CLIを使用したSMBの設定

ONTAP 9

NetApp
February 12, 2026

目次

CLIを使用したSMBの設定

ONTAP CLI を使用した SMB 構成について学習します

ONTAP 9のCLIコマンドを使用して、新規または既存のSVMの新しいボリュームまたはqtreeに格納されているファイルへのSMBクライアント アクセスを設定することができます。

SMB（Server Message Block）は、Common Internet File System（CIFS）プロトコルの最新の方言を指します。ONTAPコマンドライン インターフェイス（CLI）およびOnCommand管理ツールには、引き続き_CIFS_が表示されます。

ここで説明する手順は、ボリュームまたはqtreeへのSMBアクセスを設定する場合に使用します。想定している状況は次のとおりです。

- SMBのバージョン2以降を使用する必要がある。
- NFSクライアントではなく、SMBクライアントのみを対象とする（マルチプロトコル構成ではない）。
- 新しいボリュームをNTFSファイル権限を使用して保護する。
- SVM管理者権限ではなくクラスタ管理者権限を保有している。

  SVMとLIFを作成するにはクラスタ管理者権限が必要です。その他のSMB構成タスクには、SVM管理者権限で十分です。

- System Managerや自動スクリプト ツールではなく、CLIを使用する必要がある。

  System Manager を使用して NAS マルチプロトコルアクセスを構成するには、"NFSとSMBの両方を使用したWindowsおよびLinux用のNASストレージのプロビジョニング"を参照してください。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

  この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

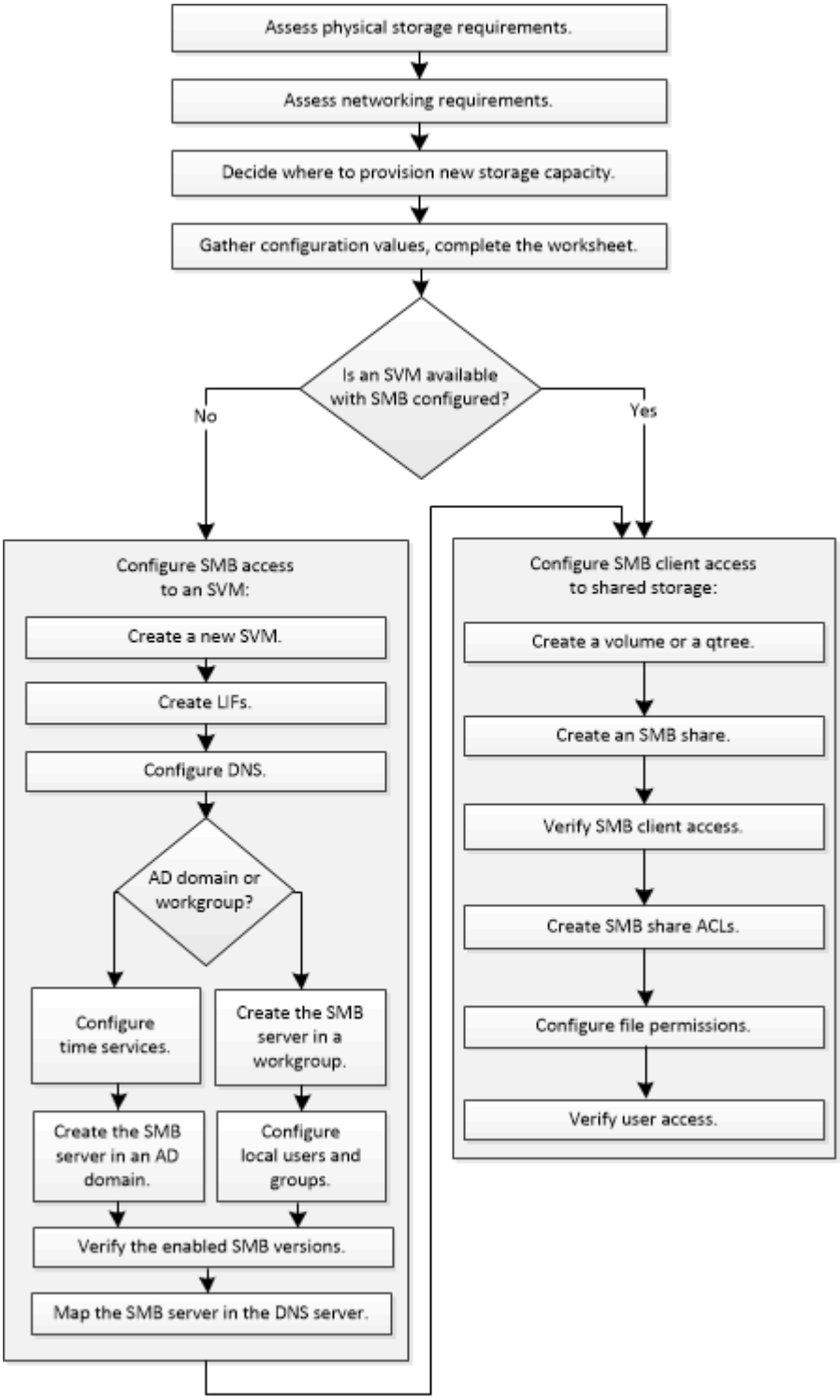
ONTAP SMB プロトコル機能の範囲の詳細については、"SMBリファレンス - 概要"を参照してください。

ONTAPでこの処理を行うその他の方法

タスクを実行するツール	参照先
新しいSystem Manager（ONTAP 9.7以降で使用可能）	"SMBを使用したWindowsサーバ用のNASストレージのプロビジョニング"
System Manager Classic（ONTAP 9.7以前で使用可能）	"SMB 構成の概要"

ONTAP SMB 構成ワークフロー

SMBを設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存のSVMへのSMBアクセスを設定するか、すでにSMBアクセスの設定が完了している既存のSVMにボリュームまたはqtreeを追加するかによってワークフローが異なります。



準備

ONTAP SMBの物理ストレージ要件を評価する

クライアントのSMBストレージをプロビジョニングする前に、既存のアグリゲート内に新しいボリュームのための十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを作成することができます。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します： `storage aggregate show`

   十分なスペースを備えたアグリゲートがある場合は、その名前をワークシートに記録します。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 十分なスペースを持つアグリゲートがない場合は、 `storage aggregate add-disks` コマンドを使用して既存のアグリゲートにディスクを追加するか、 `storage aggregate create` コマンドを使用して新しいアグリゲートを作成します。

関連情報

- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP SMBネットワーク要件を評価する

クライアントにSMBストレージを提供する前に、ネットワークが正しく設定されてSMBのプロビジョニング要件を満たしていることを確認する必要があります。

開始する前に

次のクラスタ ネットワーク オブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャスト ドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

手順

1. 使用可能な物理ポートと仮想ポートを表示します： `network port show`
   - 可能な場合は、データ ネットワークの速度が最高であるポートを使用する必要があります。
   - 最大限のパフォーマンスを得るためには、データ ネットワーク内のすべてのコンポーネントのMTU設定が同じである必要があります。

   > `network port show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-show.html["ONTAPコマンド リファレンス"^]を参照してください。

2. サブネット名を使用して LIF の IP アドレスとネットワーク マスク値を割り当てる予定の場合は、サブネットが存在し、十分なアドレスが使用可能であることを確認します： `network subnet show`

