



# **Configurare l'accesso SMB a una SVM**

## **ONTAP 9**

NetApp  
September 12, 2024

# Sommario

- Configurare l'accesso SMB a una SVM . . . . . 1
  - Configurare l'accesso SMB a una SVM . . . . . 1
  - Creare una SVM . . . . . 1
  - Verificare che il protocollo SMB sia attivato su SVM . . . . . 3
  - Aprire la policy di esportazione del volume root SVM . . . . . 4
  - Creare una LIF . . . . . 5
  - Abilitare il DNS per la risoluzione del nome host . . . . . 8
  - Configurare un server SMB in un dominio Active Directory . . . . . 10
  - Configurare un server SMB in un gruppo di lavoro . . . . . 15
  - Verificare le versioni SMB abilitate . . . . . 20
  - Mappare il server SMB sul server DNS . . . . . 22

# Configurare l'accesso SMB a una SVM

## Configurare l'accesso SMB a una SVM

Se non si dispone già di una SVM configurata per l'accesso al client SMB, è necessario creare e configurare una nuova SVM o configurare una SVM esistente. La configurazione di SMB implica l'apertura dell'accesso al volume root SVM, la creazione di un server SMB, la creazione di una LIF, l'abilitazione della risoluzione dei nomi host, la configurazione dei servizi dei nomi e, se lo si desidera, Attivazione della sicurezza Kerberos.

## Creare una SVM

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

### Prima di iniziare

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

### Fasi

1. Creare una SVM: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`

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

2. Verificare la configurazione e lo stato della SVM appena creata: `vserver show -vserver vserver_name`

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

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

### Esempi

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

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

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

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

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



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

# Verificare che il protocollo SMB sia attivato su SVM

Prima di poter configurare e utilizzare SMB su SVM, è necessario verificare che il protocollo sia attivato.

## A proposito di questa attività

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



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

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

## Fasi

1. Controllare quali protocolli sono attualmente attivati e disattivati per SVM: `vserver show -vserver vserver_name -protocols`

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

2. Se necessario, attivare o disattivare un protocollo:

- Per attivare il protocollo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
- Per disattivare un protocollo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Verificare che i protocolli attivati e disattivati siano stati aggiornati correttamente: `vserver show -vserver vserver_name -protocols`

## Esempio

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

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                        nfs, fcp, iscsi, ndmp
```

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

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

# Aprire la policy di esportazione del volume root SVM

Il criterio di esportazione predefinito del volume root SVM deve includere una regola per consentire a tutti i client l'accesso aperto tramite SMB. Senza tale regola, a tutti i client SMB viene negato l'accesso a SVM e ai relativi volumi.

## A proposito di questa attività

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

Verificare che tutti gli accessi SMB siano aperti nel criterio di esportazione predefinito e, in seguito, limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per singoli volumi o qtree.

## Fasi

1. Se si utilizza una SVM esistente, controllare il criterio di esportazione del volume root predefinito: `vserver export-policy rule show`

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

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

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

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

2. Creare una regola di esportazione per il volume root SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verificare la creazione della regola utilizzando `vserver export-policy rule show` comando.

## Risultati

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

# Creare una LIF

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

## Prima di iniziare

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

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

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

## A proposito di questa attività

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

## Fasi

### 1. Creare una LIF:

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

#### ONTAP 9.5 e versioni precedenti

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

#### ONTAP 9.6 e versioni successive

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

```
false}`
```

- Il `-role` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6).
- Il `-data-protocol` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6). Quando si utilizza ONTAP 9,5 e versioni precedenti, il `-data-protocol` Il parametro deve essere specificato al momento della creazione della LIF e non può essere modificato in seguito senza distruggere e ricreare la LIF dei dati.
- `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

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

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

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



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

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

## 2. Verificare che la LIF sia stata creata correttamente:

```
network interface show
```

## 3. Verificare che l'indirizzo IP configurato sia raggiungibile:

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



Indirizzo IPv6	network ping6
----------------	---------------

## Esempi

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

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

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

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

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

