CLIを使用したSMBの設定

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用したSMBの設定

CLIヲシヨウシタSMBセツテイノカイヨウ

ONTAP 9 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できます。

SMB(Server Message Block) は、 Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（ CLI ）および OnCommand 管理ツールでは、 _cifs_という メッセージが引き続き表示されます。

次の手順は、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バージョン2以降を使用する。
- NFSクライアントではなく、SMBクライアントのみを処理する（マルチプロトコル構成ではない）。
- 新しいボリュームはNTFSファイル権限を使用して保護されます。
- SVM管理者Privilegesではなく、クラスタ管理者Privilegesが必要です。

  SVM と LIF を作成するにはクラスタ管理者権限が必要です。他の SMB 設定タスクには、 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設定する方法については、を参照してください"NFSとSMBの両方を使用したWindowsとLinux用のNASストレージのプロビジョニング"。

- 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。

  コマンド構文の詳細については、CLIヘルプおよびONTAPのマニュアルページ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、を参照して"SMBリファレンスノガイヨウ"ください。

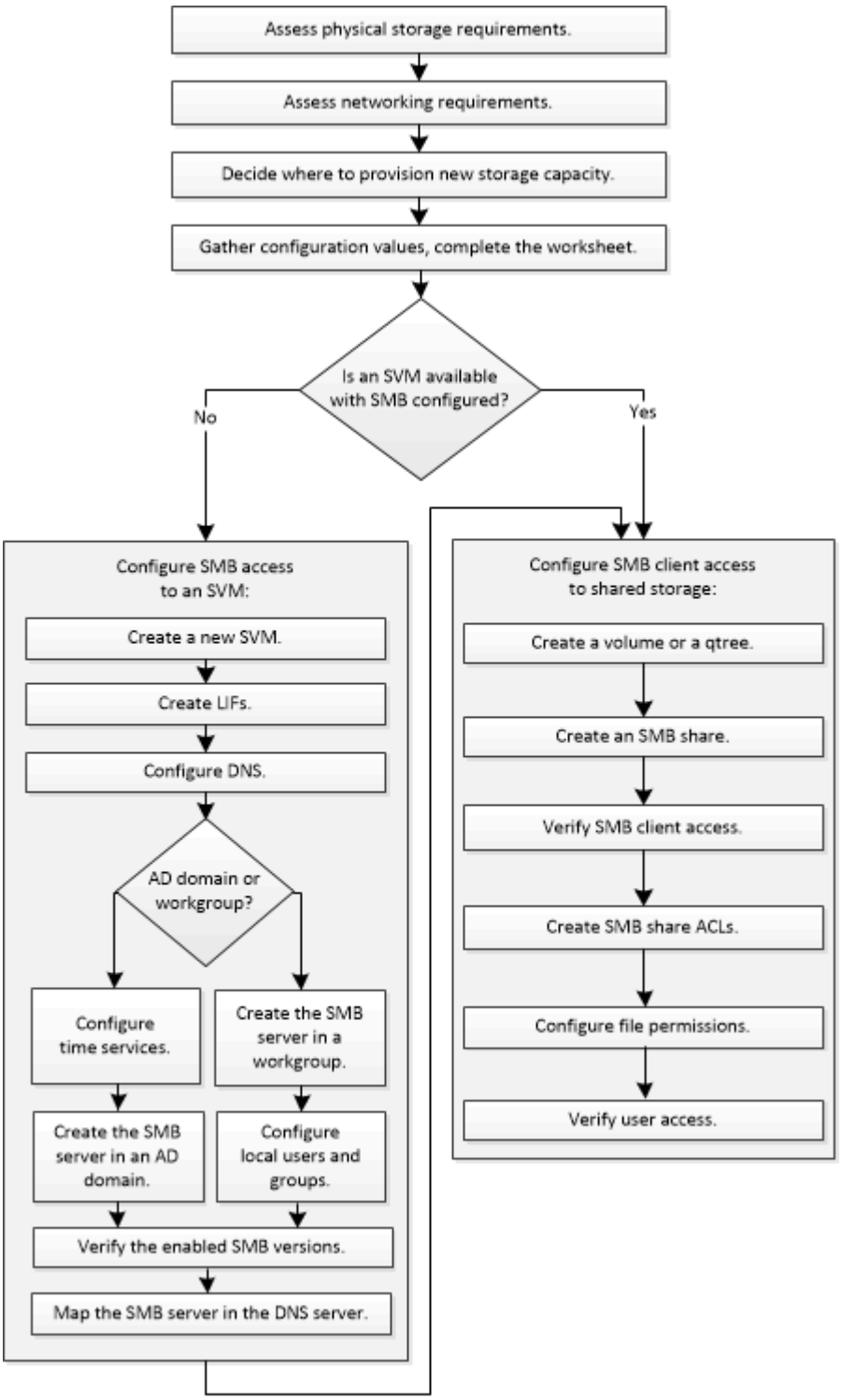
ONTAPで実行するその他の方法

実行するタスク	参照先
再設計された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セツテイノカイヨウ"

