



# Hyper-V over SMB および SQL Server over SMB

でノンストップオペレーションを実現するための **ONTAP** 設定を作成します

ONTAP 9

NetApp  
May 09, 2024

# 目次

Hyper-V over SMB および SQL Server over SMB でノンストップオペレーションを実現するための ONTAP 設定を作成します .....	1
Hyper-V および SQL Server over SMB の概要を使用して、ノンストップオペレーション用の ONTAP 設定を作成します .....	1
Kerberos 認証および NTLMv2 認証の両方が許可されていることを確認する（Hyper-V over SMB 共有） .....	1
ドメインアカウントがデフォルトの UNIX ユーザにマッピングされていることを確認します .....	3
SVM のルートボリ्यूムのセキュリティ形式が NTFS に設定されていることを確認します .....	5
必要な CIFS サーバオプションが設定されていることを確認する .....	6
パフォーマンスと冗長性を高めるために SMB マルチチャネルを設定します .....	8
NTFS データボリ्यूムを作成 .....	10
継続的可用性を備えた SMB 共有を作成 .....	11
ユーザアカウント（SMB 共有の SQL Server 用）に SeSecurityPrivilege 権限を追加する .....	13
VSS シャドウコピーのディレクトリ階層を設定する（Hyper-V over SMB 共有の場合） .....	14

# Hyper-V over SMB および SQL Server over SMB でノンストップオペレーションを実現するための ONTAP 設定を作成します

## Hyper-V および SQL Server over SMB の概要を使用して、ノンストップオペレーション用の ONTAP 設定を作成します

SMB を介したノンストップオペレーションを実現する Hyper-V および SQL Server 環境を使用するためには、ONTAP の設定手順をいくつか実行する必要があります。

Hyper-V over SMB および SQL Server over SMB でノンストップオペレーションを実現する ONTAP 構成を作成する前に、次の作業を完了する必要があります。

- クラスタでタイムサービスがセットアップされている必要があります。
- SVM 用のネットワークをセットアップします。
- SVM を作成します。
- SVM でデータ LIF インターフェイスを設定します。
- SVM で DNS を設定します。
- SVM に必要なネームサービスをセットアップします。
- SMBサーバを作成しておく必要があります。

### 関連情報

[Hyper-V または SQL Server over SMB 構成を計画](#)

[設定に関する要件と考慮事項](#)

## Kerberos 認証および NTLMv2 認証の両方が許可されていることを確認する（Hyper-V over SMB 共有）

Hyper-V over SMB のノンストップオペレーションを実行する場合、データ SVM の CIFS サーバおよび Hyper-V サーバで Kerberos 認証と NTLMv2 認証の両方が許可されていなければなりません。CIFS サーバと Hyper-V サーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

### このタスクについて

Kerberos 認証は、継続的可用性を備えた共有への接続を確立する際に必要になります。また、リモート VSS のプロセスで NTLMv2 認証が使用されます。そのため、Hyper-V over SMB 構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos 認証と NTLMv2 認証の両方が許可されるように、次の設定を行う必要があります。

- Storage Virtual Machine（SVM）で SMB のエクスポートポリシーが無効になっている必要があります。

SVM では、Kerberos 認証と NTLMv2 認証がどちらも常に有効になりますが、エクスポートポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。

SMB のエクスポートポリシーは省略可能で、デフォルトでは無効になっています。エクスポートポリシーが無効になっている場合、CIFS サーバでは Kerberos 認証と NTLMv2 認証の両方がデフォルトで許可されます。

- CIFS サーバと Hyper-V サーバが属するドメインで、Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Kerberos 認証は、Active Directory ドメインではデフォルトで有効になります。ただし、NTLMv2 認証は、セキュリティポリシーの設定またはグループポリシーで禁止されている場合があります。

#### 手順

1. 次の手順に従って、SVM でエクスポートポリシーが無効になっていることを確認します。

- a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- b. を確認します `-is-exportpolicy-enabled` CIFSサーバオプションがに設定されている `false` :

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

- c. admin 権限レベルに戻ります。

```
set -privilege admin
```

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

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

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

ドメインで許可されている認証方法を確認する方法については、Microsoft TechNet ライブラリを参照してください。

4. ドメインで NTLMv2 認証が許可されていない場合は、Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

