# Configurare NFS con la CLI

ONTAP 9

NetApp
April 24, 2024

# Sommario

# 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 |
|---|---|---|
| `-vserver` | 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. | |

| | | |
|---|---|---|
| `-aggregate` | Il nome di un aggregato nel cluster con spazio sufficiente per la nuova capacità di storage NFS. | |
| `-rootvolume` | Un nome univoco fornito per il volume root SVM. | |
| `-rootvolume-security-style` | Utilizzare lo stile di sicurezza UNIX per SVM. | `unix` |
| `-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` | Abilitare le versioni NFS in base alle esigenze.<br>La versione 4.2 è supportata anche in ONTAP 9.8 e versioni successive quando `v4.1` è attivato. | |
| `-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` |
| `-home-node` | Il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF. | |
| `-home-port` | La porta o il gruppo di interfacce a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF. | |
| `-address` | L'indirizzo IPv4 o IPv6 del cluster che verrà utilizzato per l'accesso ai dati dal nuovo LIF. | |
| `-netmask` | La maschera di rete e il gateway per LIF. | |
| `-subnet` | Un pool di indirizzi IP. Utilizzato al posto di `-address` e. `-netmask` per assegnare automaticamente indirizzi e netmask. | |
| `-firewall-policy` | 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 |
| --- | --- | --- |
| `-domains` | Fino a cinque nomi di dominio DNS. | |
| `-name-servers` | 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 (`-user`) | ID utente (`-id`) | ID gruppo (`-primary-gid`) | Nome completo (`-full-name`) |
|---|---|---|---|---|
| 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 |
|---|---|---|
| `-domain` | Il dominio NIS che SVM utilizzerà per la ricerca dei nomi. | |
| `-active` | Il server di dominio NIS attivo. | `true` oppure `false` |
| `-servers` | ONTAP 9.0, 9.1: Uno o più indirizzi IP dei server NIS utilizzati dalla configurazione del dominio NIS. | |
| `-nis-servers` | 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** |
|---|---|---|
| `-vserver` | Il nome della SVM per la quale si desidera creare una configurazione del client LDAP. | |
| `-client-config` | Il nome assegnato per la nuova configurazione del client LDAP. | |
| `-servers` | ONTAP 9.0, 9.1: Uno o più server LDAP in base all'indirizzo IP in un elenco separato da virgole. | |
| `-ldap-servers` | ONTAP 9.2: Un elenco separato da virgole di indirizzi IP e nomi host per i server LDAP. | |
| `-query-timeout` | Utilizzare l'impostazione predefinita `3` secondi per questo flusso di lavoro. | `3` |

| Campo | Descrizione | Il tuo valore |
| --- | --- | --- |
| `-min-bind-level` | Il livello minimo di autenticazione BIND. L'impostazione predefinita è `anonymous`. Deve essere impostato su `sasl` se la firma e il sigillo sono configurati. | |
| `-preferred-ad-servers` | Uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole. | |
| `-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. | |
| `-kdc-port` | Numero della porta KDC. | |
| `-adserver-name` | Solo Microsoft KDC: Nome DEL server AD. | |
| `-adserver-ip` | Solo Microsoft KDC: Indirizzo IP DEL SERVER AD. | |
| `-adminserver-ip` | Solo KDC UNIX: Indirizzo IP del server di amministrazione. | |
| `-adminserver-port` | Solo KDC UNIX: Numero di porta del server di amministrazione. | |
| `-passwordserver-ip` | Solo KDC UNIX: Indirizzo IP del server delle password. | |
| `-passwordserver-port` | Solo KDC UNIX: Porta del server delle password. | |
| `-kdc-vendor` | Vendor KDC. | { `Microsoft` |
| `Other` } | `-comment` | Eventuali commenti desiderati. |

