



# 共有ストレージへの**SMB**クライアントアクセス の設定 ONTAP 9

NetApp  
December 20, 2024

# 目次

共有ストレージへのSMBクライアントアクセスの設定 .....	1
共有ストレージへのSMBクライアントアクセスの設定 .....	1
ボリュームまたはqtreeのストレージコンテナを作成する .....	1
SMB共有の作成に関する要件と考慮事項 .....	4
SMB共有を作成する .....	5
SMBクライアントアクセスの確認 .....	6
SMB共有のアクセス制御リストの作成 .....	7
共有でのNTFSファイル権限の設定 .....	8
ユーザアクセスを確認 .....	10

# 共有ストレージへのSMBクライアントアクセスの設定

## 共有ストレージへのSMBクライアントアクセスの設定

SVM上の共有ストレージに対するSMBクライアントアクセスを許可するには、ストレージコンテナを提供するボリュームまたはqtreeを作成し、そのコンテナの共有を作成または変更する必要があります。その後、共有およびファイルの権限を設定し、クライアントシステムからのアクセスをテストできます。

開始する前に

- SVMでSMBの設定が完了している必要があります。
- ネームサービス設定に対する更新が完了している必要があります。
- Active Directoryドメインまたはワークグループ設定への追加または変更が完了している必要があります。

## ボリュームまたはqtreeのストレージコンテナを作成する

ボリュームの作成

コマンドを使用すると、ボリュームを作成し、ジャンクションポイントやその他のプロパティを指定できます `volume create`。

タスクの内容

クライアントがデータを使用できるようにするには、ボリュームに *junction path* を含める必要があります。ジャンクションパスは、新しいボリュームの作成時に指定できます。ジャンクションパスを指定せずにボリュームを作成する場合は、コマンドを使用して、SVMネームスペースでボリュームを `_mount_the` にする必要があります `volume mount`。

開始する前に

- SMBがセットアップされて実行されている必要があります。
- SVMのセキュリティ形式はNTFSである必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティの追跡を有効にするには、を指定してコマンドを `-analytics-state`実行する`volume create`か、`-activity-tracking-state`に設定します`on。`

容量分析とアクティビティ追跡の詳細については、を参照してください ["ファイルシステム分析を有効にする"](#)。

手順

1. ジャンクションポイントを設定してボリュームを作成します。 `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path]`

の選択肢は `-junction-path`次のとおりです。`

- ルートの直下。例： /new\_vol

新しいボリュームを作成し、SVMのルートボリュームに直接マウントされるように指定することができます。

- 既存のディレクトリの下（例： /existing\_dir/new\_vol

新しいボリュームを作成し、ディレクトリとして表現されている既存のボリューム（既存の階層内）にマウントされるように指定できます。

たとえば、新しいディレクトリ（新しいボリュームの下の新しい階層）にボリュームを作成する場合は /new\_dir/new\_vol、SVMのルートボリュームにジャンクションされている新しい親ボリュームを最初に作成する必要があります。その後、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 volume show -vserver svm\_name -volume volume\_name -junction

#### 例

次のコマンドは、SVM vs1.example.com およびアグリゲート aggr1 上に、users1 という名前の新しいボリュームを作成します。新しいボリュームは、で使用でき `users` ます。ボリュームのサイズは750GBで、ボリュームギャランティのタイプはvolume（デフォルト）です。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

次のコマンドでは、「home4」という名前の新しいボリュームをSVM「vs1.example.com」およびアグリゲート「aggr1」に作成します。ディレクトリは /eng/`vs1` SVMのネームスペース内にすでに存在し、新しいボリュームがで使用可能になります ` /eng/home。これがネームスペースのホームディレクトリになります。 /eng/`ボリュームのサイズは750GBで、ボリュームギャランティのタイプは（デフォルト）です `volume。

```

cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

## qtreeを作成する

コマンドを使用すると、データを含むqtreeを作成し、そのプロパティを指定できます  
`volume qtree create`。

開始する前に

- SVM と新しい qtree を格納するボリュームがすでに存在している必要があります。
- SVMのセキュリティ形式はNTFSであり、SMBがセットアップされて実行されている必要があります。

手順

1. qtreeを作成します。 `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

ボリュームとqtreeを別々の引数として指定するか、の形式でqtreeパスの引数を指定できます  
`/vol/volume_name/_qtree_name`。

2. 目的のジャンクションパスでqtreeが作成されたことを確認します。 `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

例

次の例は、ジャンクションパスがであるSVM vs1.example.com上に、qt01という名前のqtreeを作成し  
``/vol/data1``ます。

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com
          Volume Name: data1
          Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
          Security Style: ntfs
          Oplock Mode: enable
          Unix Permissions: ---rwxr-xr-x
          Qtree Id: 2
          Qtree Status: normal
          Export Policy: default
Is Export Policy Inherited: true
```

