SMBサーバの管理

ONTAP 9

NetApp
February 12, 2026

目次

SMBサーバの管理

ONTAP SMBサーバーの変更

`vserver cifs modify`コマンドを使用して、SMBサーバをワークグループからActive Directoryドメイン、ワークグループから別のワークグループ、またはActive Directoryドメインからワークグループに移動できます。

タスク概要

SMBサーバーのその他の属性（SMBサーバー名や管理ステータスなど）を変更することもできます。"ONTAP コマンド リファレンス"の `vserver cifs modify`の詳細をご覧ください。

オプション

- SMB サーバーをワークグループから Active Directory ドメインに移動します：

  a. SMB サーバーの管理ステータスを `down`に設定します。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. SMB サーバーをワークグループから Active Directory ドメインに移動します： `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  SMB サーバーの Active Directory マシン アカウントを作成するには、 *`example`*.com ドメイン内の `ou=`*example* ou`コンテナーにコンピューターを追加するための十分な権限を持つ Windows アカウントの名前とパスワードを入力する必要があります。

  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。

- SMB サーバーをワークグループから別のワークグループに移動します：

  a. SMB サーバーの管理ステータスを `down`に設定します。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. SMB サーバーのワークグループを変更します： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- SMB サーバーを Active Directory ドメインからワークグループに移動します：
  a. SMB サーバーの管理ステータスを `down`に設定します。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. SMB サーバーを Active Directory ドメインからワークグループに移動します： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> ワークグループモードに入るには、継続的可用性共有、シャドウコピー、AESなど、すべてのドメインベースの機能を無効にし、その設定をシステムによって自動的に削除する必要があります。ただし、「EXAMPLE.COM\userName」などのドメイン設定された共有ACLは正常に動作しませんが、ONTAPでは削除できません。コマンド完了後、外部ツールを使用してできるだけ早くこれらの共有ACLを削除してください。AESが有効になっている場合は、「EXAMPLE.COM」ドメインでAESを無効にするための十分な権限を持つWindowsアカウントの名前とパスワードの入力を求められる場合があります。

  - `vserver cifs modify`コマンドの適切なパラメータを使用して、他の属性を変更します。

オプションを使用したSMBサーバのカスタマイズ

利用可能な **ONTAP SMB** サーバ オプション

SMBサーバーのカスタマイズ方法を検討する際には、利用可能なオプションを知っておくと便利です。一部のオプションはSMBサーバーで一般的に使用されますが、いくつかのオプションは特定のSMB機能を有効化および設定するために使用されます。SMBサーバーのオプションは、 `vserver cifs options modify`オプションで制御されます。

以下に、admin権限レベルで使用できるSMBサーバ オプションについて説明します。

- **SMB** セッションのタイムアウト値の設定

  このオプションでは、SMBセッションがアイドルになってから切断されるまでの時間を秒数で指定できます。アイドル セッションとは、ユーザがクライアントでファイルもディレクトリも開いていないセッションのことです。デフォルト値は900秒です。

- デフォルトの**UNIX**ユーザーの設定

  このオプションを設定すると、SMBサーバが使用するデフォルトのUNIXユーザを指定できます。ONTAPは、「`pcuser`」（UID 65534）というデフォルトユーザと、「`pcuser`」（GID 65534）というグループを自動的に作成し、そのデフォルトユーザを「`pcuser`」グループに追加します。SMBサーバを作成すると、ONTAPは「`pcuser`」をデフォルトのUNIXユーザとして自動的に設定します。

- ゲスト **UNIX** ユーザーの設定

このオプションでは、信頼されていないドメインからログインしたユーザをマッピングするUNIXユーザの名前を指定できます。これにより、信頼されていないドメインのユーザがSMBサーバに接続できるようになります。デフォルトでは、このオプションは設定されていません（デフォルト値はありません）。このため、信頼されていないドメインのユーザはSMBサーバへの接続を許可されません。

- モード ビットの読み取り許可実行の有効化または無効化

  このオプションを有効または無効にすると、UNIX実行可能ビットが設定されていない場合でも、UNIXモード ビットが設定された実行可能ファイルの実行を、ファイルへの読み取り権限を持つSMBクライアントに許可するかどうかを指定できます。このオプションはデフォルトで無効になっています。

- **NFS**クライアントから読み取り専用ファイルを削除する機能を有効または無効にする

  このオプションを有効または無効にすることで、NFSクライアントが読み取り専用属性が設定されているファイルまたはフォルダを削除できるかどうかを決定します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されているファイルまたはフォルダの削除は許可されません。UNIXの削除セマンティクスでは、読み取り専用ビットは無視され、代わりに親ディレクトリの権限を使用してファイルまたはフォルダの削除可否が判断されます。デフォルト設定は `disabled`で、NTFSの削除セマンティクスが適用されます。

- **Windows Internet Name Service** サーバー アドレスの設定

  このオプションでは、複数のWindows Internet Name Service（WINS）サーバ アドレスをカンマで区切って指定できます。IPv4アドレスを指定する必要があります。IPv6アドレスはサポートされません。デフォルト値はありません。

以下に、advanced権限レベルで使用できるSMBサーバ オプションについて説明します。

- **CIFS**ユーザーに**UNIX**グループ権限を付与する

  このオプションを設定すると、ファイルの所有者ではない受信 CIFS ユーザーにグループ権限を付与できるかどうかが決定されます。CIFS ユーザーが UNIX セキュリティ スタイルのファイルの所有者ではなく、このパラメータが `true`に設定されている場合、ファイルに対するグループ権限が付与されます。CIFS ユーザーが UNIX セキュリティ スタイルのファイルの所有者ではなく、このパラメータが `false`に設定されている場合、ファイル権限を付与するために通常の UNIX ルールが適用されます。このパラメータは、権限が `mode bits`に設定されている UNIX セキュリティ スタイルのファイルに適用され、NTFS または NFSv4 セキュリティ モードのファイルには適用されません。デフォルト設定は `false`です。

- **SMB 1.0** の有効化または無効化

  ONTAP 9.3でSMBサーバが作成されたSVMでは、SMB 1.0がデフォルトで無効になります。

  > ONTAP 9.3以降では、ONTAP 9.3で新しく作成されたSMBサーバについてはSMB 1.0がデフォルトで無効になります。できるだけ早く最新のSMBバージョンに移行して、セキュリティとコンプライアンスを強化してください。詳細については、NetAppの担当者にお問い合わせください。

- **SMB 2.x** の有効化または無効化

  SMB 2.0は、LIFフェイルオーバーをサポートするSMBの最小バージョンです。SMB 2.xを無効にした場合、SMB 3.Xも自動的に無効になります。

SMB 2.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- **SMB 3.0** の有効化または無効化

  SMB 3.0は、継続的可用性を備えた共有をサポートするSMBの最小バージョンです。Windows Server 2012およびWindows 8は、SMB 3.0をサポートするWindowsの最小バージョンです。

  SMB 3.0はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- **SMB 3.1** の有効化または無効化

  Windows 10は、SMB 3.1をサポートするWindowsの唯一のバージョンです。

  SMB 3.1はSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- **ODX copy offload**の有効化または無効化

  ODX コピー オフロードは、それをサポートする Windows クライアントによって自動的に使用されます。このオプションはデフォルトで有効になっています。

- **ODX copy offload**のダイレクト コピー メカニズムの有効化または無効化

  直接コピー メカニズムは、コピー中のファイル変更を禁止するモードでWindowsクライアントがコピー元のファイルを開こうとした場合に、コピー オフロード処理のパフォーマンスを向上させます。デフォルトでは、直接コピー メカニズムは有効になっています。

- 自動ノード リファーラルの有効化または無効化

  自動ノード リファーラルでは、SMBサーバはクライアントに対して、要求した共有を介してアクセスするデータのホスト ノードに対してローカルなデータLIFを自動的に参照することになります。

- **SMB** のエクスポート ポリシーの有効化または無効化

  このオプションはデフォルトで無効になっています。

- ジャンクション ポイントを再解析ポイントとして使用することを有効化または無効化

  このオプションを有効にすると、SMBサーバーはジャンクションポイントを再解析ポイントとしてSMBクライアントに公開します。このオプションはSMB 2.xまたはSMB 3.0接続でのみ有効です。このオプションはデフォルトで有効です。

  このオプションはSVMでのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- **TCP** 接続あたりの最大同時操作数の設定

  デフォルト値は255です。

- ローカル **Windows** ユーザーとグループの機能の有効化または無効化

  このオプションはデフォルトで有効になっています。

- ローカル **Windows** ユーザー認証の有効化または無効化

このオプションはデフォルトで有効になっています。

- **VSS shadow copy**機能の有効化または無効化

  ONTAPでは、シャドウ コピー機能によって、Hyper-V over SMBソリューションを使用して格納されたデータのリモート バックアップを実行します。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- **shadow copy** ディレクトリの深さの設定

  このオプションを設定すると、シャドウ コピー機能を使用するときに、シャドウ コピーを作成するディレクトリの最大階層を定義できます。

  このオプションは、SVM、およびHyper-V over SMB構成でのみサポートされます。このオプションは、SVMではデフォルトで有効になります。

- 名前マッピングのマルチドメイン検索機能の有効化または無効化

  有効にすると、Windowsユーザ名のドメイン部分にワイルドカード（）を使用して**UNIX**ユーザが**Windows**ドメインユーザにマッピングされた場合（例：\joe）、ONTAPはホームドメインとの双方向の信頼関係を持つすべてのドメインで指定されたユーザを検索します。ホームドメインとは、SMBサーバのコンピュータアカウントが含まれるドメインです。

  双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして、信頼できるドメインのリストを設定すると、マルチドメイン ネーム マッピングの検索はそのリストを使用して実行されます。

  デフォルトでは、マルチドメイン ネーム マッピングの検索は有効になります。

- ファイル システムのセクター サイズの設定

  このオプションを設定すると、ONTAPがSMBクライアントに報告するファイルシステムのセクターサイズ（バイト単位）を設定できます。このオプションには、 `4096`と `512`の2つの有効な値があります。デフォルト値は `4096`です。Windowsアプリケーションが512バイトのセクターサイズしかサポートしていない場合は、この値を `512`に設定する必要があるかもしれません。

- **Dynamic Access Control** の有効化または無効化

  このオプションを有効にすると、監査を使用した集約型アクセス ポリシーのステージングや、グループ ポリシー オブジェクトを使用した集約型アクセス ポリシーの実装を含めて、ダイナミック アクセス制御を使用してSMBサーバのオブジェクトを保護できます。このオプションはデフォルトでは無効になっています。

  このオプションはSVMでのみサポートされます。

- 認証されていないセッションのアクセス制限の設定（匿名を制限）

  このオプションでは、認証されていないセッションに適用されるアクセス制限を指定します。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- **UNIX** 有効セキュリティのボリューム（**UNIX** セキュリティ形式のボリュームまたは **UNIX** 有効セキュリテ

