gruppi Windows di accedere alla condivisione.
 - a. Accedere alla finestra **Shares**.

- b. Selezionare la condivisione e fare clic su **Modifica**.
 - c. Selezionare la scheda **Permissions** e assegnare agli utenti o ai gruppi l'accesso alla condivisione.
4. In System Manager, aggiungere regole ai criteri di esportazione per consentire ai client NFS di accedere alla condivisione.
 - a. Selezionare la macchina virtuale di storage (SVM) e fare clic su **SVM Settings** (Impostazioni SVM).
 - b. Nel riquadro **Policies**, fare clic su **Export Policies** (Esporta policy).
 - c. Selezionare il criterio di esportazione applicato al volume.
 - d. Nella scheda **regole di esportazione**, fare clic su **Aggiungi** e specificare un set di client.
 - e. Selezionare **2** come **Rule Index** in modo che questa regola venga eseguita dopo la regola che consente l'accesso all'host di amministrazione.
 - f. Selezionare **CIFS** e **NFSv3**.
 - g. Specificare i dettagli di accesso desiderati e fare clic su **OK**.

È possibile fornire l'accesso completo in lettura/scrittura ai client digitando la subnet 10.1.1.0/24. Come **Client Specification** (specifica client) e selezionando tutte le caselle di controllo Access (accesso) ad eccezione di **Allow Superuser Access** (Consenti accesso superutente).

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols: ☐ CIFS ☐ NFS ☒ NFSv3 ☐ NFSv4 ☐ Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: ☒ Read-Only ☒ Read/Write

UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Allow Superuser Access
Superuser access is set to all

5. Su un client Windows, accedere come uno degli utenti che ora ha accesso alla condivisione e ai file e verificare di poter accedere alla condivisione e creare un file.
6. Su un client UNIX, accedere come uno degli utenti che ora ha accesso al volume e verificare che sia possibile montare il volume e creare un file.

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.