SMBの設定ワークフロー

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、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を追加します。



準備

物理ストレージ要件の評価

クライアント用の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用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. 十分なスペースを備えたアグリゲートがない場合は、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 `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成し `storage aggregate create`ます。

ネットワーク要件の評価

クライアントにSMBストレージを提供する前に、SMBプロビジョニングの要件を満たすようにネットワーク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。

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も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。
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場合は、サブネットが存在し、十分な数のアドレスが使用可能であることを確認します。 `network subnet show`

   サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。
3. 使用可能なIPspaceを表示します。 `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。
4. IPv6アドレスを使用する場合は、IPv6がクラスタで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、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

新しい**SMB**ストレージ容量のプロビジョニング先を決定する

新しい SMB ボリュームまたは qtree を作成する前に、その配置先を新規、既存のどちらの SVM にするかを決め、 SVM に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。この決定によって、ワークフローが決まります。

選択肢

- 新しい SVM 、または SMB が有効になっているものの設定されていない既存の SVM 上でボリュームまたは 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」の両方の手順を実行します。

  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を初めて有効にする場合。
  - クラスタ内の既存のSVMでSMBサポートを有効にするのが望ましくない場合。
  - クラスタ内に SMB 対応 SVM が 1 つ以上あり、次のいずれかの接続が必要な場合。
    - ワークグループ内の別の Active Directory フォレストへの接続。
    - 分離されたネームスペース内の SMB サーバへの接続（マルチテナンシーシナリオ）。SMBが有効になっているが設定はまだ完了していない既存のSVMで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、SANアクセス用のSVMを作成した場合や、SVM作成時にプロトコルが有効になっていなかった場合に該当します。

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 アクセスの設定が完了している既存の SVM でボリュームまたは 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」の手順を実行します。

  共有ストレージへの SMB クライアントアクセスの設定

SMB設定情報を収集するためのワークシート

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関する決定に応じて、ワークシートのいずれか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

パラメータの詳細については、コマンドのマニュアルページを参照してください。

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、コマンドで次の値を指定します `vserver create`。

フィールド	説明	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。	

フィールド	説明	あなたの価値
`-rootvolume-security-style`	SVMのNTFSセキュリティ形式を使用します。	`ntfs`
`-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 が配置される個別の IP アドレススペースです。	

- LIF 作成用のパラメータ *

LIFを作成する場合は、コマンドで次の値を指定します `network interface create`。

フィールド	説明	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`	LIFに対してコマンドを実行したときにLIFが戻るノード `network interface revert`。	
`-home-port`	LIFに対してコマンドを実行したときにLIFが戻るポートまたはインターフェイスグループ `network interface revert`。	
`-address`	新しいLIFによるデータアクセスに使用する、クラスタ上のIPv4アドレスまたは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。	
`-subnet`	IPアドレスのプール。および `-netmask`の代わりに使用して `-address`、アドレスとネットマスクを自動的に割り当てます。	

フィールド	説明	あなたの価値
`-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下でデータ LIF がホームノードに自動的にリバートされるかどうかを指定します。デフォルト設定はです `false`。	

- DNS ホスト名解決のパラメータ *

DNSを設定する場合は、コマンドで次の値を指定します `vserver services name-service dns create`。

フィールド	説明	あなたの価値
`-domains`	最大5つのDNSドメイン名。	
`-name-servers`	DNSネームサーバごとに最大3つのIPアドレス。	

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 *

タイムサービスを設定する場合は、コマンドで次の値を指定します `cluster time-service ntp server create`。

フィールド	説明	あなたの価値
`-server`	Active Directory ドメイン用の NTP サーバのホスト名または IP アドレスを指定します。	

- Active Directory ドメイン内に 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、ドメイン情報を指定する場合は、コマンドで次の値を指定します `vserver cifs create`。