```
network interface show
```

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

5 entries were displayed.

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

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

## Abilitare il DNS per la risoluzione del nome host

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

vengono risolti utilizzando server DNS esterni.

### Prima di iniziare

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

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

### A proposito di questa attività

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

### Fasi

1. Abilitare il DNS sulla SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

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

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



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

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

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

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

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

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

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

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

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

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

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

## Configurare un server SMB in un dominio Active Directory

### Configurare i servizi di gestione dell'orario

Prima di creare un server SMB in un controller di dominio attivo, è necessario assicurarsi che il tempo del cluster e quello dei controller di dominio del dominio a cui il server SMB appartiene corrispondano entro cinque minuti.

#### A proposito di questa attività

È necessario configurare i servizi NTP del cluster in modo che utilizzino gli stessi server NTP per la sincronizzazione dell'ora utilizzati dal dominio Active Directory.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

#### Fasi

1. Configurare i servizi di gestione del tempo utilizzando `cluster time-service ntp server create` comando.
  - Per configurare i servizi temporali senza autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_ip_address`
  - Per configurare i servizi temporali con autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_ip_address -key-id key_id`  
`cluster time-service ntp server create -server 10.10.10.1 cluster`  
`time-service ntp server create -server 10.10.10.2`


2. Verificare che i servizi di orario siano impostati correttamente utilizzando `cluster time-service ntp server show` comando.


```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

## Comandi per la gestione dell'autenticazione simmetrica sui server NTP

A partire da ONTAP 9.5, è supportato il protocollo NTP (Network Time Protocol) versione 3. NTPv3 include l'autenticazione simmetrica utilizzando chiavi SHA-1 che aumenta la sicurezza della rete.

A tal fine...	Utilizzare questo comando...
Configurare un server NTP senza autenticazione simmetrica	<code>cluster time-service ntp server create -server server_name</code>
Configurare un server NTP con autenticazione simmetrica	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Abilitare l'autenticazione simmetrica per un server NTP esistente. È possibile modificare il server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configurare una chiave NTP condivisa	<code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <div> Le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP</div>
Configurare un server NTP con un ID chiave sconosciuto	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>

A tal fine...	Utilizzare questo comando...
Configurare un server con un ID chiave non configurato sul server NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>L'ID, il tipo e il valore della chiave devono essere identici all'ID, al tipo e al valore della chiave configurati sul server NTP.</p> </div>
Disattiva autenticazione simmetrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

## Creare un server SMB in un dominio Active Directory

È possibile utilizzare `vserver cifs create` Per creare un server SMB su SVM e specificare il dominio Active Directory (ad) a cui appartiene.

### Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM e a un domain controller ad del dominio a cui si desidera accedere al server SMB.

Qualsiasi utente autorizzato a creare account di computer nel dominio ad a cui si sta entrando nel server SMB può creare il server SMB su SVM. Questo può includere utenti di altri domini.

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

### A proposito di questa attività

Quando si crea un server SMB in un dominio di Activity Directory:

- Quando si specifica il dominio, è necessario utilizzare il nome di dominio completo (FQDN).
- L'impostazione predefinita prevede l'aggiunta dell'account della macchina server SMB all'oggetto CN=computer di Active Directory.
- È possibile scegliere di aggiungere il server SMB a un'unità organizzativa (OU) diversa utilizzando `-ou` opzione.
- È possibile scegliere di aggiungere un elenco delimitato da virgole di uno o più alias NetBIOS (fino a 200) per il server SMB.

La configurazione degli alias NetBIOS per un server SMB può essere utile quando si consolidano i dati da altri file server al server SMB e si desidera che il server SMB risponda ai nomi dei server originali.

Il `vserver cifs` le pagine man contengono ulteriori parametri opzionali e requisiti di denominazione.



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

A partire da ONTAP 9.8, è possibile specificare che le connessioni ai controller di dominio siano crittografate. ONTAP richiede la crittografia per le comunicazioni del controller di dominio quando `-encryption -required-for-dc-connection` l'opzione è impostata su `true`; il valore predefinito è `false`. Quando l'opzione è impostata, per le connessioni ONTAP-DC verrà utilizzato solo il protocollo SMB3, in quanto la crittografia è supportata solo da SMB3. .

"[Gestione delle PMI](#)" Contiene ulteriori informazioni sulle opzioni di configurazione del server SMB.

## Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un dominio ad: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Quando si entra in un dominio, il completamento di questo comando potrebbe richiedere alcuni minuti.