ィの混合セキュリティ形式のボリューム）での **NTFS ACL** の表示の有効化または無効化

このオプションを有効または無効にして、UNIXセキュリティ形式のファイルやフォルダのファイル セキュリティがSMBクライアントに表示される方法を指定します。有効にすると、UNIXセキュリティ形式のボリューム内のファイルやフォルダは、NTFS ACLを使用するNTFSファイル セキュリティが設定されたファイルやフォルダとしてSMBクライアントに表示されます。無効にすると、UNIXセキュリティ形式のボリュームは、ファイル セキュリティのないFATボリュームとして表示されます。デフォルトでは、ボリュームはNTFS ACLを使用するNTFSファイル セキュリティが設定されたボリュームとして表示されます。

- **SMB** フェイク オープン機能の有効化または無効化

  この機能を有効にすると、ONTAPがファイルやディレクトリの属性情報を照会する際のオープン要求とクローズ要求の方法が最適化されて、SMB 2.xおよびSMB 3.0のパフォーマンスが向上します。デフォルトでは、SMB擬似オープン機能は有効になっています。このオプションは、SMB 2.x以降を使用する接続にのみ有効です。

- **UNIX** 拡張機能の有効化または無効化

  このオプションを有効にすると、SMBサーバでUNIX拡張が有効になります。UNIX拡張を使用すると、SMBプロトコルを介してPOSIX/UNIX形式のセキュリティを表示できます。デフォルトでは、このオプションは無効になっています。

  Mac OS Xクライアントなど、UNIXベースのSMBクライアントが環境内にある場合は、UNIX拡張を有効にしてください。UNIX拡張を有効にすると、SMBサーバはPOSIX/UNIXセキュリティ情報をSMB経由でUNIXベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報をPOSIX/UNIXセキュリティに変換します。

- 短縮名検索のサポートを有効または無効にする

  このオプションを有効にすると、SMBサーバーは短いファイル名で検索を実行できるようになります。このオプションを有効にした検索クエリは、長いファイル名だけでなく、8.3形式のファイル名も照合します。このパラメータのデフォルト値は `false`です。

- **DFS** 機能の自動アドバタイズのサポートを有効または無効にする

  このオプションを有効または無効にして、共有に接続するSMB 2.xおよびSMB 3.0クライアントにSMBサーバからDFS対応を自動的に通知するかどうかを指定します。ONTAPでは、SMBアクセス用のシンボリック リンクの実装でDFSリファーラルが使用されます。有効にすると、シンボリック リンク アクセスが有効かどうかに関係なく、SMBサーバは常にDFS対応を通知します。無効にすると、シンボリック リンク アクセスが有効になっている共有にクライアントが接続する場合にのみ、SMBサーバはDFS対応を通知します。

- **SMB** クレジットの最大数の設定

  ONTAP 9.4以降では、 `-max-credits`オプションを設定することで、クライアントとサーバがSMBバージョン2以降を実行している場合に、SMB接続で付与されるクレジットの数を制限できます。デフォルト値は128です。

- **SMB** マルチチャネルのサポートの有効化または無効化

  ONTAP 9.4以降のリリースで `-is-multichannel-enabled`オプションを有効にすると、クラスタとそのクライアントに適切なNICが導入されている場合、SMBサーバは単一のSMBセッションに対して複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。このパラメータのデフ

ォルト値は `false`です。

SMBマルチチャネルが有効な場合、次のパラメータも指定できます。

- 各マルチチャネル セッションに許可される最大接続数。このパラメータのデフォルト値は32です。
- マルチチャネル セッションごとにアドバタイズされるネットワーク インターフェイスの最大数。このパラメータのデフォルト値は 256 です。

ONTAP SMBサーバ オプションを設定する

SMBサーバ オプションは、Storage Virtual Machine（SVM）でのSMBサーバの作成後に随時設定できます。

手順

1. 次のうち必要な操作を実行します。

SMB サーバ オプションを設定する場合...	コマンドを入力してください...
admin権限レベルで設定	`vserver cifs options modify -vserver` *`vserver_name options`*
advanced権限レベルで設定	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

`vserver cifs options modify`および SMB サーバー
オプションの設定の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-options-modify.html["ONTAPコマンド リファレンス
"^]を参照してください。

ONTAP SMBユーザーにUNIXグループ権限を付与する設定

このオプションを使用して、ファイルの所有者でないSMBユーザもファイルやディレクトリにアクセスできるグループ権限を付与することができます。

手順

1. 権限レベルをadvancedに設定します： `set -privilege advanced`
2. UNIXグループ権限付与を目的に応じて設定します。

次の操作を行う場合：	入力するコマンド
ユーザがファイルの所有者でない場合にもファイルやディレクトリにアクセスするためのグループ権限を付与する	`vserver cifs options modify -grant-unix-group-perms-to-others true`
ユーザがファイルの所有者でない場合はファイルやディレクトリにアクセスするためのグループ権限を付与しない	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. オプションが目的の値に設定されていることを確認します： `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. admin権限レベルに戻ります： `set -privilege admin`

匿名ユーザーに対する **ONTAP SMB** アクセス制限を構成する

デフォルトでは、認証されていない匿名ユーザー（_nullユーザー_とも呼ばれます）はネットワーク上の特定の情報にアクセスできます。SMBサーバーオプションを使用して、匿名ユーザーへのアクセス制限を設定できます。

タスク概要

> `-restrict-anonymous`SMB サーバー オプションは、Windows の `RestrictAnonymous`レジストリ エントリに対応します。

匿名ユーザは、ネットワークのWindowsホストから、ユーザ名、ユーザの詳細、アカウント ポリシー、共有名など、特定の種類のシステム情報をリストまたは列挙できます。次の3つのうち、いずれかのアクセス制限設定を指定して、匿名ユーザのアクセスを制御することができます。

Value	概要
`no-restriction`（デフォルト）	匿名ユーザに対してアクセス制限を設定しません。
`no-enumeration`	匿名ユーザに対して列挙だけを制限します。
`no-access`	匿名ユーザに対してアクセスを制限します。

手順

1. 権限レベルをadvancedに設定します： `set -privilege advanced`
2. 匿名制限設定を構成します： `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. オプションが目的の値に設定されていることを確認します： `vserver cifs options show -vserver` *`vserver_name`*
4. admin権限レベルに戻ります： `set -privilege admin`

関連情報

利用可能なサーバー オプション

UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法の管理

UNIXセキュリティ形式のデータに対して、SMBクライアントにONTAPファイルセキュリティを提供する方法について説明します。

SMBクライアントへのNTFS ACLの提供を有効または無効にすることによって、UNIXセキュリティ形式のデータに対するファイル セキュリティのSMBクライアントへの提供方法を選択できます。それぞれの設定の利点を理解して、ビジネス要件に適した方を選ぶようにしてください。

デフォルトでは、UNIXセキュリティ形式のボリュームに対するUNIXアクセス権がNTFS ACLとしてSMBクライアントに提供されます。これは次のような場合に適しています。

- Windows のプロパティ ボックスの セキュリティ タブを使用して、UNIX 権限を表示および編集します。

  処理がUNIXシステムで許可されていなければ、Windowsクライアントからアクセス権を変更することはできません。たとえば、所有していないファイルの所有権を変更することはできません。これは、UNIXシステムではこうした処理が許可されていないためです。この制限により、SMBクライアントは、ファイルやフォルダに対して設定されたUNIXアクセス権をバイパスできないようになっています。

- UNIXセキュリティ形式のボリュームに格納されたファイルの編集や保存に特定のWindowsアプリケーション（Microsoft Officeなど）を使用しており、ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 使用するファイルのNTFS ACLを読み取ることを想定した特定のWindowsアプリケーションが環境にある場合。

状況に応じて、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることもできます。この機能を無効にすると、UNIXセキュリティ形式のボリュームがFATボリュームとしてSMBクライアントに提供されます。UNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供するのは、次のような場合です。

- UNIXアクセス権の変更は、マウントを使用してUNIXクライアントでしか行わない場合。

  UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合、[セキュリティ]タブで操作することはできません。マッピングされたドライブは、ファイル権限がない、FATファイルシステムでフォーマットされたドライブとして表示されます。

- SMBを使用するアプリケーションでアクセスするファイルやフォルダにNTFS ACLを設定しており、データがUNIXセキュリティ形式のボリュームにあると失敗する可能性がある場合。

  ONTAPではボリュームがFATとして報告され、アプリケーションでACLの変更は試行されません。

関連情報

- FlexVolでのセキュリティ形式の設定
- qtreeでのセキュリティ形式の設定

UNIXセキュリティ形式のデータ用に**ONTAP SMB**クライアントへの**NTFS ACL**のプレゼンテーションを設定する

UNIXセキュリティ形式のデータ（UNIXセキュリティ形式のボリュームおよびUNIX有効セキュリティを使用する混在セキュリティ形式のボリューム）に対して、SMBクライアントへのNTFS ACLの表示を有効または無効にできます。

タスク概要

このオプションを有効にすると、ONTAPは、有効なUNIXセキュリティ形式のボリューム上のファイルとフォルダを、NTFS ACLを持つものとしてSMBクライアントに提示します。このオプションを無効にすると、ボリュームはSMBクライアントに対してFATボリュームとして提示されます。デフォルトでは、SMBクライアントに対してNTFS ACLが提示されます。

手順

1. 権限レベルをadvancedに設定します： `set -privilege advanced`
2. UNIX NTFS ACLオプション設定を構成します。 `vserver cifs options modify -vserver *vserver_name* -is-unix-nt-acl-enabled {true|false}`
3. オプションが目的の値に設定されていることを確認します： `vserver cifs options show -vserver *vserver_name*`
4. admin権限レベルに戻ります： `set -privilege admin`

ONTAP SMB FlexVolボリュームの**UNIX**権限の保持について学習します

現在 UNIX 権限を持つFlexVolボリューム内のファイルが Windows アプリケーションによって編集および保存されると、ONTAP は UNIX 権限を保持できます。

Windows クライアント上のアプリケーションがファイルを編集して保存する場合、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用して、一時ファイルに元のファイル名を付けます。

Windowsクライアントがセキュリティプロパティのクエリを実行すると、UNIX権限を正確に表す構築済みACLが返されます。この構築済みACLの唯一の目的は、Windowsアプリケーションによってファイルが更新されてもファイルのUNIX権限を保持し、更新後のファイルに同じUNIX権限が付与されるようにすることです。ONTAPは、構築済みACLを使用してNTFS ACLを設定することはありません。

ONTAP SMBサーバの**Windows**セキュリティタブを使用して**UNIX**権限を管理する方法について学習します。

SVM上の混合セキュリティ形式のボリュームまたはqtree内のファイルまたはフォルダのUNIX権限を操作する場合は、Windowsクライアントの[セキュリティ]タブを使用できます。または、Windows ACLを照会および設定できるアプリケーションを使用することもできます。

- UNIX権限の変更

  Windowsの「セキュリティ」タブを使用して、混合セキュリティ形式のボリュームまたはqtreeのUNIX権限を表示および変更できます。Windowsのメインの「セキュリティ」タブを使用してUNIX権限を変更する場合は、変更を加える前に、編集する既存のACEを削除する必要があります（これにより、モードビットが0に設定されます）。または、詳細エディタを使用して権限を変更することもできます。