フィールド	説明	あなたの価値
`-vserver`	SMB サーバを作成する SVM の名前を指定します。	

フィールド	説明	あなたの価値
`-cifs-server`	SMB サーバの名前（最大 15 文字）を指定します。	
`-domain`	SMB サーバに関連付ける Active Directory ドメインの完全修飾ドメイン名（ FQDN ）を指定します。	
`-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を指定します。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： NetBIOS エイリアスのリストを指定します。 NetBIOS エイリアスは、 SMB サーバ名の別名です。	
`-comment`	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

ワークグループでの**SMB**サーバのセットアップ

- ワークグループで SMB サーバー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場合は、コマンドで次の値を指定します `vserver cifs create`。

フィールド	説明	あなたの価値
`-vserver`	SMB サーバを作成する SVM の名前を指定します。	
`-cifs-server`	SMB サーバの名前（最大 15 文字）を指定します。	
`-workgroup`	ワークグループの名前（最大 15 文字）を指定します。	

フィールド	説明	あなたの価値
-comment	オプション：サーバのテキストコメントを指定します。Windowsクライアントは、ネットワーク上のサーバを参照するときに、SMBサーバの説明を確認できます。	

- ローカルユーザー作成用のパラメータ *

コマンドを使用してローカルユーザを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-user create`ます。これらの値は、ワークグループ内、およびオプションで AD ドメイン内の SMB サーバに必要です。

フィールド	説明	あなたの価値
-vserver	ローカルユーザを作成する SVM の名前を指定します。	
-user-name	ローカルユーザの名前（最大 20 文字）を指定します。	
-full-name	オプション：ユーザのフルネームを指定します。フルネームにスペースが含まれている場合は、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。説明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 *

コマンドを使用してローカルグループを作成する場合は、次の値を指定し `vserver cifs users-and-groups local-group create`ます。AD ドメインおよびワークグループ内の SMB サーバの場合はオプションです。

フィールド	説明	あなたの価値
-vserver	ローカルグループを作成する SVM の名前を指定します。	

フィールド	説明	あなたの価値
`-group-name`	ローカルグループの名前（最大256 文字）を指定します。	
`-description`	オプション：ローカルグループの概要。説明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。	

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、コマンドで次の値を指定します `volume create`。

フィールド	説明	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ボリューム用の十分なスペースがある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、コマンドで次の値を指定します `volume qtree create`。

フィールド	説明	あなたの価値
`-vserver`	qtreeを含むボリュームが配置されているSVMの名前。	

フィールド	説明	あなたの価値
`-volume`	新しいqtreeを格納するボリュームの名前。	
`-qtree`	新しいqtreeには、64文字以下の一意のわかりやすい名前を指定します。	
`-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、qtreeパスをの形式で `/vol/volume_name/qtree_name\>` 指定できます。	

- SMB 共有作成のパラメータ *

コマンドでは、次の値を指定します `vserver cifs share create`。

フィールド	説明	あなたの価値
`-vserver`	SMB 共有を作成する SVM の名前を指定します。	
`-share-name`	作成する SMB 共有の名前（最大 256 文字）を指定します。	
`-path`	SMB 共有へのパスの名前（最大 256 文字）を指定します。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を指定します。デフォルト設定は `oplocks`、、 `browsable changenotify`、および `show-previous-versions`です。	
`-comment`	オプション：サーバのテキストコメント（最大 256 文字）を指定します。Windows クライアントは、ネットワーク上で参照するとき、この SMB 共有概要を確認できます。	

- 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 *

コマンドでは、次の値を指定します `vserver cifs share access-control create`。

フィールド	説明	あなたの価値
`-vserver`	SMB ACL を作成する SVM の名前を指定します。	
`-share`	作成先の SMB 共有の名前を指定します。	
`-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を指定します。デフォルトのタイプはです。`windows`	`windows`
`-user-or-group`	共有の ACL に追加するユーザまたはグループを指定します。ユーザ名を指定する場合は、「ドメイン名」の形式でユーザ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

SVMへのSMBアクセスの設定

SMB クライアントアクセス用に SVM を設定していない場合は、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 を設定する場合は、 SVM ルートボリュームへのアクセスを許可し、 SMB サーバを作成し、 LIF を作成し、ホスト名解決を有効にし、ネームサービスを設定し、必要に応じて Kerberos セキュリティの有効化。