   > `network subnet show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-show.html["ONTAPコマンド リファレンス"^]を参照してください。

   サブネットには、同じレイヤー3サブネットに属するIPアドレスのプールが含まれます。サブネットは`network subnet create`コマンドを使用して作成されます。

   > `network subnet create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-create.html["ONTAPコマンド リファレンス"^]を参照してください。

3. 使用可能な IPspace を表示： `network ipspace show`

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

`network ipspace show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-ipspace-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

4. IPv6 アドレスを使用する場合は、クラスタで IPv6 が有効になっていることを確認します： `network options ipv6 show`

   必要に応じて、 `network options ipv6 modify` コマンドを使用して IPv6 を有効にすることができます。

`network options ipv6 show`および `network options ipv6 modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+options+ipv6["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP SMBストレージ容量のプロビジョニングについて

新しいSMBボリュームまたはqtreeを作成する前に、そのボリュームを新規、既存のどちらのSVMに配置するかを決め、配置先のSVMでどのような設定が必要になるかを確認しておく必要があります。それによって以降のワークフローが決まります。

オプション

- 新しい SVM、または SMB が有効になっているが設定されていない既存の SVM にボリュームまたは qtree をプロビジョニングする場合は、「`SVM` への `SMB` アクセスの設定」と「`SMB` 対応 `SVM` へのストレージ容量の追加」の両方の手順を完了します。

  SVMへのSMB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

  次のいずれかに該当する場合は、新しいSVMを作成します。

  - クラスタで SMB を初めて有効にします。
  - SMB サポートを有効にしたくないクラスタ内に既存の SVM があります。
  - クラスタ内に 1 つ以上の SMB 対応 SVM があり、次のいずれかの接続が必要です：
    - 別の Active Directory フォレストまたはワークグループへ。
    - 分離された名前空間内のSMBサーバ（マルチテナンシーシナリオ）。SMBが有効になっているが未設定の既存のSVMにストレージをプロビジョニングする場合も、このオプションを選択する必要があります。これは、SVMをSANアクセス用に作成した場合や、SVMの作成時にプロトコルが有効になっていなかった場合に発生する可能性があります。

  SVMでSMBを有効にしたあとに、ボリュームまたはqtreeのプロビジョニングに進みます。

- SMB アクセス用に完全に設定されている既存の SVM にボリュームまたは qtree をプロビジョニングする場合は、「`SMB` 対応 `SVM` へのストレージ容量の追加」の手順を完了します。

共有ストレージへの SMB クライアント アクセスの設定

ONTAP SMB 構成ワークシート

SMB設定ワークシートを使用すると、クライアントのSMBアクセスを設定するために必要な情報を収集できます。

ストレージをプロビジョニングする場所についての決定に応じて、ワークシートの 1 つまたは両方のセクションを完了する必要があります：

- SVMへのSMBアクセスを設定する場合は、両方のセクションを完了する必要があります。

  SVMへのSMB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

- SMB対応SVMにストレージ容量を追加する場合は、2番目のセクションのみを完了する必要があります。

  共有ストレージへの SMB クライアント アクセスの設定

"ONTAPコマンド リファレンス"のパラメータの詳細については、こちらをご覧ください。

SVMへのSMBアクセスの設定

SVMを作成するためのパラメータ

新しいSVMを作成する場合は、 `vserver create`コマンドでこれらの値を指定します。"ONTAPコマンド リファレンス"の `vserver create`の詳細をご覧ください。

フィールド	概要	あなたの価値
`-vserver`	新しいSVMの名前を指定します。完全修飾ドメイン名（FQDN）を指定するか、クラスタ内で一意のSVM名を適用する別の命名規則に従います。	
`-aggregate`	新しいSMBストレージ容量に対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-rootvolume`	SVMルート ボリュームの一意の名前を指定します。	
`-rootvolume-security-style`	SVMのNTFSセキュリティ形式を使用します。	`ntfs`

フィールド	概要	あなたの価値
`-language`	このワークフローではデフォルトの言語設定を使用します。	`C.UTF-8`
`ipspace`	オプション：IPspace は、SVM が存在する個別の IP アドレス空間です。	

LIFを作成するためのパラメータ

これらの値は、LIFを作成する際に `network interface create`コマンドで指定します。"ONTAPコマンド リファレンス"の `network interface create`の詳細を確認してください。

フィールド	概要	あなたの価値
`-lif`	新しいLIFの名前を指定します。	
`-role`	このワークフローではデータLIFのロールを使用します。	`data`
`-data-protocol`	このワークフローではSMBプロトコルのみを使用します。	`cifs`
`-home-node`	`network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノード。 `network interface revert`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-revert.html["ONTAPコマンド リファレンス"^]を参照してください。	

フィールド	概要	あなたの価値
-home-port	`network interface revert`コマンドがLIFで実行されたときにLIFが戻るポートまたはインターフェイスグループ。	
-address	新しいLIFによるデータ アクセスに使用されるクラスタ上のIPv4またはIPv6アドレスを指定します。	
-netmask	LIFのネットワーク マスクとゲートウェイを指定します。	
-subnet	IPアドレスのプール。 `-address`と`-netmask`の代わりに使用され、アドレスとネットマスクを自動的に割り当てます。	
-firewall-policy	このワークフローではデフォルトのデータ ファイアウォール ポリシーを使用します。	data
-auto-revert	オプション：起動時またはその他の状況で、データLIFが自動的にホームノードに戻るかどうかを指定します。デフォルト設定は `false`です。	

DNSホスト名解決のパラメータ

これらの値は、DNSを設定する際に `vserver services name-service dns create`コマンドで指定します。"ONTAPコマンド リファレンス"の `vserver services name-service dns create`の詳細をご覧ください。

フィールド	概要	あなたの価値
-domains	最大5つのDNSドメイン名を指定します。	
-name-servers	DNSネーム サーバごとに最大3つのIPアドレスを指定します。	

Active Directoryドメインでの**SMB**サーバのセットアップ

タイム サービス設定のパラメータ

これらの値は、タイムサービスを設定する際に `cluster time-service ntp server create`コマンドで指定します。"ONTAPコマンド リファレンス"の `cluster time-service ntp server create`の詳細をご覧ください。

フィールド	概要	あなたの価値
`-server`	Active Directory ドメインの NTP サーバのホスト名または IP アドレス。	

Active Directoryドメインに **SMB** サーバを作成するためのパラメータ

新しいSMBサーバーを作成し、ドメイン情報を指定する際に、 `vserver cifs create`コマンドでこれらの値を指定します。"ONTAPコマンド リファレンス"の `vserver cifs create`の詳細を確認してください。

フィールド	概要	あなたの価値
`-vserver`	SMB サーバーを作成する SVM の名前。	
`-cifs-server`	SMB サーバーの名前（最大 15 文字）。	
`-domain`	SMB サーバーに関連付ける Active Directory ドメインの完全修飾ドメイン名（FQDN）。	
`-ou`	オプション：SMB サーバに関連付ける Active Directory ドメイン内の組織単位。デフォルトでは、このパラメータは CN=Computers に設定されています。	
`-netbios-aliases`	オプション：SMB サーバー名の別名である NetBIOS エイリアスのリスト。	
`-comment`	オプション：サーバーに関するテキストコメント。Windowsクライアントは、ネットワーク上のサーバーを参照する際に、このSMBサーバーの説明を参照できます。	