モード権限を使用する場合、リストされているUID、GID、その他（コンピューターにアカウントを持つ他のすべてのユーザー）のモード権限を直接変更できます。例えば、表示されているUIDにr-x権限がある場合、UID権限をrwxに変更できます。

- UNIX 権限から NTFS 権限への変更

  Windows セキュリティ タブを使用すると、ファイルとフォルダに UNIX 対応のセキュリティ スタイルが設定されている、混合セキュリティ スタイルのボリュームまたは qtree 上で、UNIX セキュリティ オブジェクトを Windows セキュリティ オブジェクトに置き換えることができます。

  必要なWindowsユーザおよびグループオブジェクトに置き換える前に、まずリストされているすべてのUNIX権限エントリを削除する必要があります。その後、WindowsユーザおよびグループオブジェクトにNTFSベースのACLを設定できます。すべてのUNIXセキュリティオブジェクトを削除し、混合セキュリティ形式のボリュームまたはqtreeのファイルまたはフォルダにWindowsユーザおよびグループのみを追加することで、ファイルまたはフォルダの有効なセキュリティ形式がUNIXからNTFSに変更されます。

  フォルダの権限を変更すると、Windowsのデフォルトの動作では、これらの変更がすべてのサブフォルダとファイルに反映されます。したがって、セキュリティスタイルの変更をすべての子フォルダ、サブフォルダ、およびファイルに反映させたくない場合は、反映方法を適切な設定に変更する必要があります。

SMBサーバのセキュリティ設定の管理

ONTAP SMBクライアント認証の処理について学ぶ

SMB接続を確立してSVMに格納されているデータにアクセスする前に、ユーザはSMBサーバが属しているドメインで認証される必要があります。SMBサーバでは、KerberosとNTLM（NTLMv1またはNTLMv2）の2つの認証方法がサポートされます。ドメイン ユーザの認証に使用されるデフォルトの方法はKerberosです。

Kerberos認証

ONTAPは、許可されたSMBセッションの作成時にKerberos認証をサポートします。

KerberosはActive Directoryのプライマリ認証サービスです。KerberosサーバのKerberos Key Distribution Center（KDC;キー配布センター）サービスは、Active Directoryに対してセキュリティ プリンシパルに関する情報の格納や取得を行います。NTLMモデルと異なる点は、Active Directoryクライアントが SMBサーバなどの別のコンピュータとのセッションの確立を求める場合、直接KDCにアクセスしてそのセッションのクレデンシャルを取得するところです。

NTLM認証

NTLMクライアント認証は、パスワードをベースとするユーザ固有のシークレットを共有し、チャレンジ-応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザ アカウントを使用してSMB接続を確立した場合、認証は、SMBサーバによってNTLMv2を使用してローカルで行われます。

ONTAP SVM ディザスタ リカバリ構成の SMB サーバ セキュリティ設定について学習します

IDが保持されない（SnapMirror構成で `-identity-preserve`オプションが `false`に設定されている）ディザスタリカバリデスティネーションとして設定されたSVMを作成する前に、デスティネーションSVMでSMBサーバセキュリティ設定がどのように管理されるかを知っておく必要があります。

- デフォルト以外の SMB サーバー セキュリティ設定は宛先に複製されません。

  デスティネーションSVMにSMBサーバを作成すると、すべてのSMBサーバセキュリティ設定がデフォルト値に設定されます。SVMディザスタリカバリデスティネーションが初期化、更新、または再同期されても、ソースのSMBサーバセキュリティ設定はデスティネーションにレプリケートされません。

- デフォルト以外の SMB サーバー セキュリティ設定を手動で構成する必要があります。

  ソース SVM でデフォルト以外の SMB サーバ セキュリティ設定が設定されている場合は、デスティネーションが読み取り/書き込み可能になった後（SnapMirror 関係が解除された後）、デスティネーション SVM で同じ設定を手動で設定する必要があります。

ONTAP SMB サーバのセキュリティ設定に関する情報を表示します

Storage Virtual Machine（SVM）上のSMBサーバのセキュリティ設定に関する情報を表示できます。この情報は、セキュリティ設定が適切かどうかを確認するときに役立ちます。

タスク概要

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値か、ONTAP CLIまたはActive Directoryグループ ポリシー オブジェクト（GPO）を使用して設定されたデフォルト以外の値です。

ワークグループ モードの SMB サーバーでは `vserver cifs security show`コマンドを使用しないでください。一部のオプションが無効です。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合	コマンドを入力してください...
指定したSVMのすべてのセキュリティ設定	`vserver cifs security show -vserver` *`vserver_name`*
SVMの特定のセキュリティ設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]`使用できるフィールドを確認するには、 `-fields ?`と入力します。

例

次の例は、SVM vs1のすべてのセキュリティ設定を表示します。

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                           Kerberos Clock Skew:        5 minutes
                           Kerberos Ticket Age:        10 hours
                          Kerberos Renewal Age:        7 days
                          Kerberos KDC Timeout:        3 seconds
                           Is Signing Required:        false
                Is Password Complexity Required:        true
           Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:        false
                         LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:        false
                        Client Session Security:        none
                SMB1 Enabled for DC Connections:        false
                SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
               Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

表示される設定は、実行中のONTAPバージョンによって異なります。

次の例は、SVM vs1のKerberosのクロック スキューを表示します。

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

関連情報

GPO設定に関する情報の表示

ローカル**SMB**ユーザの**ONTAP**パスワードの複雑さを設定する

パスワードの複雑さの要件を有効にすると、Storage Virtual Machine（SVM）上のローカルSMBユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この要件の有効と無効はいつでも切り替えることができます。

開始する前に

CIFSサーバでローカル ユーザ、ローカル グループ、およびローカル ユーザ認証が有効になっている必要があります。

タスク概要

ワークグループ モードの CIFS サーバーでは `vserver cifs security modify`コマンドを使用しないでください。一部のオプションが無効です。

手順

1. 次のいずれかを実行します。

ローカル**SMB**ユーザに対するパスワードの複雑さの要件の設定	コマンドを入力してください...
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. 必要なパスワードの複雑さのセキュリティ設定を確認します `vserver cifs security show -vserver` *`vserver_name`*

例

次の例は、SVM vs1のローカルSMBユーザに対してパスワードの複雑さの要件を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

関連情報

- サーバーのセキュリティ設定に関する情報を表示する
- ローカル ユーザとグループについて
- ローカル ユーザのパスワードの要件
- ローカル ユーザのアカウント パスワードの変更

ONTAP SMBサーバのKerberosセキュリティ設定を変更する

CIFSサーバのKerberosセキュリティ設定の一部を変更できます。対象となる設定には、Kerberosクロック スキューの許容最大時間やKerberosチケットの有効期間、チケットを更新できる最長有効期間（日数）などがあります。

タスク概要

`vserver cifs security modify`コマンドを使用してCIFSサーバのKerberos設定を変更すると、 `-vserver`パラメータで指定した単一のストレージ仮想マシン（SVM）の設定のみが変更されます。Active Directoryグループポリシーオブジェクト（GPO）を使用すると、同じActive Directoryドメインに属するクラスタ内のすべてのSVMのKerberosセキュリティ設定を一元管理できます。

手順

1. 次の操作を1つ以上実行します。

状況	入力する内容
Kerberosクロック スキューの許容最大時間を分（9.13.1以降）または秒（9.12.1以前）で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* デフォルトの設定は5分です。
Kerberosチケットの有効期間を時間で指定する。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` デフォルトの設定は10時間です。
チケットを更新できる最長有効期間を日数で指定する。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* デフォルトの設定は7日です。
KDCのソケットのタイムアウトを指定する（この時間を過ぎるとすべてのKDCが到達不能とマークされます）。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* デフォルトの設定は3秒です。

2. Kerberosセキュリティ設定を確認します。

   `vserver cifs security show -vserver` *`vserver_name`*

例

次の例では、Kerberosセキュリティに次の変更を加えます。SVM vs1の「Kerberos Clock Skew」は3分に設定され、「Kerberos Ticket Age」は8時間に設定されています（：）

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                     Kerberos Clock Skew:                    3 minutes
                     Kerberos Ticket Age:                    8 hours
                    Kerberos Renewal Age:                    7 days
                    Kerberos KDC Timeout:                    3 seconds
                     Is Signing Required:                 false
          Is Password Complexity Required:                  true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

関連情報

"サーバーのセキュリティ設定に関する情報を表示する"

"サポートされるGPO"

"CIFSサーバへのグループ ポリシー オブジェクトの適用"

ONTAP SMBサーバの最小認証セキュリティレベルを設定する

SMBサーバーの最小セキュリティレベル（_LMCompatibilityLevel_とも呼ばれます）を設定することで、SMBクライアントアクセスに関するビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルとは、SMBサーバーがSMBクライアントから受け入れるセキュリティトークンの最小レベルです。

タスク概要

- 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ます。Kerberos認証はサポートされません。
- LMCompatibilityLevelはSMBクライアント認証にのみ適用され、管理者認証には適用されません。

最低限の認証セキュリティ レベルは、サポートされている4つのセキュリティ レベルのうちの1つに設定することができます。

Value	概要
`lm-ntlm-ntlmv2-krb`（デフォルト）	Storage Virtual Machine（SVM）は、LM、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。
`ntlm-ntlmv2-krb`	SVMは、NTLM、NTLMv2、Kerberos認証セキュリティを許可します。SVMはLM認証を拒否します。
`ntlmv2-krb`	SVMは、NTLMv2とKerberos認証セキュリティを許可します。SVMはLMとNTLM認証を拒否します。
`krb`	SVMは、Kerberos認証セキュリティのみを許可します。SVMはLM、NTLM、NTLMv2認証を拒否します。

手順

1. 最小認証セキュリティ レベルを設定します：`vserver cifs security modify -vserver *vserver_name* -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 認証セキュリティ レベルが希望のレベルに設定されていることを確認します：`vserver cifs security show -vserver *vserver_name*`

関連情報

Kerberosベースの通信用にAES暗号化を設定する

AES暗号化を使用したKerberosベースの通信用の強力なONTAP SMBセキュリティを構成する

Kerberosベースの通信による最も強固なセキュリティを実現するために、AES-256暗号化とAES-128暗号化をSMBサーバで有効にすることができます。デフォルトでは、SVMでのSMBサーバの作成時にAdvanced Encryption Standard（AES）暗号化は無効になっています。AES暗号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

SMBのKerberos関連の通信は、SVMでSMBサーバを作成する際や、SMBセッションの設定フェーズで使用されます。SMBサーバはKerberos通信で次の暗号化タイプをサポートしています。

- AES 256
- AES 128
- DES
- RC4-HMAC

Kerberos通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、SVMのKerberos通信でAES暗号化を有効にする必要があります。