SVMの作成

SMBクライアントにデータアクセスを提供するSVMがクラスタ内に1つもない場合は、SVMを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、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

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*

- オプションにはNTFS設定を使用し `-rootvolume-security-style`ます。
- デフォルトのC.UTF-8オプションを使用し `-language`ます。
- この `ipspace`設定はオプションです。

2. 新しく作成したSVMの設定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`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`フィールドには状態が表示されている必要があり`running`ます。状態が表示された場合は`initializing`、ルートボリュームの作成などの中間処理が失敗したため、`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、データアクセス用のSVMをIPspace内に作成し `ipspaceA`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でSVMが作成され、自動的に起動されて状態になっていることを示しています `running`。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あるため、ルートボリュームは作成時に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の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

SVMでSMBプロトコルが有効になっていることを確認する

SVMでSMBを設定して使用する前に、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。

タスクの内容

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

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

手順

1. SVMに対して現在有効または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`

   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 `vserver show-protocols`。

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手順は次のとおりです。 `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. 有効なプロトコルと無効な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 SVM で現在有効 / 無効（許可 / 不許可）になっている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SVMで有効になっているプロトコルのリストにを追加することで、SMB経由のアクセスを許可し `cifs`ます。

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

SVMルートボリュームのエクスポートポリシーを開く

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。

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対して自動的に作成されます。SVM上のデータにクライアントから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のルールを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アクセスが開いていることを確認してから、個 々 のボリュームまたはqtreeにカスタムのエクスポートポリシーを作成して個 々 の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エクスポートポリシーを確認します。
`vserver export-policy rule show`

   次のようなコマンド出力が表示されます。

```
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このようなルールが存在する場合、このタスクは完了です。表示されない場合は、次の手順に進みます。

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. コマンドを使用してルールの作成を確認します `vserver export-policy rule show`。

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、すべてのSMBクライアントからアクセスできるようになります。

LIFの作成

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ため、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の管理 `up`ステータスがに設定されている必要があります。
- 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、そのサブネットがすでに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3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

- LIFで処理され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、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。
- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、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内の指定したホームノード上の任意のポートを自動的に選択します。

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}`

   - `-role`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。
   - `-data-protocol`サービスポリシー（ONTAP 9 6以降）を使用してLIFを作成する場合は、パラメータは必要ありません。ONTAP 9 .5以前を使用している場合は `-data-protocol`、LIFの作成時にパラメータを指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
   - `-home-node`は、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

     オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
- オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
- 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（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。 `network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

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

  ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。

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	使用方法
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、パラメータと `-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値を指定し `-address`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。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
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、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 `default-data-files`ます。

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

ホスト名解決のための**DNS**の有効化

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 `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

開始する前に

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

SVM での動的 DNS の設定については、『ネットワーク管理ガイド』を参照してください。

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
   ```

   ONTAP 9 .2以降では `vserver services name-service dns create`、コマンドによって設定の自動検証が実行され、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が報告されます。

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

   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
```

次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

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

   この `vserver services name-service dns check`コマンドは、ONTAP 9 .2以降で使用できます。

```
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

タイムサービスの設定

アクティブ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サーバが属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。

タスクの内容

Active Directoryドメインと同じNTPサーバを時刻の同期に使用するようにクラスタNTPサービスを設定する必要があります。

手順

1. コマンドを使用してタイムサービスを設定します `cluster time-service ntp server create`。
   - 対称認証を使用せずにタイムサービスを設定するには、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設定するには、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. 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`。

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

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

NTPサーバの対称認証の管理用コマンド

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キーを使用した対称認証が含まれているため、ネットワークセキュリティが向上します。

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サーバの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することができます。	`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サーバの両方で同じである必要があります。

作業	使用するコマンド
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`
NTPサーバで設定されていないキーIDでサーバを設定します。	`cluster time-service ntp server create -server server_name -key-id key_id` キーID、タイプ、および値は、NTPサーバに設定されているキーID、タイプ、および値と同じである必要があります。
対称認証を無効にする	`cluster time-service ntp server modify -server server_name -authentication disabled`

Active Directoryドメインに**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のActive Directory（AD）ドメインを指定できます `vserver cifs create`。

開始する前に

データ処理に使用する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サーバの追加先の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すべてのユーザが、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以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

