# Creazione di configurazioni ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB

ONTAP 9

NetApp
April 24, 2024

# Sommario

# Creazione di configurazioni ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB

## Crea configurazioni ONTAP per operazioni senza interruzioni con la panoramica di Hyper-V e SQL Server su SMB

Per preparare le installazioni di ONTAP e Hyper-V, è necessario eseguire diverse operazioni di configurazione di SQL Server che forniscono operazioni senza interruzioni su SMB.

Prima di creare la configurazione ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB, è necessario completare le seguenti attività:

- I servizi Time devono essere impostati sul cluster.
- È necessario configurare la rete per SVM.
- È necessario creare la SVM.
- Le interfacce Data LIF devono essere configurate su SVM.
- Il DNS deve essere configurato sulla SVM.
- I servizi Names desiderati devono essere impostati per la SVM.
- È necessario creare il server SMB.

**Informazioni correlate**

Pianificare la configurazione di Hyper-V o SQL Server su SMB

Requisiti di configurazione e considerazioni

## Verificare che sia consentita l'autenticazione Kerberos e NTLMv2 (Hyper-V su condivisioni SMB)

Le operazioni senza interruzioni per Hyper-V su SMB richiedono che il server CIFS su una SVM dati e il server Hyper-V consentano l'autenticazione Kerberos e NTLMv2. È necessario verificare le impostazioni sul server CIFS e sui server Hyper-V che controllano i metodi di autenticazione consentiti.

**A proposito di questa attività**

L'autenticazione Kerberos è necessaria quando si effettua una connessione di condivisione continuamente disponibile. Parte del processo VSS remoto utilizza l'autenticazione NTLMv2. Pertanto, le connessioni che utilizzano entrambi i metodi di autenticazione devono essere supportate per le configurazioni Hyper-V su SMB.

È necessario configurare le seguenti impostazioni per consentire l'autenticazione Kerberos e NTLMv2:

- I criteri di esportazione per SMB devono essere disattivati sulla macchina virtuale di storage (SVM).

L'autenticazione Kerberos e NTLMv2 è sempre abilitata sulle SVM, ma è possibile utilizzare i criteri di esportazione per limitare l'accesso in base al metodo di autenticazione.

I criteri di esportazione per SMB sono opzionali e sono disattivati per impostazione predefinita. Se i criteri di esportazione sono disattivati, l'autenticazione Kerberos e NTLMv2 è consentita per impostazione predefinita su un server CIFS.

- Il dominio a cui appartengono il server CIFS e i server Hyper-V deve consentire l'autenticazione Kerberos e NTLMv2.

L'autenticazione Kerberos è attivata per impostazione predefinita nei domini Active Directory. Tuttavia, l'autenticazione NTLMv2 può essere non consentita, utilizzando le impostazioni dei criteri di protezione o i criteri di gruppo.

**Fasi**

1. Eseguire le seguenti operazioni per verificare che i criteri di esportazione siano disattivati su SVM:
   a. Impostare il livello di privilegio su Advanced (avanzato):

      ```
      set -privilege advanced
      ```

   b. Verificare che il `-is-exportpolicy-enabled` L'opzione del server CIFS è impostata su `false`:

      ```
      vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
      ```

   c. Tornare al livello di privilegio admin:

      ```
      set -privilege admin
      ```

2. Se i criteri di esportazione per SMB non sono disattivati, disabilitarli:

   ```
   vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
   ```

3. Verificare che l'autenticazione NTLMv2 e Kerberos sia consentita nel dominio.

   Per informazioni sulla determinazione dei metodi di autenticazione consentiti nel dominio, consultare la Microsoft TechNet Library.

4. Se il dominio non consente l'autenticazione NTMLv2, attivare l'autenticazione NTLMv2 utilizzando uno dei metodi descritti nella documentazione Microsoft.

**Esempio**

I seguenti comandi verificano che i criteri di esportazione per SMB siano disattivati su SVM vs1:

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

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

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

# Verificare che gli account di dominio siano associati all'utente UNIX predefinito

Hyper-V e SQL Server utilizzano gli account di dominio per creare connessioni SMB alle condivisioni continuamente disponibili. Per creare correttamente la connessione, l'account del computer deve essere mappato correttamente a un utente UNIX. Il modo più conveniente per eseguire questa operazione consiste nel mappare l'account del computer all'utente UNIX predefinito.

#### A proposito di questa attività

Hyper-V e SQL Server utilizzano gli account dei computer di dominio per creare connessioni SMB. Inoltre, SQL Server utilizza un account utente di dominio come account di servizio che effettua anche connessioni SMB.