SMBサーバを作成すると、ドメイン コントローラによってActive Directoryにコンピュータ マシン アカウント

が作成されます。この時点で、KDCは特定のマシン アカウントの暗号化機能を認識するようになっています。これ以降は、認証の際にクライアントがサーバに提示するサービス チケットを暗号化するために特定の暗号化タイプが選択されます。

ONTAP 9.12.1以降では、Active Directory（AD）KDCにアドバタイズする暗号化タイプを指定できるようになりました。 `-advertised-enc-types`オプションを使用して、推奨される暗号化タイプを有効にしたり、より弱い暗号化タイプを無効にしたりできます。"Kerberosベースの通信用にAES暗号化を設定する"方法をご確認ください。

SMB 3.0で利用可能なIntel AES New Instructions（Intel AES NI）はAESアルゴリズムの改良版で、サポート対象のプロセッサ ファミリーでのデータ暗号化処理を高速化します。SMB 3.1.1以降では、SMB暗号化で使用されるハッシュ アルゴリズムとして、AES-128-CCMに代わってAES-128-GCMが使用されます。

関連情報

サーバーのセキュリティ設定を変更する

ONTAP SMB KerberosベースのAES暗号化を設定する

Kerberosベースの通信で最大限のセキュリティを確保するには、SMBサーバでAES-256およびAES-128暗号化を使用する必要があります。ONTAP 9.13.1以降では、AES暗号化がデフォルトで有効になります。SMBサーバでActive Directory（AD）KDCとのKerberosベースの通信にAES暗号化タイプを選択したくない場合は、AES暗号化を無効にすることができます。

AES暗号化がデフォルトで有効になっているかどうかと、暗号化タイプを指定できるかどうかは、ONTAPのバージョンによって異なります。

ONTAPのバージョン	AES暗号化を有効にする方法	暗号化タイプ指定の可否
9.13.1以降	デフォルト	はい
9.12.1	手動	はい
9.11.1以前	手動	いいえ

ONTAP 9.12.1以降では、 `-advertised-enc-types`オプションを使用してAES暗号化を有効化または無効化できます。このオプションでは、AD KDCにアドバタイズされる暗号化タイプを指定できます。デフォルト設定は`rc4`と `des`ですが、AESタイプを指定するとAES暗号化が有効になります。また、オプションを使用して、より弱いRC4およびDES暗号化タイプを明示的に無効にすることもできます。ONTAP 9.11.1以前では、 `-is-aes-encryption-enabled`オプションを使用してAES暗号化を有効化または無効化する必要があり、暗号化タイプを指定することはできません。

セキュリティを強化するため、Storage Virtual Machine（SVM）はAESセキュリティ オプションが変更されるたびに、AD内のマシン アカウントのパスワードを変更します。パスワードの変更には、マシン アカウントが所属する組織単位（OU）の管理ADクレデンシャルが必要になることがあります。

SVMが、IDが保持されないディザスタリカバリ先として設定されている場合（SnapMirror設定で `-identity-preserve`オプションが `false`に設定されている場合）、デフォルト以外のSMBサーバセキュリティ設定はレプリケート先に複製されません。ソースSVMでAES暗号化を有効にしている場合は、手動で有効にする必要があります。

例 **1.** 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

Kerberos 通信に **AES** 暗号化タイプを使用する場合...	コマンドを入力してください...
有効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
無効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

注： `-is-aes-encryption-enabled`オプションはONTAP 9.12.1では廃止予定であり、今後のリリースで削除される可能性があります。

2. AES暗号化が必要に応じて有効または無効になっていることを確認します： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMBサーバが所属するOUの管理ADクレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信に **AES** 暗号化タイプを使用する場合...	コマンドを入力してください...
有効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
無効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. AES 暗号化が必要に応じて有効または無効になっていることを確認します： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

> `is-aes-encryption-enabled`フィールドには、AES 暗号化が有効になっている場合は `true`、無効になっている場合は `false`が表示されます。

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMBサーバが所属するOUの管理ADクレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

関連情報

"ドメイン ユーザーが Domain-Tunnel を使用してクラスタにログインできない"

SMB署名を使用したネットワーク セキュリティの強化

ONTAP SMB署名を使用してネットワーク セキュリティを強化する方法について学習します

SMB署名は、リプレイ攻撃を防ぐことで、SMBサーバとクライアント間のネットワークトラフィックの侵害を防止します。デフォルトでは、ONTAPはクライアントからの要求に応じてSMB署名をサポートします。オプションで、ストレージ管理者はSMBサーバでSMB署名を必須にするように設定できます。

署名ポリシーが**ONTAP SMB**サーバとの通信にどのように影響するかを学びます

CIFSサーバーのSMB署名セキュリティ設定に加えて、Windowsクライアント上の2つのSMB署名ポリシーが、クライアントとCIFSサーバー間の通信のデジタル署名を制御します。ビジネス要件に合った設定を構成できます。

クライアント SMB ポリシーは、Windows のローカル セキュリティ ポリシー設定によって制御されます。これらの設定は、Microsoft Management Console（MMC）または Active Directory GPO を使用して構成されます。クライアント SMB 署名とセキュリティの問題の詳細については、Microsoft Windows のドキュメントを参照してください。

Microsoft クライアント上の 2 つの SMB 署名ポリシーについて説明します：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  この設定は、クライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。クライアントでこの設定が無効になっている場合、CIFSサーバとのクライアント通信は、CIFSサーバのSMB署名設定に依存します。

- `Microsoft network client: Digitally sign communications (always)`

  この設定は、クライアントがサーバーとの通信にSMB署名を必要とするかどうかを制御します。デフォルトでは無効になっています。クライアントでこの設定が無効になっている場合、SMB署名の動作は `Microsoft network client: Digitally sign communications (if server agrees)`のポリシー設定とCIFSサーバーの設定に基づいて行われます。

> ⓘ 環境にSMB署名を必要とするように設定されたWindowsクライアントが含まれている場合は、CIFSサーバーでSMB署名を有効にする必要があります。有効にしないと、CIFSサーバーはこれらのシステムにデータを提供できません。

クライアントとCIFSサーバの実質的なSMB署名設定は、SMBセッションでSMB 1.0が使用されるかSMB 2.x以降が使用されるかによって異なります。

次の表に、セッションでSMB 1.0が使用される場合のSMB署名の動作を示します。

クライアント	**ONTAP—**署名は不要	**ONTAP—**署名が必要です
署名は無効になっており、必要ありません	署名なし	署名される
署名が有効で必須ではありません	署名なし	署名される
署名が無効になっていますが必須です	署名される	署名される
署名が有効で必須	署名される	署名される

古いバージョンのWindowsのSMB 1クライアントや一部のWindows以外のSMB 1クライアントでは、クライアントでは署名が無効になっていてCIFSサーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションでSMB 2.xまたはSMB 3.0が使用される場合のSMB署名の動作を示します。

SMB 2.x および SMB 3.0 クライアントでは、SMB 署名は常に有効です。無効にすることはできません。

クライアント	**ONTAP—**署名は不要	**ONTAP—**署名が必要です
署名は不要です	署名なし	署名される
署名が必要です	署名される	署名される

次の表は、Microsoft クライアントおよびサーバーの SMB 署名のデフォルトの動作をまとめたものです：

プロトコル	ハッシュアルゴリズム	有効化/無効化できます	必須にできる/必須にしないことができる	クライアントのデフォルト	サーバーのデフォルト	**DC**デフォルト
SMB 1.0	MD5	はい	はい	有効（必須ではありません）	無効（必須ではありません）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい	不要	不要	必須
SMB 3.0	AES-CMAC。	いいえ	はい	不要	不要	必須

Microsoftは、 `Digitally sign communications (if client agrees)`または `Digitally sign communications (if server agrees)`グループポリシー設定の使用を推奨しなくなりました。Microsoftは、 `EnableSecuritySignature`レジストリ設定の使用も推奨しなくなりました。これらのオプションはSMB 1の動作にのみ影響し、 `Digitally sign communications (always)`グループポリシー設定または `RequireSecuritySignature`レジストリ設定で置き換えることができます。Microsoftブログからも詳細情報を入手できます。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[SMB署名の基礎（SMB1とSMB2の両方をカバー）]

ONTAP SMB署名のパフォーマンスへの影響について学ぶ

SMBセッションでSMB署名を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行中のクラスタ ノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワーク トラフィックの量に変化がないにもかかわらずクライアントとサーバ両方のCPU使用率が増加する形で表れます。

その程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9.7以降では、新しい暗号化オフロード アルゴリズムによって署名済みSMBトラフィックのパフォーマンスを向上させることができます。SMB署名オフロードは、SMB署名が有効になっている場合はデフォルトで有効になります。

SMB署名のパフォーマンス向上には、AES-NIオフロード機能が必要です。ご使用のプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

SMBバージョン3.11を使用できる場合は、より高速なGCMアルゴリズムがサポートされるため、さらなるパフォーマンスの向上が可能です。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB署名のパフォーマンスへの影響は大幅に変わってくるため、検証するためには使用しているネットワーク環境でテストを実施する必要があります。

ほとんどのWindowsクライアントは、サーバでSMB署名が有効になっている場合は、SMB署名をデフォルトでネゴシエートします。Windowsクライアントの一部でSMB保護が必要で、SMB署名がパフォーマンスの問題を引き起こしている場合は、リプレイ アタックからの保護を必要としないWindowsクライアントに対してSMB署名を無効にすることができます。WindowsクライアントでのSMB署名の無効化については、Microsoft Windowsのマニュアルを参照してください。

ONTAP SMB署名設定の推奨事項

SMBクライアントとCIFSサーバの間のSMB署名の動作は、セキュリティ要件に応じて設定することができます。CIFSサーバでのSMB署名の設定は、セキュリティ要件の内容によって異なります。

SMB署名は、クライアントとCIFSサーバのどちらでも設定できます。SMB署名を設定する際の推奨事項を次に示します。

状況	推奨事項...
クライアントとサーバの間の通信のセキュリティを強化する	クライアントで `Require Option (Sign always)`セキュリティ設定を有効にして、SMB 署名を必須にします。
特定のStorage Virtual Machine（SVM）へのすべてのSMBトラフィックに署名する	セキュリティ設定でSMB署名を必須にするように設定して、CIFSサーバでSMB署名を必須にします。

Windowsクライアントのセキュリティ設定の詳細については、Microsoftのドキュメントを参照してください。

複数のデータ**LIF**に対する**ONTAP SMB**署名設定について学習します

SMB サーバーで必要な SMB 署名を有効または無効にする場合は、SVM の複数のデータ LIF 構成に関するガイドラインに注意する必要があります。

SMBサーバを設定する場合、複数のデータLIFが設定されている場合があります。その場合、DNSサーバには、CIFSサーバの `A`レコード エントリが複数含まれます。これらのレコード エントリはすべて同じSMBサーバ ホスト名を使用していますが、IPアドレスはそれぞれ異なります。たとえば、2つのデータLIFが設定されているSMBサーバの場合、DNS `A`レコード エントリは次のようになります：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、必要なSMB署名設定を変更すると、クライアントからの新規接続のみがSMB署名設定の変更の影響を受けます。ただし、この動作には例外があります。クライアントが既に共有に接続しており、設定変更後に元の接続を維持しながら、同じ共有への新規接続を作成する場合があります。この場合、新規接続と既存のSMB接続の両方に新しいSMB署名要件が適用されます。