タスクの内容

Activity DirectoryドメインにSMBサーバを作成する場合は、次の点に注意してください。

- ドメインを指定するときは、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）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。
- オプションを使用すると、SMBサーバを別の組織単位（OU）に追加できます `-ou`。
- 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）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、SMBサーバが元のサーバの名前に応答するようにする場合に役立ちます。

その他のオプションのパラメータと命名要件については、のマニュアルページを参照して `vserver cifs`ください。

> SMB.1以降では、ONTAP 9バージョン2.0からドメインコントローラ（DC）への接続を有効にすることができます。この処理は、ドメインコントローラでSMB 1.0を無効にしている場合に必要です。SMB.2以降では、ONTAP 9 2.0がデフォルトで有効になります。

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。ONTAPオプションがに設定され `true`ている場合、ドメインコントローラの通信に暗号化が必要です `-encryption-required-for-dc-connection`。デフォルトはです。 `false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。です。

"SMBの管理"SMBサーバ設定オプションの詳細については、を参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"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「 '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「 m ydomain.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. コマンドを使用して、SMBサーバの設定を確認します `vserver cifs show`。

   この例では、「 `s MB_SERVER01' 」という名前の SMB サーバが SVM vs1.example.com 上に作成され、「 example.com`" ドメイン」に追加されたことがコマンド出力に示されています。

```
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（ONTAP 9 .8以降）との暗号化通信を有効にします。 `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 の「 example.com`" 」ドメインに「 'MB_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（ここでは信頼できるドメインの管理者）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。オプションは `-domain`、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。オプションは `username`、信頼できる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
- 信頼できるドメインのユーザ名： Administrator1

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

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

SMB認証用の**keytab**ファイルの作成

ONTAP 9.7 以降 ONTAP では、 keytab ファイルを使用した Active Directory （ AD ）サーバとの SVM 認証がサポートされます。AD管理者はkeytabファイルを生成し、Uniform Resource Identifier（URI）としてONTAP管理者が使用できるようにします。このURIは、コマンドでADドメインとのKerberos認証が必要な場合に指定します `vserver cifs`。

AD管理者は、Windows Serverの標準コマンドを使用してkeytabファイルを作成できます `ktpass`。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。 `ktpass`コマンドを使用してkeytabファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされません。

keytab 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かぎり、特定の暗号化タイプとドメインに対して生成された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を変更するたびに、新しいkeytab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 では、 DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプは AES256 です。 ONTAP システムで有効な場合は AES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、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、 keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、 keytab 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

ワークグループでの**SMB**サーバのセットアップの概要

ワークグループ内のメンバーとして SMB サーバをセットアップするには、 SMB サーバを作成してから、ローカルユーザとローカルグループを作成します。

Microsoft Active Directory ドメインインフラを使用できない場合は、ワークグループに SMB サーバを設定できます。

ワークグループモードの SMB サーバでは NTLM 認証のみがサポートされ、 Kerberos 認証はサポートされません。

ワークグループに**SMB**サーバを作成する

コマンドを使用すると、SVM上にSMBサーバを作成し、所属先のワークグループを指定できます `vserver cifs create`。

開始する前に

データ処理に使用する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。

タスクの内容

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

- SMB3カンシフロトコル
- 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）

その他のオプションの設定パラメータと命名要件については、のマニュアルページを参照して `vserver cifs`ください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

   SMBライセンスはに含まれてい"ONTAP One"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. ワークグループ内に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" 内に SMB サーバ "'smb_server01" を作成します

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

3. コマンドを使用して、SMBサーバの設定を確認します `vserver cifs show`。

   次の例では、コマンド出力は、ワークグループ「 workgroup01 」内の SVM vs1.example.com 上に「

'smb_server01' 」という名前の SMB サーバが作成されたことを示しています。

```
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

ワークグループ内のCIFSサーバの場合は、SVM上にローカルユーザ、および必要に応じて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"

ローカルユーザアカウントの作成

SVMに格納されたデータへのSMB接続を介したアクセスの認証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。SMBセッションの作成時の認証にローカルユーザアカウントを使用することもできます。

タスクの内容

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`マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

手順

1. ローカルユーザを作成します。 `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の入力を求められます。