Quando si crea una macchina virtuale per lo storage (SVM), ONTAP crea automaticamente l'utente predefinito "pcuser" (con un UID di `65534`) E il gruppo denominato "pcuser" (con un GID di `65534`) e aggiunge l'utente predefinito al gruppo "pcuser". Se si configura una soluzione Hyper-V su SMB su una SVM esistente prima dell'aggiornamento del cluster a Data ONTAP 8.2, l'utente e il gruppo predefiniti potrebbero non esistere. In caso contrario, è necessario crearli prima di configurare l'utente UNIX predefinito del server CIFS.

#### Fasi

1. Determinare se esiste un utente UNIX predefinito:

   **`vserver cifs options show -vserver`** ***`vserver_name`***

2. Se l'opzione utente predefinita non è impostata, determinare se esiste un utente UNIX che può essere designato come utente UNIX predefinito:

   **`vserver services unix-user show -vserver`** ***`vserver_name`***

3. Se l'opzione utente predefinita non è impostata e non esiste un utente UNIX che può essere designato come utente UNIX predefinito, creare l'utente UNIX predefinito e il gruppo predefinito, quindi aggiungere l'utente predefinito al gruppo.

In genere, all'utente predefinito viene assegnato il nome utente "pcuser" e deve essere assegnato l'UID di `65534`. Al gruppo predefinito viene generalmente assegnato il nome "pcuser". Il GID assegnato al gruppo deve essere `65534`.

a. Creare il gruppo predefinito:
**`vserver services unix-group create -vserver vserver_name -name pcuser -id 65534`**

b. Creare l'utente predefinito e aggiungerlo al gruppo predefinito:
**`vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534`**

c. Verificare che l'utente e il gruppo predefinito siano configurati correttamente:
**`vserver services unix-user show -vserver vserver_name`**+ **`vserver services unix-group show -vserver vserver_name -members`**

4. Se l'utente predefinito del server CIFS non è configurato, eseguire le seguenti operazioni:

   a. Configurare l'utente predefinito:

   **`vserver cifs options modify -vserver *vserver_name`** `-default-unix-user pcuser*`

   b. Verificare che l'utente UNIX predefinito sia configurato correttamente:

   **`vserver cifs options show -vserver vserver_name`**

5. Per verificare che l'account del computer del server applicazioni sia associato correttamente all'utente predefinito, mappare un'unità a una condivisione che risiede sulla SVM e confermare l'associazione dell'utente Windows all'utente UNIX utilizzando `vserver cifs session show` comando.

   Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

**Esempio**

I seguenti comandi determinano che l'utente predefinito del server CIFS non è impostato, ma determinano l'esistenza dell'utente "pcuser" e del gruppo "pcuser". L'utente "pcuser" viene assegnato come utente predefinito del server CIFS su SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

```
cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

## Verificare che lo stile di protezione del volume root SVM sia impostato su NTFS

Per garantire il successo delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB, i volumi devono essere creati con lo stile di sicurezza NTFS. Poiché lo stile di sicurezza del volume root viene applicato per impostazione predefinita ai volumi creati sulla macchina virtuale di storage (SVM), lo stile di sicurezza del volume root deve essere impostato su NTFS.

**A proposito di questa attività**

- È possibile specificare lo stile di sicurezza del volume root al momento della creazione di SVM.

- Se SVM non viene creato con il volume root impostato sullo stile di protezione NTFS, è possibile modificare lo stile di protezione in un secondo momento utilizzando `volume modify` comando.

**Fasi**

1. Determinare lo stile di sicurezza corrente del volume root SVM:

   **`volume show -vserver vserver_name -fields vserver,volume,security-style`**

2. Se il volume root non è un volume di sicurezza NTFS, impostare lo stile di protezione su NTFS:

   **`volume modify -vserver vserver_name -volume root_volume_name -security-style ntfs`**

3. Verificare che il volume root SVM sia impostato sullo stile di protezione NTFS:

   **`volume show -vserver vserver_name -fields vserver,volume,security-style`**

**Esempio**

I seguenti comandi verificano che lo stile di protezione del volume root sia NTFS su SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

# Verificare che le opzioni del server CIFS richieste siano configurate

È necessario verificare che le opzioni del server CIFS richieste siano attivate e configurate in base ai requisiti delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

**A proposito di questa attività**

- SMB 2.x e SMB 3.0 devono essere abilitati.
- L'offload delle copie di ODX deve essere abilitato per utilizzare l'offload delle copie che migliora le performance.
- I servizi di copia shadow di VSS devono essere attivati se la soluzione Hyper-V su SMB utilizza servizi di backup abilitati per VSS remoto (solo Hyper-V).

**Fasi**

1. Verificare che le opzioni del server CIFS richieste siano attivate sulla macchina virtuale di storage (SVM):
   a. Impostare il livello di privilegio su Advanced (avanzato):

      ```
      set -privilege advanced
      ```

   b. Immettere il seguente comando:

      ```
      vserver cifs options show -vserver vserver_name
      ```

      Le seguenti opzioni devono essere impostate su `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Solo Hyper-V)
2. Se una delle opzioni non è impostata su `true`, eseguire le seguenti operazioni:
   a. Impostarli su `true` utilizzando `vserver cifs options modify` comando.
   b. Verificare che le opzioni siano impostate su `true` utilizzando `vserver cifs options show` comando.
3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

**Esempio**

I seguenti comandi verificano che le opzioni richieste per la configurazione Hyper-V su SMB siano attivate su SVM vs1. Nell'esempio, l'offload delle copie ODX deve essere abilitato per soddisfare i requisiti delle opzioni.

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

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

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

# Configurare SMB multicanale per performance e ridondanza

A partire da ONTAP 9.4, è possibile configurare SMB multicanale in modo da fornire più connessioni tra ONTAP e client in una singola sessione SMB. In questo modo si migliora il throughput e la tolleranza agli errori per Hyper-V e SQL Server rispetto alle configurazioni SMB.

#### Di cosa hai bisogno

È possibile utilizzare la funzionalità SMB multicanale solo quando i client negoziano con SMB 3.0 o versioni successive. SMB 3.0 e versioni successive sono attivate sul server SMB ONTAP per impostazione predefinita.

#### A proposito di questa attività

I client SMB rilevano e utilizzano automaticamente più connessioni di rete se viene identificata una configurazione corretta nel cluster ONTAP.

Il numero di connessioni simultanee in una sessione SMB dipende dalle schede NIC implementate:

- **NIC 1G su client e cluster ONTAP**

  Il client stabilisce una connessione per NIC e associa la sessione a tutte le connessioni.

- **NIC da 10 G e capacità superiore su cluster client e ONTAP**

  Il client stabilisce fino a quattro connessioni per NIC e associa la sessione a tutte le connessioni. Il client può stabilire connessioni su più NIC da 10 G e capacità maggiore.

È inoltre possibile modificare i seguenti parametri (privilegio avanzato):

- **`-max-connections-per-session`**

  Numero massimo di connessioni consentite per sessione multicanale. L'impostazione predefinita è 32 connessioni.

  Se si desidera attivare più connessioni rispetto a quelle predefinite, è necessario apportare modifiche simili alla configurazione del client, che ha anche un valore predefinito di 32 connessioni.

- **`-max-lifs-per-session`**

  Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. L'impostazione predefinita è 256 interfacce di rete.

**Fasi**

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

   ```
   set -privilege advanced
   ```

2. Abilitare SMB Multichannel sul server SMB:

   ```
   vserver cifs options modify -vserver vserver_name -is-multichannel-enabled
   true
   ```

3. Verificare che ONTAP stia segnalando sessioni multicanale SMB:

   ```
   vserver cifs session options show
   ```

4. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

**Esempio**

Nell'esempio seguente vengono visualizzate informazioni su tutte le sessioni SMB, che mostrano più connessioni per una singola sessione:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate su una sessione SMB con id sessione 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                   NetBIOS Name: -
```

## Creare volumi di dati NTFS

È necessario creare volumi di dati NTFS sulla macchina virtuale di storage (SVM) prima di poter configurare condivisioni continuamente disponibili per l'utilizzo con Hyper-V o

SQL Server su server applicazioni SMB. Utilizzare il foglio di lavoro per la configurazione del volume per creare i volumi di dati.

**A proposito di questa attività**

Per personalizzare un volume di dati, è possibile utilizzare parametri opzionali. Per ulteriori informazioni sulla personalizzazione dei volumi, vedere xref:./smb-hyper-v-sql/"Gestione dello storage logico".

Durante la creazione dei volumi di dati, non è necessario creare punti di giunzione all'interno di un volume contenente quanto segue:

- File Hyper-V per i quali ONTAP crea copie shadow
- File di database di SQL Server di cui viene eseguito il backup mediante SQL Server

> Se si crea inavvertitamente un volume che utilizza uno stile di sicurezza misto o UNIX, non è possibile modificare il volume in un volume di sicurezza NTFS e utilizzarlo direttamente per creare condivisioni continuamente disponibili per operazioni senza interruzioni. Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB non funzionano correttamente, a meno che i volumi utilizzati nella configurazione non vengano creati come volumi di sicurezza NTFS.è necessario eliminare il volume e ricrearlo con lo stile di protezione NTFS, In alternativa, è possibile mappare il volume su un host Windows e applicare un ACL nella parte superiore del volume e propagare l'ACL a tutti i file e cartelle del volume.