## SMB共有の作成に関する要件と考慮事項

SMB 共有を作成する前に、特にホームディレクトリに関して、共有パスと共有プロパティの要件を理解しておく必要があります。

SMB共有を作成するには、クライアントがアクセスするディレクトリパス構造を（コマンドのオプションを `vserver cifs share create` 使用して）指定する必要があります。`-path` は、ディレクトリパスは、SVM ネームスペース内に作成したボリュームまたは qtree のジャンクションパスに相当します。ディレクトリパスと対応するジャンクションパスは、共有を作成する前に存在している必要があります。

共有パスには次の要件があります。

- ディレクトリパス名の最大文字数は255文字です。
- パス名にスペースが含まれている場合は、文字列全体を引用符で囲む必要があります（例：`"/new volume/mount here"`）。
- (`\\servername\sharename\filepath` 共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭のは除く）、Windowsの[プロパティ]ボックスの\*[セキュリティ]\*タブは使用できません。

これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

共有プロパティのデフォルト値は変更できます。

- すべての共有のデフォルトの初期プロパティは oplocks、 browsable、 `changenotify` および `show-previous-versions` です。
- 共有の作成時、共有プロパティの指定はオプションです。

ただし、共有の作成時に共有プロパティを指定した場合、デフォルト値は使用されません。共有の作成時にパラメータを使用する場合 `share-properties` は、共有に適用するすべての共有プロパティをカンマで区切って指定する必要があります。

- ホームディレクトリ共有を指定するには、プロパティを使用し `homedirectory` ます。

この機能を使用すると、接続するユーザと一連の変数に基づいてさまざまなディレクトリにマッピングされる共有を設定できます。ユーザごとに別個の共有を作成する必要はありません。1つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とユーザのホームディレクトリ（SVM上のディレクトリ）間のユーザの関係を定義します。



共有の作成後にこのプロパティを追加または削除することはできません。

ホームディレクトリの共有には次の要件があります。

- SMBホームディレクトリを作成する前に、コマンドを使用して、ホームディレクトリ検索パスを少なくとも1つ追加する必要があります `vserver cifs home-directory search-path add`。
- パラメータの `-share-properties` 値に指定するホームディレクトリ共有で `homedirectory` は、（Windowsユーザ名）動的変数を共有名に含める必要があります `%w`。

共有名には、さらに（ドメイン名）動的変数（など %d/%w）を含めることも、静的な部分（など `home1_%w`）を含めることもできます %d。

- 管理者またはユーザが他のユーザのホームディレクトリに接続するために共有を使用する場合（コマンドのオプションを使用）は `vserver cifs home-directory modify`、動的共有名のパターンの先頭にチルダを付ける必要があります (~) ます。

"[SMBの管理](#)" および `vserver cifs share` のマニュアルページに追加情報が記載されています。

## SMB共有を作成する

SMB サーバのデータを SMB クライアントと共有するには、SMB 共有を作成する必要があります。共有を作成するときは、共有をホームディレクトリとして指定するなど、共有プロパティを設定できます。オプションの設定により、共有をカスタマイズすることもできます。

### 開始する前に

共有を作成する前に、ボリュームまたは `qtree` のディレクトリパスが SVM ネームスペース内に存在している必要があります。

### タスクの内容

共有を作成するときのデフォルトの共有ACL（デフォルトの共有権限）は `Everyone / Full Control`。共有へのアクセスをテストしたら、デフォルトの共有ACLを削除し、より安全な方法で置き換える必要があります。

### 手順

1. 必要に応じて、共有のディレクトリパス構造を作成します。

コマンドは `vserver cifs share create`、共有の作成時にオプションで指定されたパスをチェックし、`-path` します。指定したパスが存在しない場合、コマンドは失敗します。

2. 指定したSVMに関連付けられているSMB共有を作成します。 `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. 共有が作成されたことを確認します。 `vserver cifs share show -share-name share_name`

#### 例

次のコマンドは、「SHARE1」という名前のSMB共有をSVM上に作成し `vs1.example.com` します。ディレクトリパスは `/users`、デフォルトのプロパティを使用して作成されます。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

## SMBクライアントアクセスの確認

共有にアクセスしてデータを書き込むことで、SMBが正しく設定されていることを確認する必要があります。SMBサーバ名とNetBIOSエイリアスを使用してアクセスをテストします。

#### 手順

1. Windowsクライアントにログインします。
2. SMBサーバ名を使用してアクセスをテストします。
  - a. エクスプローラで、次の形式で共有にドライブをマッピングします。 `\\SMB_Server_Name\Share_Name`

正常にマッピングされない場合は、DNSマッピングがネットワーク全体にまだ反映されていない可能性があります。しばらく待ってから、再度SMBサーバ名を使用してアクセスをテストしてください。