Il seguente comando crea il server SMB "smb\_server01" nel dominio "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

Il seguente comando crea il server SMB "smb\_server02" nel dominio "mydomain.com" e autentica l'amministratore ONTAP con un file keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

In questo esempio, l'output del comando mostra che un server SMB denominato "SMB\_SERVER01" è stato creato su SVM vs1.example.com ed è stato Unito al dominio "example.com".

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

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. Se lo si desidera, attivare la comunicazione crittografata con il controller di dominio (ONTAP 9.8 e versioni successive): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

### Esempi

Il seguente comando crea un server SMB denominato “smb\_server02” su SVM vs2.example.com nel dominio “example.com”. L’account del computer viene creato nel contenitore “OU=eng,OU=corp,DC=example,DC=com”. Al server SMB viene assegnato un alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

Il seguente comando consente a un utente di un dominio diverso, in questo caso un amministratore di un dominio attendibile, di creare un server SMB denominato “smb\_server03” su SVM vs3.example.com. Il `-domain` Option specifica il nome del dominio principale (specificato nella configurazione DNS) in cui si desidera creare il server SMB. Il `username` consente di specificare l’amministratore del dominio attendibile.

- Dominio domestico: example.com
- Dominio attendibile: trust.lab.com
- Nome utente del dominio trusted: Administrator1



```
cluster1::> vsync cifs create -vsync vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

Username: Administrator1@trust.lab.com

Password: . . .

## Creare file keytab per l'autenticazione SMB

A partire da ONTAP 9.7, ONTAP supporta l'autenticazione SVM con server Active Directory (ad) utilizzando file keytab. Gli amministratori DEGLI ANNUNCI generano un file keytab e lo rendono disponibile agli amministratori di ONTAP come URI (Uniform Resource Identifier), che viene fornito quando `vsync cifs` I comandi richiedono l'autenticazione Kerberos con il dominio ad.

Gli amministratori DEGLI ANNUNCI possono creare i file keytab utilizzando Windows Server standard `ktpass` comando. Il comando deve essere eseguito sul dominio primario in cui è richiesta l'autenticazione. Il `ktpass` il comando può essere utilizzato per generare i file keytab solo per gli utenti del dominio primario; le chiavi generate utilizzando gli utenti del dominio trusted non sono supportate.

I file keytab vengono generati per specifici utenti amministratori di ONTAP. Se la password dell'utente amministratore non viene modificata, le chiavi generate per il tipo di crittografia e il dominio specifico non verranno modificate. Pertanto, è necessario un nuovo file keytab ogni volta che viene modificata la password dell'utente amministratore.

Sono supportati i seguenti tipi di crittografia:

- AES256-SHA1
- DES-CBC-MD5



ONTAP non supporta il tipo di crittografia DES-CBC-CRC.

- RC4-HMAC

AES256 è il tipo di crittografia più elevato e deve essere utilizzato se abilitato sul sistema ONTAP.

I file keytab possono essere generati specificando la password admin o utilizzando una password generata casualmente. Tuttavia, in qualsiasi momento è possibile utilizzare una sola opzione di password, poiché sul server ad è necessaria una chiave privata specifica per l'utente amministratore per decifrare le chiavi all'interno del file keytab. Qualsiasi modifica della chiave privata per un amministratore specifico invaliderà il file keytab.

## Configurare un server SMB in un gruppo di lavoro

### Configurare un server SMB in una panoramica del gruppo di lavoro

L'impostazione di un server SMB come membro di un gruppo di lavoro consiste nella creazione del server SMB e quindi nella creazione di utenti e gruppi locali.

È possibile configurare un server SMB in un gruppo di lavoro quando l'infrastruttura di dominio Microsoft Active Directory non è disponibile.

Un server SMB in modalità workgroup supporta solo l'autenticazione NTLM e non l'autenticazione Kerberos.

## Creare un server SMB in un gruppo di lavoro

È possibile utilizzare `vserver cifs create` Per creare un server SMB sulla SVM e specificare il gruppo di lavoro a cui appartiene.

### Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM.

### A proposito di questa attività

I server SMB in modalità workgroup non supportano le seguenti funzionalità SMB:

- Protocollo di controllo SMB3
- Condivisioni SMB3 CA
- SQL su SMB
- Reindirizzamento cartelle
- Profili roaming
- Oggetto Criteri di gruppo (GPO)
- Servizio Volume Snapshot (VSS)

Il `vserver cifs` le pagine man contengono ulteriori parametri di configurazione opzionali e requisiti di denominazione.

### Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un gruppo di lavoro: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

Il seguente comando crea il server SMB "smb\_server01" nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

Nell'esempio seguente, l'output del comando mostra che un server SMB denominato "smb\_server01" è stato creato su SVM vs1.example.com nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

### Al termine

Per un server CIFS in un gruppo di lavoro, è necessario creare utenti locali e, facoltativamente, gruppi locali su SVM.

### Informazioni correlate

["Gestione delle PMI"](#)

## Creare account utente locali

È possibile creare un account utente locale da utilizzare per autorizzare l'accesso ai dati contenuti nella SVM tramite una connessione SMB. È inoltre possibile utilizzare account utente locali per l'autenticazione quando si crea una sessione SMB.

### A proposito di questa attività

La funzionalità utente locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un account utente locale, è necessario specificare un nome utente e la SVM a cui associare l'account.

Il `vserver cifs users-and-groups local-user` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

### Fasi

1. Creare l'utente locale: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Potrebbero essere utili i seguenti parametri opzionali:

- `-full-name`

Il nome completo dell'utente.

- `-description`

Una descrizione per l'utente locale.

◦ `-is-account-disabled {true|false}`

Specifica se l'account utente è attivato o disattivato. Se questo parametro non viene specificato, l'impostazione predefinita prevede l'attivazione dell'account utente.

Il comando richiede la password dell'utente locale.

2. Immettere una password per l'utente locale, quindi confermarla.
3. Verificare che l'utente sia stato creato correttamente: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene creato un utente locale "SMB\_SERVER01 `Ssue", con il nome completo "ue Chang", associato a SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator    Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

## Creare gruppi locali

È possibile creare gruppi locali che possono essere utilizzati per autorizzare l'accesso ai dati associati alla SVM tramite una connessione SMB. È inoltre possibile assegnare privilegi che definiscono i diritti o le funzionalità di un membro del gruppo.

### A proposito di questa attività

La funzionalità del gruppo locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un gruppo locale, è necessario specificare un nome per il gruppo e la SVM a cui associare il gruppo. È possibile specificare un nome di gruppo con o senza il nome di dominio locale ed è possibile specificare una descrizione per il gruppo locale. Non è possibile aggiungere un gruppo locale a un altro gruppo locale.

Il `vserver cifs users-and-groups local-group` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

### Fasi

1. Creare il gruppo locale: `vserver cifs users-and-groups local-group create -vserver`