次の例を考えてみましょう。

1. Client1 は、パス `O:\`を使用して、必要な SMB 署名なしで共有に接続します。
2. ストレージ管理者は、SMB 署名を要求するように SMB サーバー構成を変更します。
3. Client1 は、パス `S:\`を使用して必要な SMB 署名で同じ共有に接続します（パス `O:\`を使用した接続を維持しながら）。
4. その結果、 `O:\`ドライブと `S:\`ドライブの両方を介してデータにアクセスするときに SMB 署名が使用されます。

受信**SMB**トラフィック用の**ONTAP**署名を設定する

SMBメッセージへのクライアントによる署名を強制するには、SMB署名要求を有効にします。有効にすると、ONTAPは有効な署名のあるSMBメッセージのみを受け入れます。SMB署名を許可するが要求しない場合は、SMB署名要求を無効にできます。

タスク概要

デフォルトでは、SMB署名要求は無効になっています。SMB署名要求は随時有効または無効にできます。

次の状況では、SMB署名はデフォルトで無効になりません。

1. SMB署名要求が有効になっており、クラスタがSMB署名をサポートしていないバージョンのONTAPにリバートされた。
2. その後、クラスタがSMB署名をサポートするバージョンのONTAPにアップグレードされた。

   このような場合は、サポートされているバージョンのONTAPで最初に行われたSMB署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine（SVM）のディザスタ リカバリ関係を設定する場合、 `snapmirror create`コマンドの `-identity-preserve`オプションに選択した値によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

`-identity-preserve`オプションを `true`（ID保持）に設定すると、SMB署名のセキュリティ設定が宛先に複製されます。

`-identity-preserve`オプションを `false`（ID保持なし）に設定した場合、SMB署名セキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバ セキュリティ設定はデフォルト値に設定されます。ソースSVMでSMB署名要求を有効にしている場合は、デスティネーションSVMでも手動でSMB署名要求を有効にする必要があります。

手順

1. 次のいずれかを実行します。

必須のSMB署名を有効にする場合...	コマンドを入力してください...
有効	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
無効	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. 次のコマンドの出力の `Is Signing Required`フィールドの値が目的の値に設定されているかどうかを確認して、必要なSMB署名が有効か無効かを確認します。 `vserver cifs security show -vserver vserver_name -fields is-signing-required`

例

次の例は、SVM vs1でSMB署名要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

暗号化設定の変更点は、新しい接続に対して有効になります。既存の接続は影響を受けません。

関連情報

- "snapmirror create"

ONTAPSMBセッションが署名されているかどうかを確認する

CIFSサーバで接続中のSMBセッションに関する情報を表示できます。この情報を使用して、SMBセッションが署名されているかどうかを確認できます。これは、必要なセキュ

リティ設定を使用してSMBクライアント セッションが接続されているかどうかを確認する場合に役立ちます。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合	コマンドを入力してください...
指定したStorage Virtual Machine（SVM）上の署名されたすべてのセッション	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
SVM上の指定したセッションIDを持つ署名されたセッションの詳細	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

例

次のコマンドは、SVM vs1上の署名済みセッションに関するセッション情報を表示します。デフォルトのサマリー出力には、「`Is Session Signed`」出力フィールドは表示されません：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドは、セッションID 2のSMBセッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報を表示します。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

関連情報

SMB署名済みセッションの統計の監視

ONTAP SMB署名セッション統計を監視する

SMBセッションの統計を監視し、確立されたセッションのうち、署名されたセッションと署名されていないセッションを区別できます。

タスク概要

`statistics`上級権限レベルのコマンドは、署名済みSMBセッションの数を監視するために使用できる `signed_sessions`カウンタを提供します。
`signed_sessions`カウンタは、以下の統計オブジェクトで使用できます：

- `cifs`を使用すると、すべての SMB セッションの SMB 署名を監視できます。
- `smb1`を使用すると、SMB 1.0 セッションの SMB 署名を監視できます。
- `smb2`では、SMB 2.x および SMB 3.0 セッションの SMB 署名を監視できます。

  `smb2`オブジェクトの出力には `SMB 3.0` 統計が含まれます。

署名されたセッションの数とセッションの合計数を比較する場合は、 `signed_sessions`カウンターの出力と

`established_sessions`カウンターの出力を比較できます。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定のサンプル データが表示されます。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

手順

1. 権限レベルを詳細に設定します：+ `set -privilege advanced`
2. データ収集を開始する：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   `-sample-id`パラメータを指定しない場合、コマンドはサンプル識別子を生成し、このサンプルをCLIセッションのデフォルト サンプルとして定義します。 `-sample-id`の値はテキスト文字列です。同じCLIセッション中にこのコマンドを実行し、 `-sample-id`パラメータを指定しない場合、コマンドは以前のデフォルト サンプルを上書きします。

   オプションで、統計情報を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

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

3. `statistics stop`コマンドを使用して、サンプルのデータ収集を停止します。

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

4. 次のコマンドによりSMB署名統計を表示します。

...の情報を表示する場合は	入力する内容
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	署名されたセッションおよび確立されたセッション
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   1 つのノードのみの情報を表示する場合は、オプションの `-node`パラメータを指定します。

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

5. admin権限レベルに戻ります：+ `set -privilege admin`

例

次の例は、「vs1」というStorage Virtual Machine（SVM）について、SMB 2.xとSMB 3.0のそれぞれの署名統計情報を監視する方法を示します。

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

次のコマンドでは、ノードが署名、確立した各SMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- ------------------------
    established_sessions                                            0
    node_name                                                   node1
    signed_sessions                                                 0
    established_sessions                                            1
    node_name                                                   node2
    signed_sessions                                                 1
    established_sessions                                            0
    node_name                                                   node3
    signed_sessions                                                 0
    established_sessions                                            0
    node_name                                                   node4
    signed_sessions                                                 0
```

次のコマンドでは、ノード2が署名したSMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- ------------------------
    node_name                                                   node2
    signed_sessions                                                 1
```

次のコマンドで、admin権限レベルに戻ります。

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

関連情報

- SMBセッションが署名されているかどうかの確認
- "パフォーマンスの監視と管理 - 概要"

SMB経由のデータ転送でのSMBサーバのSMB暗号化要求の設定

ONTAP SMB暗号化について学ぶ

SMBを介したデータ転送でのSMB暗号化は、SMBサーバで有効化または無効化できるセキュリティ強化です。共有プロパティ設定を使用して共有ごとに必要なSMB暗号化を設定することもできます。

デフォルトでは、Storage Virtual Machine（SVM）でのSMBサーバの作成時にSMB暗号化は無効になっています。SMB暗号化が提供する強固なセキュリティを活用するには、SMB暗号化を有効にする必要があります。

暗号化SMBセッションを作成するには、SMBクライアントがSMB暗号化をサポートしている必要があります。SMB暗号化は、Windows Server 2012およびWindows 8以降のWindowsクライアントでサポートされています。

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

- SMBサーバのセキュリティ オプション：SVMでこの機能を有効にする
- SMB共有プロパティ：共有ごとにSMB暗号化を設定する

SVM上のすべてのデータへのアクセスに暗号化を要求するか、選択した共有のデータにアクセスする場合のみにSMB暗号化を要求するかを決定できます。SVMレベルの設定は、共有レベルの設定よりも優先されます。

実際に適用されるSMB暗号化設定は、この2つの設定の組み合わせによって決まります。次の表を参照してください。

SMB サーバの **SMB** 暗号化が有効	共有暗号化データ設定が有効	サーバー側の暗号化の動作
True	False	SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
True	True	共有レベルの暗号化には関係なく、SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
False	True	共有ごとに共有レベルの暗号化が有効になります。この設定では、ツリー接続から暗号化が行われます。

SMB サーバの SMB 暗号化が有効	共有暗号化データ設定が有効	サーバー側の暗号化の動作
False	False	暗号化はすべて無効になります。

暗号化をサポートしないSMBクライアントは、暗号化が必要なSMBサーバや共有には接続できません。

暗号化設定の変更点は、新しい接続に対して有効になります。既存の接続は影響を受けません。

ONTAP SMB暗号化のパフォーマンスへの影響について学ぶ

SMBセッションでSMB暗号化を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスに影響が生じ、クライアントとサーバ（SMBサーバを含むSVMを実行中のクラスタ ノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワーク トラフィックの量に変化がないにもかかわらずクライアントとサーバ両方のCPU使用率が増加する形で表れます。

その程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9.7以降では、新しい暗号化オフロード アルゴリズムによって暗号化されたSMBトラフィックのパフォーマンスを向上させることができます。SMB暗号化オフロードは、SMB暗号化が有効になっている場合はデフォルトで有効になります。

SMB暗号化のパフォーマンス向上には、AES-NIオフロード機能が必要です。ご使用のプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

SMBバージョン3.11を使用できる場合は、より高速なGCMアルゴリズムがサポートされるため、さらなるパフォーマンスの向上が可能です。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB暗号化のパフォーマンスへの影響は大幅に変わってくるため、検証するためには使用しているネットワーク環境でテストを実施する必要があります。

SMB暗号化はSMBサーバではデフォルトで無効になっています。SMB暗号化は、暗号化を必要とするSMB共有またはSMBサーバでのみ有効にしてください。SMB暗号化を有効にすると、ONTAPはすべての要求に対して要求を復号化して応答を暗号化する必要があります。そのため、SMB暗号化は必要な場合にのみ有効にしてください。

受信トラフィックの**ONTAP SMB**暗号化を有効または無効にする

受信SMBトラフィックにSMB暗号化を必須にしたい場合は、CIFSサーバーまたは共有レベルで有効にすることができます。デフォルトでは、SMB暗号化は必須ではありません。

タスク概要

CIFSサーバーでSMB暗号化を有効にすると、CIFSサーバー上のすべての共有に適用されます。CIFSサーバー上のすべての共有でSMB暗号化を必須にしたくない場合、または共有ごとに受信SMBトラフィックでSMB暗号化を必須にしたい場合は、CIFSサーバーでSMB暗号化を必須にすることを無効にできます。

ストレージ仮想マシン（SVM）のディザスタ リカバリ関係を設定する場合、 `snapmirror create`コマンドの`-identity-preserve`オプションに選択した値によって、宛先 SVM に複製される設定の詳細が決まります。

`-identity-preserve`オプションを `true`（ID保持）に設定すると、SMB暗号化セキュリティ設定が宛先に複製されます。

`-identity-preserve`オプションを `false`（ID保持なし）に設定した場合、SMB暗号化セキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバセキュリティ設定はデフォルト値に設定されます。ソースSVMでSMB暗号化を有効にしている場合は、デスティネーションでCIFSサーバのSMB暗号化を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