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

| Campo | Descrizione | Il tuo valore |
|---|---|---|
| `-vserver` | Il nome della SVM per la quale si desidera creare una configurazione Kerberos. | |
| `-lif` | I dati LIF sui quali attivare Kerberos. È possibile attivare Kerberos su più LIF. | |

| | | |
|---|---|---|
| `-spn` | Nome del principio di servizio (SPN) | |
| `-permitted-enc-types` | I tipi di crittografia consentiti per Kerberos su NFS; `aes-256` 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. | |
| `-rwrule` | Metodo di autenticazione per l'accesso in lettura/scrittura. | |
| `-superuser` | Metodo di autenticazione per l'accesso del superutente. | |
| `-anon` | 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 |
|---|---|---|
| `-vserver` | Il nome di una SVM nuova o esistente che ospiterà il nuovo volume. | |
| `-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 NFS. | |
| `-size` | 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 `/vol/`*`volume_name/qtree_name`*`\>` 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::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -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::> vserver show -vserver 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 vserver_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** | `network interface create -vserver *vserver_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}` |
| **ONTAP 9.6 e versioni successive** | `network interface create -vserver *vserver_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}` |

- 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 | `network ping` |
| Indirizzo IPv6 | `network ping6` |

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 e1c -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 e1c -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

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         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.

**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
                                                  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 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 | `vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files` |
| Informazioni sul gruppo | `vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files` |
| Informazioni sul netgroup | `vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files` |

## 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 risolutibili 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 | Necessario per la fase DI INIT GSS.<br><br>Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.<br><br>L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS. |
| 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 adatti 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 | a. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:<br>`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*<br><br>Separare più tipi di crittografia con una virgola.<br><br>b. Verificare che la modifica sia stata eseguita correttamente:<br>`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types` |
| AES-128 o AES-256 | a. Identificare su quali SVM e LIF Kerberos sono attivati:<br>`vserver nfs kerberos interface show`<br>b. Disattiva Kerberos su tutti i LIF della SVM il cui tipo di crittografia Kerberos NFS consentiva di modificare:<br>`vserver nfs kerberos interface disable -lif` *`lif_name`*<br>c. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:<br>`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*<br><br>Separare più tipi di crittografia con una virgola.<br><br>d. Verificare che la modifica sia stata eseguita correttamente:<br>`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`<br>e. Riabilitare Kerberos su tutti i LIF su SVM:<br>`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*<br>f. Verificare che Kerberos sia attivato su tutti i LIF:<br>`vserver nfs kerberos interface show` |

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

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…** |
|---|---|
| `any` | Sempre, indipendentemente dal tipo di sicurezza in entrata. |
| `none` | 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. |
| `never` | Mai, indipendentemente dal tipo di sicurezza in entrata. |
| `krb5` | Se autenticato da Kerberos 5. Authentication Only (solo autenticazione): L'intestazione di ogni richiesta e risposta viene firmata. |
| `krb5i` | Se autenticato da Kerberos 5i. Autenticazione e integrità: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati. |
| `krb5p` | 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. |
| `ntlm` | Se autenticato da CIFS NTLM. |
| `sys` | Se autenticato da NFS AUTH_SYS. |

Il tipo di protezione consigliato è `sys`Oppure, se si utilizza Kerberos, `krb5`, `krb5i`, o. `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 | a. Visualizzare le regole esistenti nel criterio: `vserver export-policy rule show -instance -policyname` *`your_policy`*<br>b. Selezionare un numero di indice per la nuova regola in base all'ordine in cui deve essere valutata. |

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 exp1
-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      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                   Vserver: vs1
                               Policy Name: exp1
                                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::> vserver 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::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver 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 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

- 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 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 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
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   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 -v1server 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` *`vserver_name`* `-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 -v1server 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
                                        Policy    Policy     Rule
Path                     Policy         Owner     Owner Type 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 `/etc/exports` 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 | • Le esportazioni si applicano a un percorso di file o qtree specificato.<br>• È necessario creare una voce separata in `/etc/exports` per ogni percorso di file o qtree.<br>• Le esportazioni sono persistenti solo se sono definite in `/etc/exports` file. | • I criteri di esportazione si applicano a un intero volume, inclusi tutti i percorsi di file e i qtree contenuti nel volume.<br>• Se si desidera, è possibile applicare i criteri di esportazione a più volumi.<br>• 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 `/etc/exports` 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 `-actual` quando si definisce un'esportazione in `/etc/exports` file. | 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.<br>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. |

## 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 *squashed* 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_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Applicare i criteri alle qtree:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [prossimo 4 qtree…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [prossimo 4 qtree…]

Se in un secondo momento è necessario aggiungere qtree aggiuntivi per tali host, si utilizzerebbero le stesse policy di esportazione.