SMBサーバの名前が `vs1.example.com` で、共有の名前が `SHARE1` の場合は、次のように入力します。  
`\\vs0.example.com\SHARE1`

- b. 新しく作成したドライブで、テストファイルを作成して削除します。



SMB サーバ名を使用した共有への書き込みアクセスが可能であることを確認できました。

3. NetBIOS エイリアスについて手順 2 を繰り返します。

## SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List (ACL ; アクセス制御リスト) を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

開始する前に

共有へのアクセスを許可するユーザまたはグループを決めておく必要があります。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control` ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。 `vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. 新しいACLを設定します。

設定する ACL に使用するアカウント	入力するコマンド
Windowsユーザ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Windowsグループ	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com`"SVM:」上の「sales」共有の「sales Team」Windowsグループに権限を与えます Change。

```

cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show

```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

次のコマンドは、SVM「vs1」上の「datavol5」共有に対する「Tiger Team」という名前のローカルWindowsグループへの権限と「See Chang」という名前のローカルWindowsユーザへの権限 Full\_Control`を付与します `Change。

```

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsserver cifs share access-control show -vsserver vs1

```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

## 共有でのNTFSファイル権限の設定

共有にアクセスできるユーザまたはグループにファイルアクセスを有効にするには、その共有内のファイルおよびディレクトリに対するNTFSファイル権限をWindowsクライアントから設定する必要があります。

## 開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

## タスクの内容

"SMBの管理"標準および詳細なNTFS権限の設定方法については、Windowsのマニュアルを参照してください。

## 手順

1. Windows クライアントに管理者としてログインします。
2. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
3. [ ネットワークドライブの割り当て \* ] ボックスに入力します。
  - a. ドライブ文字を選択します。
  - b. [ \* フォルダ \* ] ボックスに、権限を適用するデータと共有名を含む共有を含む SMB サーバー名を入力します。

SMBサーバ名がSMB\_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。

\\SMB\_SERVER01\SHARE1



SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

- c. [ 完了 ] をクリックします。

選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
5. ファイルまたはディレクトリを右クリックし、\* プロパティ \* を選択します。
6. [ \* セキュリティ \* ] タブを選択します。

Security タブには、NTFS 権限が設定されているユーザとグループのリストが表示されます。[ < オブジェクト > のアクセス許可 ] ボックスには、選択したユーザーまたはグループの有効なアクセス許可と拒否のアクセス許可のリストが表示されます。

7. [ 編集 ( Edit ) ] をクリックします。

[ < オブジェクト > のアクセス許可 ] ボックスが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループに対する標準の NTFS 権限を設定します	<p>a. [追加]*をクリックします。</p> <p>[ユーザー、コンピュータ、サービスアカウント、またはグループの選択] ウィンドウが開きます。</p> <p>b. [選択するオブジェクト名を入力してください*] ボックスに、NTFS アクセス権を追加するユーザまたはグループの名前を入力します。</p> <p>c. [OK]*をクリックします。</p>
ユーザまたはグループに対する標準の NTFS 権限を変更または削除する	[*グループ名またはユーザー名*] ボックスで、変更または削除するユーザーまたはグループを選択します。

9. 次のうち必要な操作を実行します。

状況	実行する処理
新規または既存のユーザまたはグループに対する標準の NTFS 権限を設定する	[*パーミッション for <オブジェクト>*] ボックスで、選択したユーザーまたはグループに対して許可または許可しないアクセスのタイプの [許可*] または [拒否*] ボックスを選択します。
ユーザまたはグループを削除します	[削除 (Remove)] をクリックします。



標準の権限ボックスの一部またはすべてを選択できない場合、権限は親オブジェクトから継承されます。[\*特別な権限\*] ボックスは選択できません。選択されている場合は、選択したユーザまたはグループに対して詳細な権限が1つ以上設定されていることを意味します。

10. そのオブジェクトの NTFS アクセス権の追加、削除、または編集が完了したら、**OK** をクリックします。

## ユーザアクセスを確認

設定したユーザが、SMB 共有およびその中に含まれるファイルにアクセスできることをテストする必要があります。

手順

1. Windows クライアントで、共有へのアクセスを許可したいいずれかのユーザとしてログインします。
2. Windows Explorer の \* ツール \* メニューから、\* ネットワークドライブのマップ \* を選択します。
3. [ネットワークドライブの割り当て\*] ボックスに入力します。
  - a. ドライブ文字を選択します。

b. [\* フォルダー \*] ボックスに、ユーザーに提供する共有名を入力します。

SMBサーバ名がSMB\_SERVER01で、共有の名前が「SHARE1」の場合は、と入力します。

\\SMB\_SERVER01\share1

c. [完了] をクリックします。

選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

4. テストファイルを作成し、その存在を確認し、テキストを書き込んで、テストファイルを削除します。

## 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。