CIFSサーバでの受信**SMB**トラフィックの**SMB**暗号化要求の設定	コマンドを入力してください...
有効	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true`
無効	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. CIFS サーバーで必要な SMB 暗号化が必要に応じて有効または無効になっていることを確認します（：）`vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   `is-smb-encryption-required`フィールドには、CIFS サーバーで必要な SMB 暗号化が有効になっている場合は `true`、無効になっている場合は `false`が表示されます。

例

次の例は、SVM vs1でCIFSサーバの受信SMBトラフィックのSMB暗号化要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

関連情報

- "snapmirror create"

クライアントが暗号化された**ONTAP SMB**セッションを使用して接続されているかどうかを確認する

接続されたSMBセッションに関する情報を表示することで、クライアントが暗号化されたSMB接続を使用しているかどうかを確認できます。これは、SMBクライアントセッションが適切なセキュリティ設定で接続しているかどうかを確認するのに役立ちます。

タスク概要

SMB クライアント セッションには、次の 3 つの暗号化レベルのいずれかを設定できます：

- `unencrypted`

  SMBセッションは暗号化されていません。Storage Virtual Machine（SVM）レベルまたは共有レベルの暗号化は設定されていません。

- `partially-encrypted`

  ツリー接続が発生すると暗号化が開始されます。共有レベルの暗号化が設定されています。SVMレベルの暗号化は有効になっていません。

- `encrypted`

  SMBセッションは完全に暗号化されています。SVMレベルの暗号化は有効です。共有レベルの暗号化は有効になっている場合と無効になっている場合があります。SVMレベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合	コマンドを入力してください...
指定されたSVM上のセッションに対して指定された暗号化設定を持つセッション	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定されたSVM上の特定のセッションIDの暗号化設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

例

次のコマンドは、セッション ID が 2 の SMB セッションの暗号化設定を含む詳細なセッション情報を表示します：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

ONTAP SMB暗号化統計を監視する

SMB暗号化の統計を監視し、確立されたセッションおよび共有接続のうち、暗号化されたものと暗号化されていないものを区別できます。

タスク概要

`statistics`コマンドは、advanced権限レベルで、暗号化されたSMBセッションと共有接続の数を監視するために使用できる次のカウンターを提供します：

カウンタ名	説明
encrypted_sessions	暗号化されたSMB 3.0セッション数
encrypted_share_connections	ツリー接続によって暗号化された共有数
rejected_unencrypted_sessions	クライアントに暗号化機能がないために拒否されたセッション セットアップ数
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを利用できます。

- `cifs`を使用すると、すべての SMB 3.0 セッションの SMB 暗号化を監視できます。

  SMB 3.0 の統計情報は、 `cifs` オブジェクトの出力に含まれています。暗号化されたセッション数とセッションの総数を比較したい場合は、 `encrypted_sessions` カウンタの出力と `established_sessions` カウンタの出力を比較してください。

  暗号化された共有接続の数を共有接続の合計数と比較する場合は、 `encrypted_share_connections`カウンターの出力を `connected_shares`カウンターの出力と比較できます。

- `rejected_unencrypted_sessions`は、SMB暗号化をサポートしていないクライアントから、暗号化を必要とするSMBセッションを確立しようとした回数を示します。
- `rejected_unencrypted_shares`は、SMB 暗号化をサポートしていないクライアントから、暗号化を必要とする SMB 共有への接続を試行した回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定のサンプル データが表示されます。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

手順

1. 権限レベルを詳細に設定します：+ `set -privilege advanced`
2. データ収集を開始する：+ `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   `-sample-id`パラメータを指定しない場合、コマンドはサンプル識別子を生成し、このサンプルをCLIセッションのデフォルト サンプルとして定義します。 `-sample-id`の値はテキスト文字列です。同じCLIセッション中にこのコマンドを実行し、 `-sample-id`パラメータを指定しない場合、コマンドは以前のデフォルト サンプルを上書きします。

   オプションで、統計情報を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

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

3. `statistics stop`コマンドを使用して、サンプルのデータ収集を停止します。

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

4. SMB暗号化統計情報を表示します。

...の情報を表示する場合は	入力する内容
暗号化されたセッション	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	暗号化されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	暗号化された共有接続
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
暗号化された共有接続と接続された共有	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒否された暗号化されていないセッション	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された暗号化されていない共有接続
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

単一のノードの情報のみを表示する場合は、オプションの `-node`パラメータを指定します。

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

5. admin権限レベルに戻ります：+ `set -privilege admin`

例

次の例は、「vs1」というStorage Virtual Machine（SVM）について、SMB 3.0の暗号化統計情報を監視する方法を示します。

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

次のコマンドは、指定したノードについて、暗号化されたSMBセッション数と確立されたセッション数をサンプルから表示します。

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMBセッション数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

次のコマンドは、指定したノードについて、接続されたSMB共有数と暗号化されたSMB共有数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

次のコマンドは、指定したノードについて、拒否された暗号化されていないSMB共有接続数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

関連情報

- サーバー上で利用可能な統計、オブジェクト、カウンターを決定する
- "パフォーマンスの監視と管理 - 概要"

LDAPセッションの通信の保護

ONTAP SMB LDAP署名とシーリングについて学ぶ

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会に対

するLDAPセッション セキュリティを有効にすることができます。Storage Virtual Machine（SVM）のCIFSサーバ セキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、秘密鍵技術を使用してLDAPペイロード データの整合性を確認します。シーリングは、機密情報をクリアテキストで送信しないようにLDAPペイロード データを暗号化します。_LDAPセキュリティ レベル_オプションは、LDAPトラフィックに署名が必要か、署名とシーリングの両方が必要か、あるいはどちらも不要かを指定します。デフォルトは `none`です。

LDAP署名とシーリングがSVM上のCIFSトラフィックで有効になっているのは、 `vserver cifs security modify`コマンドの `-session-security-for-ad-ldap`オプションによるものです。

ONTAP SMBサーバでLDAP署名とシーリングを有効にする

CIFSサーバがActive Directory LDAPサーバとの安全な通信に署名とシーリングを使用するには、事前にCIFSサーバのセキュリティ設定を変更してLDAP署名とシーリングを有効にする必要があります。

開始する前に

適切なセキュリティ構成値を決定するには、ADサーバ管理者に相談する必要があります。

手順

1. Active Directory LDAPサーバとの署名およびシールされたトラフィックを有効にするCIFSサーバ セキュリティ設定を構成します（：） `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   署名(`sign`（データ整合性）、署名とシーリング(`seal`（データ整合性と暗号化）、またはどちらも有効にしない `none`（署名もシーリングも有効にしない）ことができます。デフォルト値は `none`です。

2. LDAP署名および封印のセキュリティ設定が正しく設定されていることを確認します： `vserver cifs security show -vserver` *`vserver_name`*

   > SVMが名前マッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）を照会するために同じLDAPサーバを使用する場合は、 `vserver services name-service ldap client modify`コマンドの `-session-security`オプションを使用して対応する設定を有効にする必要があります。

LDAP over TLSの設定

ONTAP SMB SVMの自己署名ルートCA証明書をエクスポートする

Active Directory通信の保護にLDAP over SSL/TLSを使用するには、まずActive Directory証明書サービスの自己署名ルートCA証明書のコピーを証明書ファイルにエクスポートし、それをASCIIテキスト ファイルに変換する必要があります。ONTAPは、このテキスト ファイルを使用して証明書をStorage Virtual Machine（SVM）にインストールします。

開始する前に

Active Directory証明書サービスがすでにインストールされ、CIFSサーバが属するドメイン用に設定されている必要があります。Active Directory証明書サービスのインストールと設定の詳細については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ：technet.microsoft.com/ja-jp/library/"

手順

1. `.pem`テキスト形式のドメイン コントローラのルート CA 証明書を取得します。

   "Microsoft TechNetライブラリ：technet.microsoft.com/ja-jp/library/"

終了後の操作

SVMに証明書をインストールします。

関連情報

"Microsoft TechNetライブラリ"

ONTAP SMB SVMに自己署名ルート**CA**証明書をインストールする

LDAPサーバにバインドするときにTLSを使用したLDAP認証が必要な場合は、まず自己署名されたルートCA証明書をSVMにインストールする必要があります。

タスク概要

TLS通信を使用するONTAP内のすべてのアプリケーションは、Online Certificate Status Protocol（OCSP）を使用してデジタル証明書のステータスを確認できます。LDAP over TLSでOCSPが有効になっている場合、失効した証明書は拒否され、接続は失敗します。

手順

1. 自己署名ルートCA証明書をインストールします。
   a. 証明書のインストールを開始します： `security certificate install -vserver vserver_name -type server-ca`

      コンソール出力に次のメッセージが表示されます： `Please enter Certificate: Press <Enter> when done`

   b. 証明書`.pem`ファイルをテキスト エディターで開き、`-----BEGIN CERTIFICATE-----`で始まり`-----END CERTIFICATE-----`で終わる行を含む証明書をコピーして、コマンド プロンプトの後に貼り付けます。
   c. 証明書が正しく表示されることを確認します。
   d. Enterキーを押して、インストールを完了します。
2. 証明書がインストールされていることを確認します： `security certificate show -vserver vserver_name`

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するためには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

ONTAP 9.10.1以降、Active Directory（AD）とネームサービスのLDAP接続の両方で、LDAPチャネルバインディングがデフォルトでサポートされます。ONTAPは、Start-TLSまたはLDAPSが有効で、セッションセキュリティが署名またはシールに設定されている場合にのみ、LDAP接続でチャネルバインディングを試行します。ADサーバとのLDAPチャネルバインディングを無効化または再有効化するには、 `vserver cifs security modify`コマンドで `-try-channel-binding-for-ad-ldap`パラメータを使用します。

詳細については、以下を参照してください。

- "ONTAP NFS SVMのLDAPについて学ぶ"
- "Windows の 2020 年 LDAP チャネル バインディングおよび LDAP 署名要件"。

手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を許可するSMBサーバのセキュリティ設定を構成します： `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. LDAP over TLS セキュリティ設定が次のように設定されていることを確認します： `true vserver cifs security show -vserver vserver_name`

> SVMが名前マッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、 `vserver services name-service ldap client modify`コマンドを使用して `-use-start-tls`オプションも変更する必要があります。

パフォーマンスと冗長性を確保するために **ONTAP SMB** マルチチャネルを構成する

ONTAP 9.4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立することができます。有効にすると、スループットとフォールト トレランスが向上します。

開始する前に

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

タスク概要

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

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

- クライアントと**ONTAP**クラスタ上の**1G NIC**

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

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

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

さらに、次のパラメータを変更することができます（advanced権限）。

- `-max-connections-per-session`

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

  デフォルトよりも多くの接続を許可する場合は、クライアントの設定も調整する必要があります（クライアントもデフォルトの接続数は32です）。

- `-max-lifs-per-session`

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

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

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

3. SMBマルチチャネル セッションがONTAPのレポート対象になっていることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

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

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

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

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

SMBサーバでのデフォルトWindowsユーザからUNIXユーザへのマッピングの設定

デフォルトのONTAP SMB UNIXユーザーを設定する

特定のユーザーに対する他のすべてのマッピング試行が失敗した場合、またはUNIXとWindows間で個々のユーザーをマッピングしたくない場合は、デフォルトのUNIXユーザーを設定できます。一方、マッピングされていないユーザーの認証を失敗させたい場合には、デフォルトのUNIXユーザーを設定しないでください。