ワークグループでの**SMB**サーバのセットアップ

ワークグループに**SMB**サーバを作成するためのパラメータ

新しいSMBサーバを作成し、サポートされるSMBバージョンを指定する際に、 `vserver cifs create`コマンドでこれらの値を指定します。"ONTAPコマンド リファレンス"の `vserver cifs create`の詳細を確認してください。

フィールド	概要	あなたの価値
`-vserver`	SMB サーバーを作成する SVM の名前。	
`-cifs-server`	SMB サーバーの名前（最大 15 文字）。	
`-workgroup`	ワークグループの名前（最大 15 文字）。	
`-comment`	オプション：サーバーに関するテキストコメント。Windowsクライアントは、ネットワーク上のサーバーを参照する際に、このSMBサーバーの説明を参照できます。	

ローカルユーザを作成するためのパラメータ

これらの値は、 `vserver cifs users-and-groups local-user create`コマンドを使用してローカル ユーザを作成する際に指定します。ワークグループ内のSMBサーバでは必須ですが、ADドメインではオプションです。 `vserver cifs users-and-groups local-user create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

フィールド	概要	あなたの価値
`-vserver`	ローカル ユーザーを作成する SVM の名前。	
`-user-name`	ローカル ユーザーの名前（最大 20 文字）。	
`-full-name`	オプション：ユーザーのフルネーム。フルネームにスペースが含まれる場合は、フルネームを二重引用符で囲みます。	
`-description`	オプション：ローカル ユーザの概要。概要にスペースが含まれている場合は、パラメータを引用符で囲みます。	
`-is-account-disabled`	オプション：ユーザ アカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザ アカウントはデフォルトで有効になります。	

ローカルグループを作成するためのパラメータ

これらの値は、 `vserver cifs users-and-groups local-group create`コマンドを使用してローカルグループを作成する際に指定します。ADドメインおよびワークグループ内のSMBサーバーではオプションです。"ONTAP コマンド リファレンス"の `vserver cifs users-and-groups local-group create`の詳細をご覧ください。

フィールド	概要	あなたの価値
`-vserver`	ローカル グループを作成する SVM の名前。	
`-group-name`	ローカル グループの名前（最大 256 文字）。	
`-description`	オプション：ローカル グループの説明。説明にスペースが含まれる場合は、パラメータを引用符で囲んでください。	

SMB対応SVMへのストレージ容量の追加

ボリュームを作成するためのパラメータ

qtree ではなくボリュームを作成する場合は、 `volume create`コマンドでこれらの値を指定します。"ONTAP コマンド リファレンス"の `volume create`の詳細を参照してください。

フィールド	概要	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	
`-volume`	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
`-aggregate`	新しいSMBボリュームに対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
`-size`	新しいボリュームのサイズとして任意の整数を指定します。	
`-security-style`	このワークフローにはNTFSセキュリティ形式を使用します。	`ntfs`
`-junction-path`	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	

qtreeを作成するためのパラメータ

ボリュームではなくqtreeを作成する場合は、 `volume qtree create`コマンドでこれらの値を指定します。"ONTAPコマンド リファレンス"の `volume qtree create`の詳細を確認してください。

フィールド	概要	あなたの価値
`-vserver`	qtreeを格納するボリュームが配置されているSVMの名前を指定します。	
`-volume`	新しいqtreeを格納するボリュームの名前を指定します。	
`-qtree`	新しいqtreeに対して、一意のわかりやすい名前を64文字以内で指定します。	
`-qtree-path`	ボリュームとqtreeを別々の引数として指定する代わりに、 `/vol/volume_name/qtree_name\>` 形式でqtreeパス引数を指定できます。	

SMB 共有を作成するためのパラメータ

これらの値は `vserver cifs share create`コマンドで指定します。 `vserver cifs share create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

フィールド	概要	あなたの価値
`-vserver`	SMB 共有を作成する SVM の名前。	
`-share-name`	作成する SMB 共有の名前（最大 256 文字）。	
`-path`	SMB共有へのパス名（最大256文字）。このパスは、共有を作成する前にボリューム内に存在している必要があります。	
`-share-properties`	オプション：共有プロパティのリスト。デフォルト設定は `oplocks`、 `browsable`、 `changenotify`、および `show-previous-versions`です。	

フィールド	概要	あなたの価値
`-comment`	オプション：サーバーへのテキストコメント（最大256文字）。Windowsクライアントは、ネットワークを閲覧する際にこのSMB共有の説明を参照できます。	

SMB 共有アクセス制御リスト（**ACL**）を作成するためのパラメータ

これらの値は `vserver cifs share access-control create`コマンドで指定します。 `vserver cifs share access-control create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

フィールド	概要	あなたの価値
`-vserver`	SMB ACL を作成する SVM の名前。	
`-share`	作成する SMB 共有の名前。	
`-user-group-type`	共有の ACL に追加するユーザまたはグループのタイプ。デフォルトのタイプは `windows`です。	`windows`
`-user-or-group`	共有のACLに追加するユーザーまたはグループ。ユーザー名を指定する場合は、「`domain\username`」という形式でユーザーのドメインを含める必要があります。	
`-permission`	ユーザまたはグループの権限を指定します。	`[No_access
Read	Change	Full_Control]`

SVMへのSMBアクセスの設定

ONTAP SVMへのSMBアクセスを構成する

SMBクライアント アクセス用にSVMがまだ設定されていない場合は、新しいSVMを作成して設定するか、既存のSVMを設定する必要があります。SMBの設定には、SVMルート ボリューム アクセスの有効化、SMBサーバの作成、LIFの作成、ホスト名解決の有効化、ネーム サービスの設定、そして必要に応じてKerberosセキュリティの有効化が含まれます。

SMBデータアクセスを提供するためのONTAP SVMを作成する

クラスタ内にSMBクライアントにデータ アクセスを提供するSVMが1つもない場合は、作成する必要があります。

開始する前に

- ONTAP 9.13.1以降では、ストレージVMの最大容量を設定できます。また、SVMの容量がしきい値に近づいた場合にアラートを設定することもできます。詳細については、SVMの容量の管理を参照してください。

手順

1. SVM を作成します。 `vserver create -vserver *svm_name* -rootvolume *root_volume_name* -aggregate *aggregate_name* -rootvolume-security-style ntfs -language C.UTF-8 -ipspace *ipspace_name*`
   - `-rootvolume-security-style`オプションには NTFS 設定を使用します。
   - デフォルトの C.UTF-8 `-language` オプションを使用します。
   - `ipspace`設定はオプションです。
2. 新しく作成された SVM の構成とステータスを確認します： `vserver show -vserver *vserver_name*`

   `Allowed Protocols`フィールドには `CIFS` を含める必要があります。このリストは後で編集できます。

   `Vserver Operational State`フィールドには `running`状態が表示される必要があります。 `initializing`状態が表示される場合、ルート ボリュームの作成などの中間操作が失敗したことを意味し、SVMを削除して再作成する必要があります。

例

次のコマンドは、IPspace `ipspaceA`内のデータ アクセス用の SVM を作成します：

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

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

次のコマンドは、1GBのルートボリュームを持つSVMが作成され、自動的に起動されて `running`状態になっていることを示しています。ルートボリュームにはルールが含まれていないデフォルトのエクスポート ポリシーが適用されているため、作成時にルートボリュームはエクスポートされません。

```
cluster1::> vserver show -vserver 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
```