**Fasi**

1. Creare il volume di dati immettendo il comando appropriato:

| Se si desidera creare un volume in una SVM in cui lo stile di sicurezza del volume root è… | Immettere il comando… |
|---|---|
| NTFS | `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB\|MB\|GB\|TB\|PB] -junction-path path` |
| Non NTFS | `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB\|MB\|GB\|TB\|PB]-security-style ntfs -junction-path path` |

2. Verificare che la configurazione del volume sia corretta:

   `volume show -vserver vserver_name -volume volume_name`

# Creare condivisioni SMB continuamente disponibili

Dopo aver creato i volumi di dati, è possibile creare le condivisioni continuamente disponibili utilizzate dai server applicazioni per accedere alla macchina virtuale Hyper-V, ai file di configurazione e ai file di database di SQL Server. È necessario utilizzare il foglio

di lavoro di configurazione della condivisione per creare le condivisioni SMB.

**Fasi**

1. Visualizzare informazioni sui volumi di dati esistenti e sui relativi percorsi di giunzione:

   **`volume show -vserver vserver_name -junction`**

2. Creare una condivisione SMB sempre disponibile:

   **`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties oplocks,continuously-available -symlink "" [-comment text]`**

   - È possibile aggiungere un commento alla configurazione della condivisione.
   - Per impostazione predefinita, la proprietà di condivisione dei file offline è configurata sulla condivisione ed è impostata su `manual`.
   - ONTAP crea la condivisione con l'autorizzazione di condivisione predefinita di `Everyone` / `Full Control`.

3. Ripetere il passaggio precedente per tutte le condivisioni nel foglio di lavoro di configurazione della condivisione.
4. Verificare che la configurazione sia corretta utilizzando `vserver cifs share show` comando.
5. Configurare le autorizzazioni dei file NTFS sulle condivisioni continuamente disponibili mappando un disco a ciascuna condivisione e configurando le autorizzazioni dei file utilizzando la finestra **Proprietà di Windows**.

**Esempio**

I seguenti comandi creano una condivisione continuamente disponibile denominata "data2" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. I collegamenti simbolici vengono disattivati impostando `-symlink` parametro a. `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

# Aggiungere il privilegio SeSecurityPrivilege all'account utente (per SQL Server delle condivisioni SMB)

All'account utente di dominio utilizzato per l'installazione del server SQL deve essere assegnato il privilegio "SeSecurityPrivilege" per eseguire determinate azioni sul server CIFS che richiedono privilegi non assegnati per impostazione predefinita agli utenti di dominio.

#### Di cosa hai bisogno

L'account di dominio utilizzato per l'installazione di SQL Server deve già esistere.

#### A proposito di questa attività

Quando si aggiunge il privilegio all'account del programma di installazione di SQL Server, ONTAP potrebbe validare l'account contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

**Fasi**

1. Aggiungere il privilegio “SeSecurityPrivilege”:

   **`vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name account_name -privileges SeSecurityPrivilege`**

   Il valore di `-user-or-group-name` Parameter è il nome dell’account utente di dominio utilizzato per l’installazione di SQL Server.

2. Verificare che il privilegio sia applicato all’account:

   **`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name account_name`**

**Esempio**

Il seguente comando aggiunge il privilegio “SeSecurityPrivilege” all’account del programma di installazione di SQL Server nel dominio DI ESEMPIO per la macchina virtuale di storage (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

# Configurare la profondità della directory della copia shadow VSS (per Hyper-V su condivisioni SMB)

Facoltativamente, è possibile configurare la profondità massima delle directory all’interno delle condivisioni SMB su cui creare le copie shadow. Questo parametro è utile se si desidera controllare manualmente il livello massimo di sottodirectory in cui ONTAP deve creare copie shadow.

**Di cosa hai bisogno**

La funzione di copia shadow del VSS deve essere attivata.

**A proposito di questa attività**

L’impostazione predefinita prevede la creazione di copie shadow per un massimo di cinque sottodirectory. Se il valore è impostato su `0`, ONTAP crea copie shadow per tutte le sottodirectory.

> Sebbene sia possibile specificare che la profondità della directory shadow set copy includa più di cinque sottodirectory o tutte le sottodirectory, Microsoft richiede che la creazione del set di copie shadow venga completata entro 60 secondi. La creazione del set di copie shadow non riesce se non può essere completata entro questo intervallo di tempo. La profondità della directory di copia shadow scelta non deve far superare il tempo di creazione.

**Fasi**

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

   ```
   set -privilege advanced
   ```

2. Impostare la profondità della directory della copia shadow del VSS al livello desiderato:

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer
   ```

   ```
   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```