#### 例

次に、SVM vs1 で SMB のエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

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

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

vsserver  is-exportpolicy-enabled
-----
vs1       false

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

## ドメインアカウントがデフォルトの **UNIX** ユーザにマッピングされていることを確認します

Hyper-V および SQL Server では、継続的可用性を備えた共有への SMB 接続を作成する際にドメインアカウントを使用します。接続を作成するには、コンピュータアカウントが UNIX ユーザに正しくマッピングされている必要があります。そのための最も便利な方法は、コンピュータアカウントをデフォルトの UNIX ユーザにマッピングすることです。

このタスクについて

Hyper-V および SQL Server は、ドメインコンピュータアカウントを使用して SMB 接続を作成します。また、SQL Server は、SMB 接続を作成するサービスアカウントとしてドメインユーザアカウントを使用します。

Storage Virtual Machine (SVM) を作成すると、「pcuser」という名前のデフォルトユーザが ONTAP によって自動的に作成されます (UID はになります) 65534) および「pcuser」という名前のグループ (GID はです `65534` をクリックし、デフォルトユーザを "pcuser" グループに追加します。クラスタを Data ONTAP 8.2 にアップグレードする前に使用していた SVM で Hyper-V over SMB 解決策を設定する場合は、デフォルトのユーザとグループが存在していない可能性があります。デフォルトの UNIX ユーザを設定していない場合は、CIFS サーバのデフォルトの UNIX ユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

手順

1. デフォルトの UNIX ユーザが存在するかどうかを確認します。

```
vsserver cifs options show -vsserver vsserver_name
```

2. デフォルトユーザオプションが設定されていない場合は、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

```
vsserver services unix-user show -vsserver vsserver_name
```

3. デフォルトユーザオプションが設定されておらず、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

ーザも存在しない場合は、デフォルトの UNIX ユーザとデフォルトのグループを作成し、デフォルトのユーザをそのグループに追加します。

通常、デフォルトユーザにはユーザ名「pcuser」が与えられ、のUIDを割り当てる必要があります 65534。デフォルトのグループには '通常' グループ名として pcuser が与えられますグループに割り当てるGIDはである必要があります 65534。

- a. デフォルトグループを作成します。[+] **vserver services unix-group create -vserver vserver\_name -name pcuser -id 65534**
- b. デフォルトユーザを作成し、デフォルトグループに追加します。[+] **vserver services unix-user create -vserver vserver\_name -user pcuser -id 65534 -primary-gid 65534**
- c. デフォルトのユーザとデフォルトグループが正しく設定されていることを確認します。[] **`vserver services unix-user show -vserver \_vserver\_name\_` [] vserver services unix-group show -vserver vserver\_name -members**

4. CIFS サーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。

- a. デフォルトユーザを設定します。

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

- b. デフォルトの UNIX ユーザが正しく設定されていることを確認します。

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

5. アプリケーションサーバのコンピュータアカウントがデフォルトのユーザに正しくマッピングされていることを確認するには、SVMの共有にドライブをマッピングし、を使用してWindowsユーザとUNIXユーザのマッピングを確認します **vserver cifs session show** コマンドを実行します

このコマンドの使用の詳細については、マニュアルページを参照してください。

## 例

次のコマンドでは、CIFS サーバのデフォルトのユーザが設定されていないことがわかりますが、「pcuser」ユーザと「pcuser」グループは存在します。「pcuser」ユーザは、SVM vs1 上の CIFS サーバのデフォルトのユーザとして割り当てられています。

```
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::> vsserver services unix-user show
```

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

```
cluster1::> vsserver services unix-group show -members
```

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0
	Users: -	

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

```
cluster1::> vsserver cifs options show
```

```
Vserver: vs1
```

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

## SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合は、ボリュームを NTFS セキュリティ形式で作成する必要があります。ルートボリュームのセキュリティ形式には、Storage Virtual Machine（SVM）で作成されたボリュームのデフォルトが適用されるため、ルートボリュームのセキュリティ形式は NTFS に設定する必要があります。