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限を適用できます。このポリシーは、SVMを作成した後にのみ適用できます。このプロセスの詳細については、アダプティブ ポリシー グループ テンプレートの設定を参照してください。

ONTAP SVM で SMB プロトコルが有効になっていることを確認します

SVMでSMBを設定して使用する前に、このプロトコルが有効になっていることを確認する必要があります。

タスク概要

これは通常、SVM のセットアップ中に実行されますが、セットアップ中にプロトコルを有効にしなかった場合は、後で `vserver add-protocols`コマンドを使用して有効にできます。

LIF を作成した後は、プロトコルを追加したり削除したりすることはできません。

`vserver remove-protocols`コマンドを使用して
SVM上のプロトコルを無効にすることもできます。

手順

1. SVM に対して現在有効になっているプロトコルと無効になっているプロトコルを確認します： `vserver show -vserver vserver_name -protocols`

   `vserver show-protocols`コマンドを使用して、クラスタ内のすべての
   SVMで現在有効になっているプロトコルを表示することもできます。

2. 必要に応じて、プロトコルを有効または無効にします：
   - SMB プロトコルを有効にするには： `vserver add-protocols -vserver vserver_name -protocols cifs`
   - プロトコルを無効にするには： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 有効化されたプロトコルと無効化されたプロトコルが正しく更新されたことを確認します： `vserver show -vserver vserver_name -protocols`

例

次のコマンドは、vs1 という名前の SVM で現在有効になっているプロトコルと無効になっているプロトコル（許可されているプロトコルと許可されていないプロトコル）を表示します：

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

次のコマンドは、vs1という名前のSVM上の有効なプロトコルのリストに`cifs`を追加することで、SMB経由のアクセスを許可します：

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

ONTAP SVMルートボリュームのSMBエクスポート ポリシーを開きます

SVMルート ボリュームのデフォルトのエクスポート ポリシーには、すべてのクライアントにSMB経由のアクセスを許可するルールが含まれている必要があります。このようなルールを追加しないと、SVMとそのボリュームに対するSMBクライアントのアクセスがすべて拒否されます。

タスク概要

新しいSVMが作成されると、SVMのルート ボリュームに対してデフォルトのエクスポート ポリシー（default

）が自動的に作成されます。クライアントがSVM上のデータにアクセスできるようにするには、デフォルトのエクスポート ポリシーにルールを1つ以上作成する必要があります。

デフォルトのエクスポート ポリシーですべてのSMBアクセスが許可されていることを確認してから、ボリュームまたはqtreeごとにカスタムのエクスポート ポリシーを作成して各ボリュームへのアクセスを制限します。

手順

1. 既存の SVM を使用している場合は、デフォルトのルート ボリュームのエクスポート ルールを確認します：`vserver export-policy rule show`

   コマンド出力は次のようになります：

```
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
```

   オープン アクセスを許可するルールが存在する場合、このタスクは完了です。存在しない場合は、次のステップに進みます。

2. SVM ルート ボリュームのエクスポート ルールを作成します。`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. `vserver export-policy rule show`コマンドを使用してルールの作成を確認します。

結果

これで、SVMで作成されたすべてのボリュームまたはqtreeに、SMBクライアントからアクセスできるようになりました。

ONTAP SMB LIFを作成する

LIFは、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるので、引き続きネットワークと通信できます。

開始する前に

- 基盤となる物理または論理ネットワーク ポートが管理 `up`ステータスに設定されている必要があります。"ONTAPコマンド リファレンス"の `up`の詳細を確認してください。
- サブネット名を使用してLIFのIPアドレスとネットワーク マスク値を割り当てる場合は、そのサブネットが存在している必要があります。

  サブネットには、同じレイヤー3サブネットに属するIPアドレスのプールが含まれます。 `network subnet create`コマンドを使用して作成されます。

  `network subnet create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-create.html["ONTAPコマンド リファレンス"^]を参照してください。

- LIFが処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5以前ではロールで指定していました。ONTAP 9.6以降ではサービス ポリシーで指定します。

タスク概要

- 同じネットワーク ポート上にIPv4とIPv6の両方のLIFを作成できます。
- クラスタ内に多数のLIFがある場合は、 `network interface capacity show`コマンドを使用してクラスタでサポートされているLIF容量を確認し、 `network interface capacity details show`コマンド（高度な権限レベル）を使用して各ノードでサポートされているLIF容量を確認できます。

  `network interface`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface["ONTAPコマンド リファレンス"^]をご覧ください。

- ONTAP 9.7以降では、同じサブネットにSVM用の他のLIFがすでに存在していれば、LIFのホーム ポートを指定する必要はありません。同じサブネットにすでに設定されている他のLIFと同じブロードキャスト ドメインにあるホーム ノードから任意のポートが自動的に選択されます。

手順

1. LIFを作成します。

   ```
   network interface create -vserver vserver_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以前*
`network interface create -vserver *vserver_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以降*

`network interface create -vserver *vserver_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}`

- サービス ポリシーを使用して LIF を作成する場合、 `-role`パラメータは必要ありません（ONTAP 9.6 以降）。
- サービス ポリシーを使用して LIF を作成する場合、 `-data-protocol`パラメータは不要です（ONTAP 9.6 以降）。ONTAP 9.5 以前を使用する場合は、LIF の作成時に `-data-protocol`パラメータを指定する必要があり、後で変更するにはデータ LIF を破棄して再作成する必要があります。
- `-home-node`は、 `network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノードです。

  `-auto-revert`オプションを使用して、
  LIFがホームノードとホームポートに自動的にリバートするかどうかも指定できます。

- `-home-port`は、LIF上で `network interface revert`コマンドが実行されたときにLIFが戻る物理ポートまたは論理ポートです。
- `-address`および `-netmask`オプションを使用してIPアドレスを指定することも、 `-subnet_name`オプションを使用してサブネットからの割り当てを有効にすることもできます。
- サブネットを使用してIPアドレスとネットワーク マスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときにゲートウェイへのデフォルトルートがSVMに自動的に追加されます。
- IPアドレスを手動で割り当てる場合（サブネットを使用せず）、クライアントまたはドメインコントローラが異なるIPサブネット上にある場合は、ゲートウェイへのデフォルトルートを設定する必要がある場合があります。 `network route create`およびSVM内での静的ルートの作成方法の詳細については、"ONTAPコマンド リファレンス"を参照してください。
- `-firewall-policy`オプションには、LIFロールと同じデフォルトの `data`を使用します。

  必要に応じて、カスタム ファイアウォール ポリシーをあとから作成して追加できます。

  ONTAP 9.10.1以降、ファイアウォールポリシーは廃止され、LIFサービスポリシーに完全に置き換えられました。詳細については、"LIFのファイアウォール ポリシーの設定"を参照してください。

- `-auto-revert`では、起動時、管理データベースのステータス変更時、ネットワーク接続時などの状況において、データLIFをホームノードに自動的にリバートするかどうかを指定できます。デフォルト設定は `false`ですが、環境のネットワーク管理ポリシーに応じて `false`に設定できます。

2. LIFが正常に作成されたことを確認します。

   ```
   network interface show
   ```

3. 設定したIPアドレスに到達できることを確認します。

対象	方法
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、LIF を作成し、 `-address`および `-netmask`パラメータを使用して IP アドレスとネットワーク マスクの値を指定します：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワーク マスク値を指定したサブネット（client1_sub）から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。データLIFのdatalif1とdatalif3にはIPv4アドレスが、datalif4にはIPv6アドレスが設定されています。

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         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.
```

