共有ストレージへの SMB クライアントアクセスを設定します

ONTAP 9

NetApp
April 24, 2024

目次

共有ストレージへの SMB クライアントアクセスを設定します

共有ストレージへの SMB クライアントアクセスを設定します

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。

作業を開始する前に

- 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します

ボリュームを作成します

を使用して、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` コマンドを実行します

このタスクについて

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、新しいボリュームを作成するときに指定できます。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、を使用してSVMネームスペースにボリュームを_mount_する必要があります `volume mount` コマンドを実行します

作業を開始する前に

- 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トラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `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 File System Analytics を有効にします。

手順

1. ジャンクションポイントを指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 `-junction-path` 次のようなものがあります。

- 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。

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、次のように指定します。 `/new_dir/new_vol`その後、SVMルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。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、で使用できます `/users`。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
                           Junction                 Junction
Vserver           Volume  Active   Junction Path   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 `/eng/` はvs1 SVMのネームスペースにすでに存在し、新しいボリュームはで使用できるようになります `/eng/home`をクリックします。これがのホームディレクトリになります `/eng/` ネームスペース：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です `volume` （デフォルト）。

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

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

qtree を作成します

を使用して、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` コマンドを実行します

作業を開始する前に

- 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 である必要があります。また、 SMB が設定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. qtree が必要なジャンクションパスで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を作成します `/vol/data1`：

```
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、を使用してディレクトリパス構造を指定します `-path` のオプションを選択します `vserver cifs share create` クライアントがアクセスするコマンド）。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は 255 文字以内で指定します。
- 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"`）。
- UNCパスの場合 (`\\servername\sharename\filepath`（UNCパスの先頭のを除く）が256文字を超えている場合、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 問題ではなく Windows クライアント問題です。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です `oplocks`、 `browsable`、 `changenotify`および `show-previous-versions`。
- 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。を使用する場合 `-share-properties` パラメータ共有を作成するときは、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、を使用します `homedirectory` プロパティ。

  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、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` コマンドを実行します
- の値で指定したホームディレクトリ共有 `homedirectory` をクリックします `-share-properties` パラメータにはを含める必要があります `%w` （Windowsユーザ名）共有名の動的変数。

  共有名にはさらにを含めることができます `%d` （ドメイン名）動的変数（例： `%d/%w`）または共有名の静的な部分（例： `home1_%w`）。

- 共有が他のユーザのホームディレクトリに接続するために管理者またはユーザによって使用されている場合（のオプションを使用） `vserver cifs home-directory modify` 動的な共有名のパターンの前にチルダを付ける必要があります (~）。

"SMBの管理" および `vserver cifs share` マニュアルページには追加情報 があります。

SMB 共有を作成

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。

作業を開始する前に

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。

このタスクについて

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）はです `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。

。 `vserver cifs share create` コマンドはで指定されたパスをチェックします `-path` オプション（共有の作成時）。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上に作成します `vs1.example.com`。ディレクトリパスはです `/users`をクリックすると、デフォルトのプロパティで作成されます。

```
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を確認

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、作成できたら削除します。

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を作成

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。

作業を開始する前に

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。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名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ます `Everyone / Full Control`は、セキュリティリスクをもたらします。

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	`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`
Windows グループ	`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`

3. 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` コマンドを実行します

例

次のコマンドは、を示しています `Change` 「vs1.example.com`"SVM:」上の「sales」共有に対する「Sales Team」Windowsグループへの権限

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

cluster1::> vserver cifs share access-control show
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

以下のコマンドで説明します `Change` 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 `Full_Control` SVM「vs1」の「datavol5」共有に対する「Sue Chang」という名前のWindowsローカルユーザの権限：

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

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

共有内で **NTFS** ファイル権限を設定する

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許可するには、Windows クライアントで、その共有内のファイルおよびディレクトリに対して NTFS ファイルアクセス権を設定する必要があります。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

"SMBの管理" また、標準および詳細な NTFS アクセス権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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

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	実行する処理
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	a. [追加（ Add ）] をクリックします。 [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。 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。 c. [OK] をクリックします。
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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

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。