このタスクについて

- ルートボリュームのセキュリティ形式は SVM の作成時に指定できます。
- SVMの作成時にルートボリュームのセキュリティ形式をNTFS以外に設定した場合は、を使用してあとからセキュリティ形式を変更できます `volume modify` コマンドを実行します

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

2. ルートボリュームのセキュリティ形式が NTFS 以外になっている場合は、セキュリティ形式を NTFS に変更します。

```
volume modify -vserver vs1 -volume vs1_root -security-style ntfs
```

3. SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します。

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

例

次に、SVM vs1 のルートボリュームのセキュリティ形式が NTFS になっていることを確認するコマンドの例を示します。

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

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

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

## 必要な CIFS サーバオプションが設定されていることを確認する

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合、必要な CIFS サーバオプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

このタスクについて



- SMB 2.x と SMB 3.0 が有効になっている必要があります。
- パフォーマンスが向上したコピーオフロードを使用するには、ODX コピーオフロードが有効になっている必要があります。
- Hyper-V over SMB 解決策でリモート VSS に対応したバックアップサービスを使用する場合は、VSS シャドウコピーサービスが有効になっている必要があります（Hyper-V のみ）。

#### 手順

1. Storage Virtual Machine （SVM）で必要な CIFS サーバオプションが有効になっていることを確認します。
  - a. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

- b. 次のコマンドを入力します。

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

次のオプションはに設定する必要があります true :

- -smb2-enabled
- -smb3-enabled
- -copy-offload-enabled
- -shadowcopy-enabled （Hyper-Vのみ）

2. いずれかのオプションがに設定されていない場合 `true` 次の手順を実行します。
  - a. に設定します true を使用します vserver cifs options modify コマンドを実行します
  - b. オプションがに設定されていることを確認します true を使用します vserver cifs options show コマンドを実行します
3. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次に、SVM vs1 について、Hyper-V over SMB 構成の必要なオプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、ODX コピーオフロードのオプションを有効にする必要があります。

```

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

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

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

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

cluster1:*> set -privilege admin

```

## パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

ONTAP 9.4 以降では、SMB マルチチャネルを設定して、1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立することができます。これにより、Hyper-V および SQL Server over SMB 構成のスループットとフォールトトレランスが向上します。

### 必要なもの

SMB マルチチャネル機能は、クライアントが SMB 3.0 以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMB サーバでは、SMB 3.0 以降がデフォルトで有効になっています。

### このタスクについて

SMB クライアントは、ONTAP クラスタで適切な設定が見つかったら、複数のネットワーク接続を自動的に検出して使用します。

SMB セッションでの同時接続数は、導入している NIC によって異なります。

- \* クライアントおよび ONTAP クラスタに 1G NIC を搭載 \*

クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされます。

- \* クライアントおよび ONTAP クラスタ上の 10G 以上の NIC \*

クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の NIC で接続を確立できます。

また、次のパラメータを変更することもできます（advanced 権限）。

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

各マルチチャネルセッションに許可される最大接続数。デフォルトの接続数は 32 です。

デフォルトよりも多くの接続を有効にする場合は、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

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

各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 です。

#### 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. SMB サーバで SMB マルチチャネルを有効にします。

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

3. ONTAP が SMB マルチチャネルセッションを報告していることを確認します。

```
vserver cifs session options show
```

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

#### 例

次の例は、すべての SMB セッションに関する情報を表示します。1 つのセッションに対して複数の接続が表示されています。

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

次の例は、セッション ID 1 が割り当てられた SMB セッションに関する詳細情報を表示します。

```
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: -
```

## NTFS データボリュームを作成

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継

継続的可用性を備えた共有を設定する前に、Storage Virtual Machine（SVM）上に NTFS データボリュームを作成する必要があります。ボリューム構成ワークシートを使用して、データボリュームを作成します。

このタスクについて

データボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、[xref:./smb-hyper-v-sql/「論理ストレージ管理」](#)を参照してください。