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「 `S MB_SERVER1\Sue` 」という完全な名前のローカルユーザ「 `S ue Chang-」 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
```

ローカルグループの作成

SVM に関連付けられたデータへの 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と機能を定義した権限を割り当てることもできます。

タスクの内容

ローカルグループの機能は、 SVM の作成時にデフォルトで有効になります。

ローカルグループを作成するときは、グループの名前を指定する必要があり、グループを関連付ける SVM を指定する必要があります。グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。また、オプションで、ローカルグループの概要を指定することもできます。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。

`vserver cifs users-and-groups local-group`マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

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`

   次のオプションの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。

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 に関連付けられるローカルグループ「 `s MB_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

新しいグループにメンバーを追加する必要があります。

ローカルグループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

タスクの内容

特定のグループのメンバーシップに基づいてローカルユーザ、ドメインユーザ、またはドメイングループに付与されたアクセス権や権限を取り消す場合に、メンバーをグループから削除できます。

メンバーをローカルグループに追加する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone 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。
- ローカルグループにドメインユーザまたはグループを追加するには、 ONTAP で名前を SID に解決できる必要があります。

メンバーをローカルグループから削除する場合は、次の点に注意する必要があります。

- 特殊なグループ _Everyone 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 で名前を SID に解決できる必要があります。

手順

1. メンバーをグループに追加するか、グループから削除します。
   - メンバーを追加します。 `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できます。
   - メンバーを削除します。 `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「 `s MB_SERVER01\engineering` 」にローカルユーザ「 ````s MB_SERVER01\engineering 」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「 `s MB_SERVER1\engineering` 」からローカルユーザ「 `s MB_SERVER01\Sue` 」および「 `S MB_SERVER01\engineering` 」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**SMB**のバージョンの確認

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のリリースに応じて決まります。ご使用の環境で必要なクライアントと機能がSMBサーバでサポートされていることを確認する必要があります。

タスクの内容

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場合は、可能なかぎりSMB 2.0以降を有効にしてください。セキュリティ上の理由から、SMB 1.0の使用は避け、ご使用の環境で不要であることが確認された場合は無効にしてください。

ONTAP 9では、SMBバージョン2.0以降がクライアント接続用にデフォルトで有効になりますが、デフォルトで有効になるSMB 1.0のバージョンはONTAPのリリースによって異なります。

- ONTAP 9 .1 P8以降では、SVMでSMB 1.0を無効にすることができます。

  コマンドのオプション `vserver cifs options modify`で、`SMB 1.0`を有効または無効にします `-smb1-enabled`。

- ONTAP 9 .3以降では、新しいSVMではデフォルトで無効になっています。

SMBサーバがActive Directory（AD）ドメイン内にある場合、ONTAP 9 .1以降では、SMB 2.0を有効にしてドメインコントローラ（DC）に接続できます。DCでSMB 1.0を無効にしている場合は、この処理が必要です。SMB.2以降では、ONTAP 9 2.0はDC接続に対してデフォルトで有効になっています。

> ⓘ がwhileに `-smb1-enabled`設定されて `false`いる場合 `-smb1-enabled-for-dc-connections true`、ONTAPはクライアントとしてのSMB 1.0の接続を拒否しますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

"SMBの管理"サポートされるSMBのバージョンと機能の詳細が表示されます。

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
```

有効な値 `smb_version`は次のとおりです。

- `-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には：

```
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には：

```
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サーバでのSMBサーバのマッピング

Windows ユーザがドライブを SMB サーバ名にマッピングできるように、サイトの DNS サーバに、 SMB サーバ名および NetBIOS エイリアスをデータ LIF の IP アドレスにマッピングしたエントリを設定する必要があります。

開始する前に

サイトの DNS サーバに対する管理アクセス権が必要です。管理アクセス権がない場合は、 DNS 管理者にこのタスクの実行を依頼する必要があります。

タスクの内容

SMB サーバ名に NetBIOS エイリアスを使用する場合は、各エイリアスに DNS サーバのエントリポイントを作成することを推奨します。

手順

1. DNSサーバにログインします。
2. フォワードルックアップ（ A - アドレスレコード）とリバースルックアップ（ PTR - ポインタレコード）のエントリを作成して、 SMB サーバ名をデータ 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）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータ LIF の IP アドレスにマッピングします。

結果

ネットワーク全体にマッピングが反映されると、 Windows ユーザがドライブを SMB サーバ名またはその NetBIOS エイリアスにマッピングできるようになります。

共有ストレージへの**SMB**クライアントアクセスの設定

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
                           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
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   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`-path`ます。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`値を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`、動的な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。

"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。

   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`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`ます。ディレクトリパスはで `/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	`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. 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::> 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、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::> 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	a. [追加]*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、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。