次のコマンドは、 `default-data-files`サービス ポリシーが割り当てられたNASデータLIFを作成する方法を示しています：

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

関連情報

- "network ping"
- "network interface revert"

ONTAP SMBホスト名解決にDNSを有効にする

`vserver services name-service dns`コマンドを使用してSVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定できます。ホスト名は外部DNSサーバを使用して解決されます。link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+dns["ONTAPコマンドリファレンス"^]の `vserver services name-service dns`の詳細を確認してください。

開始する前に

ホスト名を検索するために、サイト規模のDNSサーバが使用できなければなりません。

単一障害点を回避するため、複数のDNSサーバーを設定する必要があります。 `vserver services name-service dns create`コマンドは、DNSサーバー名を1つだけ入力した場合に警告を発します。"ONTAPコマンドリファレンス"の `vserver services name-service dns create`の詳細をご覧ください。

タスク概要

"SVM でのダイナミック DNS の設定"についての詳細をご覧ください。

手順

1. SVM で DNS を有効にします： `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

   ```
   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
   ```

   この `vserver services name-service dns create`コマンドは自動構成検証を実行し、ONTAPがネームサーバに接続できない場合はエラーメッセージを報告します。

2. `vserver services name-service dns show`コマンドを使用してDNSドメイン構成を表示します。

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             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
   ```

次のコマンドは、SVM vs1のDNS設定の詳細を表示します。

```
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. `vserver services name-service dns check`コマンドを使用してネームサーバーのステータスを検証します。

```
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
```

Active DirectoryドメインでのSMBサーバのセットアップ

SMBサーバのONTAPタイムサービスを設定する

Active Directoryドメイン コントローラでSMBサーバを作成する前に、クラスタ時間とSMBサーバが参加するドメインのドメイン コントローラの時間のずれが5分以内であることを確認する必要があります。

タスク概要

Active Directory ドメインが使用するのと同じ NTP サーバーを使用するように、クラスター NTP サービスを構成する必要があります。

ONTAP 9.5以降では、対称認証を使用するようにNTPサーバをセットアップできます。

手順

1. `cluster time-service ntp server create`コマンドを使用してタイム サービスを設定します。
   - 対称認証なしでタイム サービスを構成するには、次のコマンドを入力します： `cluster time-service ntp server create -server server_ip_address`
   - 対称認証を使用してタイム サービスを構成するには、次のコマンドを入力します： `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. `cluster time-service ntp server show`コマンドを使用して、タイム サービスが正しく設定されていること

を確認します。

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

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

関連情報

- "クラスタ時刻サービス NTP"

NTPサーバ上で対称認証を管理するための**ONTAP**コマンド

ONTAP 9.5以降では、ネットワーク タイム プロトコル（NTP）バージョン3がサポートされます。NTPv3にはSHA-1鍵を使用した対称認証機能が含まれ、ネットワーク セキュリティが強化されます。

作業	使用するコマンド
対称認証を使用せずにNTPサーバを設定する	`cluster time-service ntp server create -server server_name`
対称認証を使用してNTPサーバを設定する	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
既存のNTPサーバで対称認証を有効にする。必要なキーIDを追加することで、既存のNTPサーバを変更して認証を有効にできます。	`cluster time-service ntp server modify -server server_name -key-id key_id`
共有NTPキーを設定する	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共有キーはIDで参照されます。ID、そのタイプ、および値が、ノードとNTPサーバで同じであることが必要です。
不明なキーIDでNTPサーバを設定する	`cluster time-service ntp server create -server server_name -key-id key_id`

作業	使用するコマンド
NTPサーバで設定されていないキーIDでサーバを設定する	`cluster time-service ntp server create -server server_name -key-id key_id` キーID、タイプ、および値が、NTPサーバの設定と同じであることが必要です。
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -authentication disabled`

関連情報

- "クラスタ時刻サービス NTP"

ONTAP Active Directory ドメインで SMB サーバを作成する

`vserver cifs create`コマンドを使用して、SVM 上に SMB サーバを作成し、そのサーバが属する Active Directory（AD）ドメインを指定できます。

開始する前に

データ処理に使用しているSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVM上で設定されているDNSサーバ、およびSMBサーバの追加先ドメインのADドメイン コントローラに接続できる必要があります。

SMBサーバの追加先とするADドメイン内のマシン アカウントの作成を許可されているユーザなら誰でも、SVM上にSMBサーバを作成できます。これには他のドメインのユーザを含めることができます。

ONTAP 9.7以降、AD管理者は、特権Windowsアカウントの名前とパスワードを提供する代わりに、キータブファイルへのURIを提供できるようになりました。URIを受け取ったら、 `vserver cifs`コマンドの `-keytab-uri`パラメータに含めてください。

タスク概要

Activity DirectoryドメインでSMBサーバを作成する場合の条件は次のとおりです。

- ドメインを指定するときは完全修飾ドメイン名（FQDN）を使用する必要があります。
- デフォルト設定では、SMBサーバ マシン アカウントはActive Directory CN=Computerオブジェクトに追加されます。
- `-ou`オプションを使用して、SMB サーバーを別の組織単位（OU）に追加することもできます。
- 必要に応じて、SMBサーバの1つ以上のNetBIOSエイリアス（最大200個）をカンマで区切って追加できます。

  SMBサーバのNetBIOSエイリアスを設定すると、他のファイル サーバのデータをSMBサーバに統合して、SMBサーバが元のファイル サーバの名前に応答するようにする場合に役立ちます。

`vserver cifs`とオプション
パラメータおよび命名要件の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP 9.8以降では、ドメイン コントローラへの接続を暗号化するように指定できます。 `-encryption-required-for-dc-connection`オプションが `true`に設定されている場合、ONTAPはドメイン コントローラ通信の暗号化を要求します。デフォルトは `false`です。このオプションを設定すると、暗号化はSMB3でのみサポートされているため、ONTAP-DC接続にはSMB3プロトコルのみが使用されます。。

"SMBの管理" には、SMB サーバー構成オプションに関する詳細情報が含まれています。

手順

1. クラスタで SMB のライセンスが付与されていることを確認します。 `system license show -package cifs`

   SMB ライセンスは"ONTAP One"に含まれています。ONTAP One をお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. AD ドメインに SMB サーバを作成します： `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]`

   ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

   次のコマンドは、ドメイン「`example.com`」に SMB サーバー「`smb_server01`」を作成します：

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

   次のコマンドは、ドメイン「`mydomain.com`」に SMB サーバ「`smb_server02`」を作成し、keytab ファイルを使用して ONTAP 管理者を認証します：

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

3. `vserver cifs show`コマンドを使用して SMB サーバ構成を確認します。

   この例では、コマンド出力は、SVM vs1.example.com 上に「`SMB_SERVER01`」という名前の SMB サーバが作成され、「`example.com`」ドメインに参加したことを示しています。

```
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. 必要に応じて、ドメイン コントローラとの暗号化通信を有効にします（ONTAP 9.8 以降）： `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

例

次のコマンドは、SVM vs2.example.com 上の「`example.com`」ドメインに「`smb_server02`」という名前の SMB サーバを作成します。マシン アカウントは「`OU=eng,OU=corp,DC=example,DC=com`」コンテナに作成されます。SMB サーバには NetBIOS エイリアスが割り当てられます。