データボリュームの作成時に、次の項目を含むボリューム内にはジャンクションポイントを作成しないでください。

- ONTAP によってシャドウコピーが生成される Hyper-V ファイル
- SQL Server を使用してバックアップされる SQL Server データベースファイル



mixed セキュリティ形式または UNIX セキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームを NTFS セキュリティ形式のボリュームに変更して、ノンストップオペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMB および SQL Server over SMB のノンストップオペレーションが正しく機能しないのは、この構成で使用するボリュームを NTFS セキュリティ形式のボリュームとして作成した場合だけです。ボリュームを削除し、NTFS セキュリティ形式でボリュームを再作成する必要があります。または、Windows ホストでボリュームをマッピングし、ボリュームの最上位に ACL を適用して、ボリューム内のすべてのファイルとフォルダに ACL を適用することもできます。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する SVM のルートボリュームのセキュリティ形式	入力するコマンド
NTFS	<code>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
NTFS ではありません	<code>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. ボリュームの設定が正しいことを確認します。

```
volume show -vserver vservers_name -volume volume_name
```

## 継続的可用性を備えた SMB 共有を作成

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続

的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

#### 手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

```
volume show -vserver vs1 -junction
```

2. 継続的可用性を備えた SMB 共有を作成します。

```
vs1 cifs share create -vserver vs1 -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- 必要に応じて、コメントを共有設定に追加することもできます。
- デフォルトでは、オフラインファイル共有プロパティは共有に設定され、に設定されます manual。
- ONTAP によって、Windowsのデフォルトの共有権限で共有が作成されます Everyone / Full Control。

3. 共有設定ワークシートのすべての共有について同じ手順を繰り返します。
4. を使用して、設定が正しいことを確認します vs1 cifs share show コマンドを実行します
5. 継続的な可用性が確保された共有に NTFS ファイル権限を設定するには、各共有にドライブをマッピングし、Windows のプロパティ \* ウィンドウを使用してファイル権限を設定します。

#### 例

次のコマンドを実行すると、Storage Virtual Machine（SVM、旧 Vserver）vs1 上に「data2」という名前の継続的可用性を備えた共有が作成されます。シンボリックリンクを無効にするには、を設定します -symlink パラメータの値 ""：

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

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

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

```

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

```

## ユーザアカウント（SMB 共有の SQL Server 用）に SeSecurityPrivilege 権限を追加する

SQL Server のインストールに使用するドメインユーザアカウントには、デフォルトではドメインユーザに割り当てられていない権限を必要とする特定の操作を CIFS サーバで実行するために、「すべてのユーザ」権限を割り当てる必要があります。

必要なもの

SQL Server のインストールに使用するドメインアカウントがすでに存在している必要があります。

このタスクについて

SQL Server インストーラのアカウントに権限を追加するときに、ONTAP がドメインコントローラに照会してアカウントを検証することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

## 手順

1. “s eepleed” 権限を追加します。

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

の値 `-user-or-group-name` パラメータは、SQL Serverのインストールに使用するドメインユーザアカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

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

## 例

次のコマンドでは、Storage Virtual Machine（SVM）vs1 のEXAMPLE ドメインにあるSQL Server インストーラのアカウントに「s eepleed」権限を追加しています。

```
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
```

## VSS シャドウコピーのディレクトリ階層を設定する（Hyper-V over SMB 共有の場合）

必要に応じて、シャドウコピーを作成する SMB 共有のディレクトリの最大階層を設定できます。このパラメータは、ONTAP によってシャドウコピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

### 必要なもの

VSS シャドウコピー機能を有効にする必要があります。

### このタスクについて

デフォルトでは、最大 5 つのサブディレクトリにシャドウコピーが作成されます。値がに設定されている場合 `0`ONTAP では、すべてのサブディレクトリに対してシャドウコピーが作成されます。



シャドウコピーセットのディレクトリ階層は 6 個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウコピーセットの作成は 60 秒以内に完了しなければならないという Microsoft の要件があります。この時間内に完了できない場合、シャドウコピーセットの作成は失敗します。作成時間が制限時間を超えないようにシャドウコピーのディレクトリ階層原因を設定しないでください。



## 手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. VSS シャドウコピーのディレクトリ階層を目的のレベルに設定します。

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

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

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。