```
vserver_name -group-name group_name
```

Potrebbe essere utile il seguente parametro opzionale:

- -description

Una descrizione per il gruppo locale.

2. Verificare che il gruppo sia stato creato correttamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene creato un gruppo locale "SMB\_SERVER01\engineering" associato a SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver  
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver  
vs1.example.com
```

Vserver	Group Name	Description
-----	-----	-----
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
group		
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
		privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

### Al termine

È necessario aggiungere membri al nuovo gruppo.

## Gestire l'appartenenza al gruppo locale

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

### A proposito di questa attività

Se non si desidera più che un utente locale, un utente di dominio o un gruppo di dominio disponga di diritti di accesso o privilegi in base all'appartenenza a un gruppo, è possibile rimuovere il membro dal gruppo.

Quando si aggiungono membri a un gruppo locale, è necessario tenere presente quanto segue:

- Non è possibile aggiungere utenti al gruppo speciale *Everyone*.

- Non è possibile aggiungere un gruppo locale a un altro gruppo locale.
- Per aggiungere un utente o un gruppo di dominio a un gruppo locale, ONTAP deve essere in grado di risolvere il nome in un SID.

Quando rimuovi membri da un gruppo locale, devi tenere presente quanto segue:

- Non puoi rimuovere membri dal gruppo speciale *Everyone*.
- Per rimuovere un membro da un gruppo locale, ONTAP deve essere in grado di risolvere il proprio nome in un SID.