```
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
```

次のコマンドは、別のドメインのユーザー（この場合は信頼されたドメインの管理者）が SVM vs3.example.com 上に「`smb_server03`」という名前の SMB サーバを作成できるようにします。 `-domain` オプションには、SMB サーバを作成するホーム ドメイン（DNS 設定で指定）の名前を指定します。 `username`オプションには、信頼されたドメインの管理者を指定します。

- ホーム ドメイン：example.com
- 信頼できるドメイン：trust.lab.com
- 信頼されたドメインのユーザー名：Administrator1

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

Username: Administrator1@trust.lab.com
Password: . . .
```

ONTAP SMB認証用のキータブファイルを作成する

ONTAP 9.7以降、ONTAPはキータブファイルを使用したActive Directory（AD）サーバによるSVM認証をサポートします。AD管理者はキータブファイルを生成し、ONTAP管理者がUniform Resource Identifier（URI）として使用できるようにします。このURIは、`vserver cifs`コマンドでADドメインのKerberos認証が必要な場合に提供されます。

AD管理者は、標準のWindows Server `ktpass`コマンドを使用してキータブ ファイルを作成できます。このコマンドは、認証が必要なプライマリ ドメインで実行する必要があります。この `ktpass`コマンドは、プライマリ ドメイン ユーザー用のキータブ ファイルのみを生成できます。信頼されたドメイン ユーザーを使用して生成されたキーはサポートされていません。

キータブ ファイルは、特定のONTAP管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更されない限り、特定の暗号化タイプとドメイン用に生成されるキーは変更されません。そのため、管理者ユーザのパスワードが変更されるたびに、新しいキータブ ファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- DES-CBC-MD5

  ONTAPはDES-CBC-CRC暗号化タイプをサポートしていません。

- RC4-HMAC

AES256 は最も高度な暗号化タイプであり、ONTAP システムで有効になっている場合は使用する必要があります。

キータブ ファイルは、管理者パスワードを指定するか、ランダムに生成されたパスワードを使用して生成できます。ただし、キータブ ファイル内の鍵を復号するには、AD サーバーで管理者ユーザー固有の秘密鍵が必要となるため、一度に使用できるパスワード オプションは 1 つだけです。特定の管理者の秘密鍵が変更されると、キータブ ファイルは無効になります。

ワークグループでの**SMB**サーバのセットアップ

ONTAPワークグループにおける**SMB**サーバ構成について学ぶ

SMB サーバーをワークグループのメンバーとして設定するには、SMB サーバーを作成し、次にローカル ユーザーとグループを作成します。

Microsoft Active Directory ドメイン インフラストラクチャが利用できない場合は、ワークグループ内に SMB サーバーを設定できます。

ワークグループ モードの SMB サーバーは、NTLM 認証のみをサポートし、Kerberos 認証はサポートしません。

指定されたワークグループを持つ **ONTAP SVM** 上に **SMB** サーバを作成します

`vserver cifs create`コマンドを使用して、SVM 上に SMB サーバを作成し、そのサーバが属するワークグループを指定できます。

開始する前に

データ処理に使用しているSVMおよびLIFが、SMBプロトコルを許可するように設定されている必要があります。LIFは、SVM上で設定されているDNSサーバに接続できる必要があります。

タスク概要

ワークグループ モードのSMBサーバでは、次のSMB機能はサポートされません。

- SMB3監視プロトコル
- SMB3 CA共有
- SQL over SMB
- フォルダ リダイレクト
- 移動プロファイル
- グループ ポリシー オブジェクト（GPO）
- ボリュームSnapshotサービス（VSS）

`vserver cifs`とオプションの構成パラメータおよび命名要件の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs["ONTAPコマンドリファレンス"^]を参照してください。

手順

1. クラスタで SMB のライセンスが付与されていることを確認します。 `system license show -package cifs`

   SMB ライセンスは"ONTAP One"に含まれています。ONTAP One をお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

   SMBサーバを認証のみに使用する場合は、CIFSライセンスは必要ありません。

2. ワークグループに SMB サーバを作成します： `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   次のコマンドは、ワークグループ “workgroup01” に SMB サーバー “smb_server01” を作成します：

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

3. `vserver cifs show`コマンドを使用して SMB サーバ構成を確認します。

   次の例では、コマンド出力に、“smb_server01” という名前の SMB サーバが SVM vs1.example.com のワークグループ “workgroup01” に作成されたことが示されています：

```
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: -
```

終了後の操作

ワークグループ内のCIFSサーバに関しては、SVM上でローカル ユーザ、およびオプションでローカル グループを作成する必要があります。

関連情報

"SMBの管理"

ローカル **ONTAP SMB** ユーザー アカウントを作成する

SVMに格納されたデータへのSMB接続によるアクセスの許可に使用できるローカル ユーザ アカウントを作成できます。ローカル ユーザ アカウントは、SMBセッションを作成する際の認証に使用することもできます。

タスク概要

ローカル ユーザの機能は、SVMの作成時にデフォルトで有効になります。

ローカル ユーザ アカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付けるSVMを指定する必要があります。

`vserver cifs users-and-groups local-user`とオプション
パラメータおよび命名要件の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs+users-and-groups+local-user["ONTAPコマンド リファレンス"^]を参照してください。

手順

1. ローカル ユーザーを作成します： `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   次のオプションのパラメータが役に立つ場合があります。

   - `-full-name`

     ユーザのフルネーム。

   - `-description`

     ローカル ユーザの説明。

   - `-is-account-disabled {true|false}`

     ユーザ アカウントが有効か無効かを指定します。このパラメータを指定しない場合、ユーザ アカウントはデフォルトで有効になります。

   ローカル ユーザのパスワードを入力するよう求めるプロンプトが表示されます。

2. ローカル ユーザのパスワードを入力し、確認のためにもう一度入力します。
3. ユーザーが正常に作成されたことを確認します： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

次の例では、SVM vs1.example.com に関連付けられた、フルネームが「`Sue Chang`」であるローカル ユーザー「`SMB_SERVER01\sue`」を作成します：

```
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
```

ローカル**ONTAP SMB**グループを作成する

SMB接続を介してSVMに関連付けられたデータへのアクセスを承認するために使用できるローカル グループを作成できます。また、グループのメンバーに付与するユーザ権限や機能を定義する権限を割り当てることもできます。

タスク概要

SVM の作成時に、ローカル グループ機能がデフォルトで有効になります。

ローカル グループを作成する際は、グループ名と、グループを関連付ける SVM を指定する必要があります。グループ名はローカル ドメイン名の有無にかかわらず指定でき、必要に応じてローカル グループの説明も指定できます。ローカル グループを別のローカル グループに追加することはできません。

`vserver cifs users-and-groups local-group`とオプション パラメータおよび命名要件の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs+users-and-groups+local-group["ONTAPコマンド リファレンス"^]を参照してください。

手順

1. ローカル グループを作成します： `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   次のオプション パラメータが役に立つ場合があります：

   - `-description`

     ローカル グループの説明を指定します。

2. グループが正常に作成されたことを確認します： `vserver cifs users-and-groups local-group show -vserver vserver_name`