タスク概要

デフォルトでは、デフォルトUNIXユーザの名前は「pcuser」です。これは、デフォルトUNIXユーザへのユーザマッピングがデフォルトで有効になっていることを意味します。デフォルトUNIXユーザとして使用する別の名前を指定することもできます。指定する名前は、Storage Virtual Machine（SVM）用に設定されたネームサービスデータベースに存在している必要があります。このオプションがNULL文字列に設定されている場合、UNIXデフォルトユーザとしてCIFSサーバにアクセスすることはできません。つまり、各ユーザはCIFSサーバにアクセスする前に、パスワードデータベースにアカウントを持っている必要があります。

ユーザーがデフォルトの UNIX ユーザー アカウントを使用して CIFS サーバーに接続するには、次の前提条件を満たしている必要があります：

- ユーザーは認証されています。
- ユーザーは、CIFS サーバーのローカル Windows ユーザー データベース、CIFS サーバーのホーム ドメイン、または信頼されたドメイン（CIFS サーバーでマルチドメイン名マッピング検索が有効になっている場合）に存在します。
- ユーザー名は明示的に null 文字列にマップされていません。

手順

1. デフォルトのUNIXユーザを設定します。

状況	コマンド
デフォルトのUNIXユーザー「pcuser」を使用する	`vserver cifs options modify -default -unix-user pcuser`
別のUNIXユーザーアカウントをデフォルトユーザーとして使用する	`vserver cifs options modify -default -unix-user user_name`
デフォルトのUNIXユーザを無効にする	`vserver cifs options modify -default -unix-user ""`

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

2. デフォルトの UNIX ユーザーが正しく設定されていることを確認します： `vserver cifs options show -vserver vserver_name`

次の例では、SVM vs1 上のデフォルトの UNIX ユーザーとゲスト UNIX ユーザーの両方が、UNIX ユーザ

ー「pcuser」を使用するように設定されています：

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

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

ゲスト**ONTAP SMB UNIX**ユーザーを構成する

ゲストUNIXユーザーオプションを設定すると、信頼されていないドメインからログインしたユーザーはゲストUNIXユーザーにマッピングされ、CIFSサーバーに接続できるようになります。一方、信頼されていないドメインのユーザーの認証を失敗させたい場合は、ゲストUNIXユーザーを設定しないでください。デフォルトでは、信頼されていないドメインのユーザーはCIFSサーバーに接続できません（ゲストUNIXアカウントは設定されていません）。

タスク概要

ゲスト UNIX アカウントを構成するときは、次の点に留意してください：

- CIFSサーバがホーム ドメインまたは信頼できるドメインのドメイン コントローラ、もしくはローカル データベースに対してユーザを認証できず、このオプションが有効である場合、CIFSサーバはユーザをゲスト ユーザとみなし、そのユーザを指定したUNIXユーザにマッピングします。
- このオプションがヌル文字列に設定されている場合、ゲストUNIXユーザーは無効になります。
- いずれかのStorage Virtual Machine（SVM）ネーム サービス データベースで、ゲストUNIXユーザとして使用するUNIXユーザを作成する必要があります。
- ゲスト ユーザーとしてログインしたユーザーは、自動的に CIFS サーバー上の BUILTIN\guests グループのメンバーになります。
- 「homedirs-public」オプションは認証されたユーザーにのみ適用されます。ゲストユーザーとしてログインしたユーザーにはホームディレクトリがないため、他のユーザーのホームディレクトリにアクセスできません。

手順

1. 次のいずれかを実行します。

状況	入力する内容
ゲストUNIXユーザを設定する	`vserver cifs options modify -guest -unix-user unix_name`
ゲスト UNIX ユーザーを無効にする	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. ゲスト UNIX ユーザーが正しく設定されていることを確認します： `vserver cifs options show -vserver vserver_name`

   次の例では、SVM vs1 上のデフォルトの UNIX ユーザーとゲスト UNIX ユーザーの両方が、UNIX ユーザー「pcuser」を使用するように設定されています：

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

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

管理者グループを**ONTAP SMB**ルートにマッピングする

環境内に CIFS クライアントのみがあり、ストレージ仮想マシン（SVM）がマルチプロトコル ストレージ システムとしてセットアップされている場合は、SVM 上のファイルにアクセスするためのルート権限を持つ Windows アカウントが少なくとも 1 つ必要です。そうでない場合、十分なユーザー権限がないため、SVM を管理できません。

タスク概要

ストレージ システムが NTFS 専用として設定されている場合、 `/etc`ディレクトリにはファイル レベルの ACL があり、管理者グループが ONTAP 構成ファイルにアクセスできるようになります。

手順

1. 権限レベルをadvancedに設定します： `set -privilege advanced`
2. 必要に応じて、管理者グループをルートにマッピングするCIFSサーバーオプションを構成します：

状況	操作
管理者グループのメンバーをrootにマップする	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled true`管理者グループに属するすべてのアカウントは、たとえ`/etc/usermap.cfg`アカウントをrootにマッピングするエントリがない場合でも、rootとみなされます。管理者グループに属するアカウントを使用してファイルを作成した場合、UNIXクライアントからそのファイルを表示すると、そのファイルの所有者はrootになります。
管理者グループのメンバーをrootにマッピングしないようにする	`vserver cifs options modify -vserver *vserver_name* -is-admin-users-mapped-to-root-enabled false` 管理者グループのアカウントはrootにマッピングされなくなりました。rootに明示的にマッピングできるのは単一のユーザーのみです。

3. オプションが目的の値に設定されていることを確認します： `vserver cifs options show -vserver *vserver_name*`
4. admin権限レベルに戻ります： `set -privilege admin`

ONTAP SMBセッションを介して接続されるユーザーの種類に関する情報を表示します

SMBセッション経由で接続しているユーザのタイプを表示できます。これは、適切なタイプのユーザのみがStorage Virtual Machine（SVM）上のSMBセッション経由で接続していることを確認するのに役立ちます。

タスク概要

SMBセッション経由で接続できるのは、次のタイプのユーザです。

- `local-user`

  ローカル CIFS ユーザーとして認証

- `domain-user`

  ドメイン ユーザーとして認証されている（CIFS サーバーのホーム ドメインまたは信頼されたドメインのいずれかから）

- `guest-user`

  ゲスト ユーザーとして認証されました

- `anonymous-user`

  匿名またはnullユーザーとして認証されました

手順

1. SMB セッションを介して接続されているユーザーのタイプを判別します： `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

確立されたセッションのユーザー タイプ情報を表示する場合：	入力するコマンド
指定されたユーザー タイプのすべてのセッション	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	特定のユーザーの場合

例

次のコマンドは、ユーザー「` iepubs\user1`」によって確立された SVM vs1 上のセッションのユーザー タイプに関するセッション情報を表示します：

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

過剰な **Windows** クライアントのリソース消費を制限するための **ONTAP** コマンドオプション

`vserver cifs options modify`コマンドのオプションを使用すると、Windowsクライアントのリソース消費を制御できます。これは、クライアントのリソース消費量が通常の範囲を超えている場合（例えば、開いているファイル、開いているセッション、変更通知要求の数が異常に多い場合など）に役立ちます。

`vserver cifs options modify`コマンドに、Windowsクライアントのリソース消費を制御するための以下のオプションが追加されました。これらのオプションのいずれかの最大値を超えた場合、要求は拒否され、EMSメッセージが送信されます。また、これらのオプションに設定された制限値の80%に達した場合も、EMS警告メッセージが送信されます。

- `-max-opens-same-file-per-tree`

CIFSツリーあたりの同じファイルの最大オープン数

- `-max-same-user-sessions-per-connection`

  同じユーザによる接続あたりの最大オープン セッション数

- `-max-same-tree-connect-per-session`

  同じ共有に対するセッションあたりの最大ツリー接続数

- `-max-watches-set-per-tree`

  ツリーごとに確立されるウォッチ（_change notifies_とも呼ばれる）の最大数

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

ONTAP 9.4以降、SMBバージョン2以降を実行するサーバでは、クライアントがSMB接続でサーバに送信できる未処理の要求（*SMB*クレジット）の数を制限できます。SMBクレジットの管理はクライアントによって開始され、サーバによって制御されます。

SMB接続で許可できる未処理リクエストの最大数は、 `-max-credits`オプションによって制御されます。このオプションのデフォルト値は128です。

従来の**oplock**および**oplock**リースでのクライアント パフォーマンスの向上

従来の **oplock** とリース **oplock** を使用して **ONTAP SMB** クライアントのパフォーマンスを向上させる方法について説明します。

従来のoplock（便宜的ロック）とリースoplockは、特定のファイル共有シナリオにおいて、SMBクライアントが先読み、後書き、およびロック情報をクライアント側でキャッシュすることを可能にします。これにより、クライアントは、サーバーに対象ファイルへのアクセスが必要であることを定期的に通知することなく、ファイルの読み書きを行うことができます。これによりネットワーク トラフィックが削減され、パフォーマンスが向上します。

oplockリースはoplockを強化したもので、SMB 2.1以降のプロトコルで使用できます。oplockリースでは、クライアントが、自身による複数のSMBオープンにおいてキャッシュ状態を取得、保持できます。

Oplocks は次の 2 つの方法で制御できます：

- 共有プロパティにより、共有の作成時の `vserver cifs share create`コマンド、または作成後の `vserver share properties`コマンドを使用します。
- qtreeプロパティにより、qtreeの作成時に `volume qtree create`コマンドを使用するか、作成後に `volume qtree oplock`コマンドを使用します。

oplock 使用時の ONTAP SMB キャッシュ データ損失に関する考慮事項について学習します

状況によっては、あるプロセスがファイルに対して排他的なoplockを保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスは、キャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントはoplockを放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われることがあります。

- データ損失の可能性

  書き込みキャッシュされたデータを持つアプリケーションは、次のような状況下ではそのデータを失う可能性があります：

  - 接続は SMB 1.0 を使用して行われます。
  - ファイルに対して排他的 oplock が存在します。
  - そのoplockを解除するか、ファイルを閉じるように指示されます。
  - 書き込みキャッシュをフラッシュするプロセス中に、ネットワークまたはターゲット システムでエラーが発生します。

- エラー処理と書き込み完了

  キャッシュ自体にエラー処理機能はなく、アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行う場合、書き込みは必ず完了します。反対にキャッシュがネットワーク経由でターゲット システムに書き込みを行う場合、書き込みが完了したものとみなす必要があります。そうでないと、データが失われます。