## Fasi

### 1. Aggiungere o rimuovere un membro da un gruppo.

- Aggiungere un membro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.

- Rimuovere un membro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.

## Esempi

Nell'esempio seguente viene aggiunto un utente locale "SMB\_SERVER01\ sue" al gruppo locale "SMB\_SERVER01 engineering" su SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Nell'esempio seguente vengono rimossi gli utenti locali "SMB\_SERVER01\ sue" e "SMB\_SERVER01 \Sjames" dal gruppo locale "SMB\_SERVER01 Engineering" su SVM vs1.example.com:

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

## Verificare le versioni SMB abilitate

La release di ONTAP 9 determina quali versioni SMB sono abilitate per impostazione predefinita per le connessioni con client e controller di dominio. Verificare che il server SMB supporti i client e le funzionalità richieste nell'ambiente.

### A proposito di questa attività

Per le connessioni con client e controller di dominio, è necessario attivare SMB 2.0 e versioni successive, se possibile. Per motivi di sicurezza, è consigliabile evitare di utilizzare SMB 1.0 e disattivarlo se si è verificato che non è richiesto nell'ambiente in uso.

In ONTAP 9, le versioni SMB 2.0 e successive sono attivate per impostazione predefinita per le connessioni client, ma la versione di SMB 1.0 attivata per impostazione predefinita dipende dalla versione di ONTAP in uso.

- A partire da ONTAP 9.1 P8, SMB 1.0 può essere disattivato sulle SVM.

Il `-smb1-enabled` al `vserver cifs options modify` Il comando attiva o disattiva SMB 1.0.

- A partire da ONTAP 9.3, viene disattivato per impostazione predefinita sui nuovi SVM.

Se il server SMB si trova in un dominio Active Directory (ad), è possibile abilitare SMB 2.0 per la connessione a un controller di dominio (DC) che inizia con ONTAP 9.1. Questa operazione è necessaria se SMB 1.0 è stato disattivato sui controller di dominio. A partire da ONTAP 9.2, SMB 2.0 è attivato per impostazione predefinita per le connessioni DC.



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

["Gestione delle PMI"](#) Contiene dettagli sulle versioni e sulle funzionalità SMB supportate.

## Fasi

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

```
set -privilege advanced
```

2. Verificare quali versioni SMB sono abilitate:

```
vserver cifs options show
```

È possibile scorrere l'elenco per visualizzare le versioni SMB abilitate per le connessioni client e, se si configura un server SMB in un dominio ad, per le connessioni di dominio ad.

3. Attivare o disattivare il protocollo SMB per le connessioni client secondo necessità:

- Per attivare una versione SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>  
true
```

Valori possibili per `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`

- -smb31-enabled

Questo comando abilita SMB 3,1 in SVM vs1.example.com: cluster1::\*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true

- Per disattivare una versione SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>  
false
```

4. Se il server SMB si trova in un dominio Active Directory, attivare o disattivare il protocollo SMB per le connessioni DC come richiesto:

- Per attivare una versione SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled  
-for-dc-connections true
```

- Per disattivare una versione SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled  
-for-dc-connections false
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Mappare il server SMB sul server DNS

Il server DNS del sito deve avere una voce che punta il nome del server SMB e qualsiasi alias NetBIOS all'indirizzo IP del LIF dei dati, in modo che gli utenti Windows possano mappare un disco al nome del server SMB.

### Prima di iniziare

È necessario disporre dell'accesso amministrativo al server DNS del sito. Se non si dispone dell'accesso amministrativo, è necessario chiedere all'amministratore DNS di eseguire questa attività.

### A proposito di questa attività

Se si utilizzano alias NetBIOS per il nome del server SMB, si consiglia di creare punti di ingresso del server DNS per ciascun alias.

### Fasi

1. Accedere al server DNS.
2. Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il



nome del server SMB all'indirizzo IP dei dati LIF.

3. Se si utilizzano alias NetBIOS, creare una voce di ricerca Alias Canonical name (CNAME resource record) per mappare ciascun alias all'indirizzo IP dei dati LIF del server SMB.

## **Risultati**

Una volta propagata la mappatura in rete, gli utenti di Windows possono mappare un disco al nome del server SMB o ai relativi alias NetBIOS.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.