例

次の例では、SVM vs1 に関連付けられたローカル グループ “SMB_SERVER01\engineering” を作成します：

```
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
```

終了後の操作

新しいグループにメンバーを追加する必要があります。

ローカル**ONTAP SMB**グループメンバーシップを管理する

ローカル グループのメンバーシップを管理するには、ローカル ユーザまたはドメイン ユーザを追加または削除するか、ドメイン グループを追加または削除します。これは、グループに設定されたアクセス制御に基づいてデータへのアクセスを制御する場合や、ユーザにそのグループに関連付けられた権限を付与する場合に便利です。

タスク概要

ローカル ユーザー、ドメイン ユーザー、またはドメイン グループに、グループのメンバーシップに基づくアクセス権や権限を付与する必要がなくなった場合は、グループからメンバーを削除できます。

ローカル グループにメンバーを追加するときは、次の点に留意する必要があります：

- 特別な *Everyone* グループにユーザーを追加することはできません。
- 別のローカル グループにローカル グループを追加することはできません。
- ドメイン ユーザーまたはグループをローカル グループに追加するには、ONTAP が名前を SID に解決できる必要があります。

ローカル グループからメンバーを削除するときは、次の点に留意する必要があります：

- 特別な *Everyone* グループからメンバーを削除することはできません。
- ローカル グループからメンバーを削除するには、 ONTAP がそのメンバーの名前を SID に解決できる必要があります。

手順

1. グループにメンバーを追加したり、グループからメンバーを削除したりします。

- メンバーを追加： `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  ローカル ユーザ、ドメイン ユーザ、またはドメイン グループをカンマで区切って指定し、指定したローカル グループに追加することができます。

- メンバーを削除する： `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  ローカル ユーザ、ドメイン ユーザ、またはドメイン グループをカンマで区切って指定し、指定したローカル グループから削除することができます。

例

次の例では、SVM vs1.example.com 上のローカル グループ “SMB_SERVER01\engineering” にローカル ユーザー “SMB_SERVER01\sue” を追加します：

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

次の例では、SVM vs1.example.com 上のローカル グループ “SMB_SERVER01\engineering” からローカル ユーザー “SMB_SERVER01\sue” と “SMB_SERVER01\james” を削除します：

```
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
```

有効な**ONTAP SMB**バージョンを確認する

クライアントおよびドメイン コントローラとの接続に対してデフォルトで有効になっているSMBのバージョンは、ONTAP 9のリリースによって決まります。ご使用の環境で必要なクライアントと機能を、SMBサーバがサポートしていることを確認する必要があります。

タスク概要

クライアントとドメイン コントローラの両方と接続するために、可能な場合は常にSMB 2.0以降を有効にする必要があります。セキュリティ上の理由から、SMB 1.0の使用は避け、お使いの環境で不要だと確認できた場合は無効にする必要があります。

ONTAP 9.3以降、新しいSVMではデフォルトで無効になっています。

> `-smb1-enabled-for-dc-connections`が `false`に設定されている場合に`-smb1-enabled`が `true`に設定されると、ONTAPはクライアントとしてSMB 1.0接続を拒否しますが、サーバとして着信SMB 1.0接続を引き続き受け入れます。

"SMBの管理" には、サポートされている SMB バージョンと機能に関する詳細が記載されています。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 有効になっているSMBのバージョンを確認します。

```
vserver cifs options show
```

リストを下方向にスクロールすると、クライアント接続用に有効になっているSMBのバージョンを表示できます。また、ADドメイン内のSMBサーバを設定している場合は、ADドメイン接続用に有効になっているバージョンを表示できます。

3. 必要に応じて、クライアント接続用のSMBプロトコルを有効または無効にします。
   - SMBバージョンを有効にする場合：

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

`smb_version`の可能な値：

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

     次のコマンドは、SVM vs1.example.comでSMB 3.1を有効にします： `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true`

   - SMBバージョンを無効にする場合：

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

4. SMBサーバがActive Directoryドメイン内にある場合は、必要に応じて、DC接続用のSMBプロトコルを有効または無効にします。
   - SMBバージョンを有効にする場合：

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

- SMBバージョンを無効にする場合：

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

5. admin権限レベルに戻ります。

```
set -privilege admin
```

DNS サーバー上の ONTAP SMB サーバーをマッピングする

Windows ユーザーがドライブを SMB サーバー名にマップできるように、サイトの DNS サーバーには、SMB サーバー名とすべての NetBIOS エイリアスをデータ LIF の IP アドレスにポイントするエントリが必要です。

開始する前に

サイトのDNSサーバーへの管理者権限が必要です。管理者権限がない場合は、DNS管理者にこの作業を依頼してください。

タスク概要

SMB サーバー名に NetBIOS エイリアスを使用する場合は、エイリアスごとに DNS サーバー エントリ ポイントを作成することをお勧めします。

手順

1. DNSサーバにログインします。
2. 前方（A - アドレス レコード）および逆方向（PTR - ポインター レコード）のルックアップ エントリを作成して、SMB サーバー名をデータ LIF の IP アドレスにマッピングします。
3. NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソース レコード）ルックアップ エントリを作成し、各エイリアスを SMB サーバーのデータ LIF の IP アドレスにマッピングします。

結果

マッピングがネットワーク全体に伝播された後、Windows ユーザーはドライブを SMB サーバー名またはその NetBIOS エイリアスにマッピングできます。

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ONTAPストレージへのSMBクライアントアクセスを構成する

SVM上の共有ストレージへのSMBクライアント アクセスを提供するには、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、共有と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

- SMB は SVM 上で完全に設定されている必要があります。
- ネーム サービス構成の更新はすべて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構成への追加または変更はすべて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 コンテナの作成

ONTAP SMB ボリュームを作成する

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

タスク概要

ボリュームのデータをクライアントが利用できるようにするには、ボリュームに_ジャンクション パス_が必要です。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、 `volume mount`コマンドを使用してSVMネームスペースにボリュームを_マウント_する必要があります。

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トラッキングを有効にした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、 `-analytics-state`または `-activity-tracking-state`を `on`に設定した `volume create`コマンドを発行します。

  容量分析とアクティビティ追跡の詳細については、 "ファイルシステム分析の有効化"を参照してください。"ONTAPコマンド リファレンス"の `volume create`の詳細を確認してください。

手順

1. ジャンクション ポイントを持つ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`*]

   `-junction-path`の選択肢は次のとおりです：

   - たとえば、ルートの直下に `/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に、例えば `/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（例：`/new_dir/new_vol`）、まず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する必要があります。次に、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. ボリュームが目的のジャンクション ポイントで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とアグリゲートaggr1上にusers1という新しいボリュームを作成します。この新しいボリュームは `/users`で利用可能になります。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
```

次のコマンドは、SVM「vs1.example.com」とアグリゲート「aggr1」に「home4」という名前の新しいボリュームを作成します。ディレクトリ `/eng/`はvs1 SVMの名前空間にすでに存在しており、新しいボリュームは `/eng/home`で使用可能になり、これが `/eng/`名前空間のホームディレクトリになります。ボリュームのサイズは750 GB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 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
```

ONTAP SMB qtreeを作成する

`volume qtree create`コマンドを使用して、データを格納するqtreeを作成し、そのプロパティを指定できます。

開始する前に

- 新しいqtreeを格納するSVMと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がNTFSで、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ことも、qtree パスの引数を`/vol/volume_name/_qtree_name`の形式で指定することもできます。

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

次の例では、ジャンクション パス `/vol/data1`を持つSVM vs1.example.comにあるqt01という名前のqtreeを作成します：

```
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
```

ONTAP SMB共有を作成する際の要件と考慮事項

SMB 共有を作成する前に、共有パスと共有プロパティ（特にホーム ディレクトリ）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（`vserver cifs share create`コマンドの `-path`オプションを使用して）指定する必要があります。このディレクトリ パスは、SVM ネームスペースに作成したボリュームまたはqtreeのジャンクション パスに対応します。共有を作成する前に、ディレクトリ パスと対応するジャンクション パスが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文字まで入力できます。
- パス名にスペースがある場合は、文字列全体を引用符で囲む必要があります（例： `"/new volume/mount here"`）。
- 共有の UNC パス(`\\servername\sharename\filepath`に 256 文字以上（UNC パスの最初の “\\” を除く）が含まれている場合、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ようにしてください。

共有プロパティのデフォルトは変更できます：

- 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。
- 共有の作成時に共有プロパティを指定することもできます。

  ただし、共有の作成時に共有プロパティを指定した場合、デフォルトは使用されません。 `-share-properties`パラメータを共有の作成時に使用する場合は、共有に適用するすべての共有プロパティをカンマ区切りのリストで指定する必要があります。

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

  この機能を使用すると、接続するユーザーと一連の変数に基づいて、異なるディレクトリにマッピングされる共有を設定できます。ユーザーごとに個別の共有を作成する代わりに、いくつかのホーム ディレクトリ パラメータを使用して単一の共有を設定することで、エントリ ポイント（共有）とホーム ディレクトリ（SVM上のディレクトリ）の関係を定義できます。

  共有の作成後は、このプロパティを追加または削除できません。

ホーム ディレクトリ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、 `vserver cifs home-directory search-path add`コマンドを使用して少なくとも 1 つのホーム ディレクトリ検索パスを追加する必要があります。
- `-share-properties`パラメータの `homedirectory`の値によって指定されるホーム ディレクトリ共有には、共有名に `%w`（Windows ユーザー名）動的変数を含める必要があります。

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

- 管理者またはユーザーが共有を使用して他のユーザーのホーム ディレクトリに接続する場合（ `vserver cifs home-directory modify`コマンドのオプションを使用）、動的な共有名パターンの前にチル

ダ (~`を付ける必要があります。

> `vserver cifs share`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs+share["ONTAPコマンドリファレンス"^]をご覧ください。

関連情報

- "SMBの管理"

ONTAP SMB 共有を作成する

SMB サーバから SMB クライアントとデータを共有するには、まず SMB 共有を作成する必要があります。共有を作成する際に、共有をホーム ディレクトリとして指定するなど、共有のプロパティを設定できます。また、オプションの設定を行って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 名前空間に存在している必要があります。

タスク概要

共有を作成すると、デフォルトの共有 ACL（デフォルトの共有権限）は `Everyone / Full Control`になります。共有へのアクセスをテストした後、デフォルトの共有 ACL を削除し、より安全な ACL に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、共有の作成時に `-path`オプションで指定されたパスをチェックします。指定されたパスが存在しない場合、コマンドは失敗します。

2. 指定された SVM に関連付けられた 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、SVM `vs1.example.com`上に「`SHARE1」という名前の SMB 共有を作成します。ディレクトリパスは `/users`で、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
```

ONTAP SMB クライアント アクセスを確認する

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サーバー名とNetBIOSエイリアスを使用してアクセスをテストしてください。

手順

1. Windows クライアントにログインします。
2. SMB サーバー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、次の形式でドライブを共有にマップします： `\\SMB_Server_Name\Share_Name`

      マッピングが成功しない場合は、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。後ほど、SMBサーバー名を使用してアクセスをテストする必要があります。

      SMB サーバーの名前が vs1.example.com で、共有の名前が SHARE1 の場合、次のように入力する必要があります： `\\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、そのファイルを削除します。

   SMB サーバー名を使用して共有への書き込みアクセスを確認しました。

3. すべての NetBIOS エイリアスに対して手順 2 を繰り返します。

ONTAP SMB共有アクセス制御リストを作成する

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に対するアクセス 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ーまたはグループを決定する必要があります。

タスク概要

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、セキュリティ上のリスクがあるデフォルトの共有ACL `Everyone / Full Control`を削除する必要があります。

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。

...を使用して**ACL**を構成する場合は、...	コマンドを入力してください...
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. `vserver cifs share access-control show`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。

例

次のコマンドは、「vs1.example.com」SVM 上の「sales」共有に対する Change`権限を「`Sales Team」Windows グループに付与します：

```
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
```

次のコマンドは、「Tiger Team」という名前のローカル Windows グループに Change`権限を付与し、「`Sue Chang」という名前のローカル Windows ユーザーに Full_Control`権限を付与します（「`vs1」SVM 上の「datavol5」共有）：

```
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
```

ONTAP SMB共有でNTFSファイル権限を構成する

あ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クライアントから、その共有内のファイルとディレクトリに対してNTFSファイル権限を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。

タスク概要

"SMBの管理"および Windows のドキュメントには、標準および高度な NTFS アクセス許可を設定する方法に関する情報が記載されています。

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. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て 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、権限を適用するデータが含まれている共有を含む SMB サーバー名と共有の

名前を入力します。

SMB サーバー名が SMB_SERVER01 で、共有名が「SHARE1」の場合は、`\\SMB_SERVER01\SHARE1`と入力します。

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アドレスを指定することもできます。

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となり、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。

「セキュリティ」タブには、NTFS権限が設定されているユーザーとグループのリストが表示されます。<Object>の権限ボックスには、選択したユーザーまたはグループに有効な「許可」および「拒否」権限のリストが表示されます。

7. *編集*をクリックします。

<Object>の権限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。

次の操作を行う場合は....	操作
新しいユーザーまたはグループに標準の NTFS 権限を設定する	a. *[追加]*をクリックします。 [ユーザー、コンピューター、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アクセス許可を追加するユーザー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。
ユーザーまたはグループの標準 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	以下の手順を実行してください
新規または既存のユーザーまたはグループに標準の NTFS 権限を設定する	*<Object>の権限*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拒否するアクセスの種類について、*許可*または*拒否*のチェックボックスをオンにします。
ユーザーまたはグループを削除する	*削除*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が選択できない場合は、権限が親オブジェクトから継承されているためです。*特別な権限*ボックスは選択できません。このボックスが選択されている場合は、選択したユーザーまたはグループに対して、1つ以上の詳細な権限が設定されていることを意味します。

10. そのオブジェクトに対する NTFS アクセス許可の追加、削除、または編集が完了したら、**OK** をクリックします。

ONTAP SMB ユーザー共有アクセスを確認する

設定したユーザが SMB 共有とそこ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、共有へのアクセス権を持つユーザーの 1 人としてログインします。
2. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て 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 サーバー名が SMB_SERVER01 で、共有名が「`SHARE1`」の場合は、`\\SMB_SERVER01\share1`と入力します。

   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となり、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、そのファイルが存在することを確認して、テキストを書き込んでから、テストファイルを削除します。