ONTAP SMB共有を作成するときにoplocksを有効または無効にする

oplockを使用すると、クライアントによりファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスを向上できます。Storage Virtual Machine（SVM）上にあるSMB共有では、oplockが有効になります。場合によっては、oplockの無効化が必要になることがあります。oplockは共有ごとに有効または無効にできます。

タスク概要

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームのoplockの設定よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。

oplock共有プロパティに加えて、その他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する処理を実行します。

状況	操作
共有の作成時に共有でoplockを有効にする	次のコマンドを入力します： `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` 共有にデフォルトの共有プロパティ（ `oplocks`、 `browsable`、および `changenotify`が有効）のみを設定する場合は、SMB共有の作成時に `-share-properties`パラメータを指定する必要はありません。デフォルト以外の共有プロパティの組み合わせを設定する場合は、その共有で使用する共有プロパティのリストを `-share-properties`パラメータで指定する必要があります。
共有の作成時に共有でoplockを無効にする	次のコマンドを入力します： `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` oplock を無効にする場合は、共有を作成するときに共有プロパティのリストを指定する必要がありますが、 `oplocks` プロパティは指定しないでください。

関連情報

既存のSMB共有でのoplockの有効化と無効化

oplockステータスの監視

SMBボリュームおよびqtreeでoplockを有効または無効にするONTAPコマンド

oplockを使用すると、クライアントによりファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスを向上できます。ボリュームやqtreeのoplockを有効または無効にするコマンドについて説明します。また、いつボリュームおよびqtreeでoplockを有効化または無効化できるかについても理解しておく必要があります。

- ボリュームではデフォルトでoplockが有効になっています。
- ボリュームを作成する際にoplockを無効化することはできません。

- 既存のSVMのボリュームでは、oplockをいつでも有効または無効にすることができます。
- SVMのqtreeではoplockを有効にできます。

  oplockモードは、すべてのボリュームにあるデフォルトのqtree（qtree ID 0）のプロパティで指定します。qtreeの作成時にoplock設定を指定しない場合、qtreeは親ボリュームのoplock設定（デフォルトでは有効）を継承します。ただし、新しいqtreeにoplock設定を指定した場合、ボリュームのoplock設定よりも優先されます。

状況	使用するコマンド
ボリュームまたはqtreeのoplockを有効にする	`volume qtree oplocks` と `-oplock-mode` パラメータを `enable` に設定
ボリュームまたはqtreeのoplockを無効にする	`volume qtree oplocks` と `-oplock-mode` パラメータを `disable` に設定

関連情報

oplockステータスの監視

既存のONTAP SMB共有でoplockを有効または無効にする

Storage Virtual Machine（SVM）上のSMB共有では、oplockがデフォルトで有効になっています。場合によっては、oplockの無効化が必要になることがあります。または、以前に共有でoplockを無効にした場合に、oplockを再度有効にすることもあります。

タスク概要

共有を含むボリュームでoplockが有効になっているが、その共有のoplock共有プロパティが無効になっている場合、その共有のoplockは無効になります。共有でのoplockの無効化は、ボリュームでのoplockの有効化よりも優先されます。共有でoplockを無効にすると、便宜的oplockとoplockリースの両方が無効になります。既存の共有でのoplockの有効化と無効化はいつでも実行できます。

手順

1. 該当する処理を実行します。

状況	操作
既存の共有を変更して共有でoplockを有効にする	次のコマンドを入力します： `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` 追加する共有プロパティをカンマで区切って追加指定できます。 新たに追加したプロパティは、共有プロパティの既存のリストに追加されます。以前に指定した共有プロパティは有効なままです。

状況	操作
既存の共有を変更して共有でoplockを無効にする	次のコマンドを入力します：`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 削除する共有プロパティをカンマで区切って追加指定できます。 削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しなかった設定済みの共有プロパティは有効なままになります。

例

次のコマンドは、Storage Virtual Machine（SVM、旧Vserver）vs1上の「Engineering」という名前の共有に対してoplockを有効にします：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

次のコマンドは、SVM vs1上の「Engineering」という名前の共有のoplockを無効にします：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

関連情報

- SMB共有の作成時におけるoplockの有効化と無効化
- oplockステータスの監視

- 既存の共有の共有プロパティを追加または削除する

ONTAP SMB oplockステータスを監視する

oplockステータスについて、情報を監視、表示することができます。この情報を使用すると、oplockが設定されたファイル、oplockのレベルやoplockの状態レベルのほか、oplockリースの使用の有無を特定できます。また、手動での解除が必要となる可能性のあるロックについて、情報を取得することもできます。

タスク概要

すべてのoplockについての情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、クライアントのIPアドレスやパスを指定して、該当するロックのみを返すように指定できます。

従来のoplockおよびoplockリースについて、次の情報を表示できます。

- oplockが有効なSVM、ノード、ボリューム、LIF
- ロックUUID
- oplockが有効なクライアントのIPアドレス
- oplockが有効なパス
- ロックのプロトコル（SMB）およびタイプ（oplock）
- ロックの状態
- oplockレベル
- 接続の状態およびSMBの有効期限
- oplockリースが有効な場合のOpen Group ID

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

手順

1. `vserver locks show`コマンドを使用して oplock ステータスを表示します。

例

次のコマンドは、すべてのロックに関するデフォルト情報を表示します。表示されたファイルに対するoplockは、 `read-batch` oplockレベルで付与されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

次の例は、パス `/data2/data2_2/intro.pptx`のファイルに対するロックに関する詳細情報を表示します。IPアドレス `10.3.1.3`のクライアントに対して、 `batch` oplockレベルのリースoplockがファイルに対して付与されています：

詳細情報を表示する場合に、このコマンドを使用すると、oplockの情報と共有ロックの情報を別々に表示できます。この例では、oplockの情報のみが表示されています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

関連情報

SMB共有の作成時におけるoplockの有効化と無効化

既存のSMB共有でのoplockの有効化と無効化

SMBボリュームおよびqtreeでoplockを有効または無効にするコマンド

SMBサーバへのグループ ポリシー オブジェクトの適用

ONTAP SMB サーバへのグループ ポリシー オブジェクトの適用について学習します

SMBサーバーは、Active Directory環境内のコンピュータに適用される_グループポリシー属性_と呼ばれる一連のルールであるグループポリシーオブジェクト（GPO）をサポートしています。GPOを使用すると、同じActive Directoryドメインに属するクラスタ上のすべてのStorage Virtual Machine（SVM）の設定を一元管理できます。

ONTAPは、SMBサーバでGPOが有効になっている場合、Active DirectoryサーバにLDAPクエリを送信し

てGPO情報を要求します。Active Directoryサーバは、SMBサーバに適用できるGPO定義がある場合、次のGPO情報を返します。

- GPO名
- 現在のGPOバージョン
- GPO定義の場所
- GPOポリシー セットのUniversally Unique Identifier（UUID）一覧

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- "SMBおよびNFS監査とセキュリティトレース"

サポートされている**ONTAP SMB GPO**について学ぶ

すべてのグループ ポリシー オブジェクト（GPO）をCIFS対応のStorage Virtual Machine（SVM）に適用できるわけではありませんが、SVMでは関連するGPOを認識して処理することができます。

SVMで現在サポートされているGPOは次のとおりです。

- 高度な監査ポリシー構成の設定：

  オブジェクト アクセス：集中アクセス ポリシーのステージング

  集約型アクセス ポリシー（CAP）のステージングで監査対象となるイベント タイプを次の中から指定します。

  - 監査しない
  - 成功イベントのみを監査する
  - 失敗イベントのみを監査する
  - 成功イベントと失敗イベントの両方を監査する

  > 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

  `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO の `Audit Central Access Policy Staging`設定を使用して設定します。

  > 高度な監査ポリシー構成GPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- レジストリ設定：

- CIFS対応SVMのグループポリシー更新間隔

  `Registry` GPO を使用して設定します。

- グループ ポリシー更新のランダム オフセット

  `Registry` GPO を使用して設定します。

- BranchCacheのハッシュ公開

  BranchCacheのハッシュの発行GPOは、BranchCacheの動作モードに対応します。次の3つの動作モードがサポートされています。

  - 1株当たり
  - 全株式
  - `Registry` GPO を使用して無効に設定します。

- BranchCacheのハッシュバージョンのサポート

  次の3つのハッシュ バージョン設定がサポートされています。

  - BranchCache バージョン1
  - BranchCache バージョン2
  - BranchCacheバージョン1および2 `Registry`GPOを使用して設定します。

  BranchCache GPO設定を使用するには、その設定を適用するCIFS対応のSVM上でBranchCacheを構成する必要があります。SVMでBranchCacheが構成されていない場合、GPO設定は適用されず、破棄されます。

- セキュリティ設定
  - 監査ポリシーとイベント ログ
    - ログオン イベントの監査

      監査対象となるログオン イベントのタイプを次の中から指定します。

      - 監査しない
      - 成功イベントのみを監査する
      - 障害イベントの監査
      - 成功イベントと失敗イベントの両方を監査します。 `Local Policies/Audit Policy` GPO の `Audit logon events`設定を使用して設定します。

        3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- オブジェクト アクセスの監査

  監査対象となるオブジェクト アクセスのタイプを次の中から指定します。

  - 監査しない
  - 成功イベントのみを監査する
  - 障害イベントの監査
  - 成功イベントと失敗イベントの両方を監査します。 `Local Policies/Audit Policy` GPO の `Audit object access`設定を使用して設定します。

    > 3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログ保持方法

  監査ログの保持方法を次の中から指定します。

  - ログ ファイルのサイズが最大ログ サイズを超えた場合にイベント ログを上書きする
  - イベント ログを上書きしない（ログを手動でクリアする） `Event Log` GPO 内の `Retention method for security log`設定を使用して設定します。

- 最大ログ サイズ

  監査ログの最大サイズを指定します。

  `Event Log` GPO の `Maximum security log size`設定を使用して設定します。

  > 監査ポリシーとイベント ログGPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

◦ ファイルシステムのセキュリティ

GPOでファイル セキュリティを適用するファイルまたはディレクトリのリストを指定します。

`File System` GPO を使用して設定します。

> SVM内にファイルシステム セキュリティGPOを構成するボリューム パスが存在している必要があります。

◦ Kerberosポリシー

- 最大クロック スキュー

  コンピュータ クロックの同期の許容最大誤差を分単位で指定します。

`Account Policies/Kerberos Policy` GPO の `Maximum tolerance for computer clock synchronization`設定を使用して設定します。

- チケットの最大有効期間

  ユーザ チケットの最大有効期間を時間単位で指定します。

  `Account Policies/Kerberos Policy` GPO の `Maximum lifetime for user ticket`設定を使用して設定します。

- チケットの最大更新期間

  ユーザ チケットの更新の最大有効期間を日単位で指定します。

  `Account Policies/Kerberos Policy` GPO の `Maximum lifetime for user ticket renewal`設定を使用して設定します。

◦ ユーザー権限の割り当て（特権）

- 所有権の取得

  セキュリティ保護が可能なオブジェクトの所有権を取得できるユーザとグループのリストを指定します。

  `Local Policies/User Rights Assignment` GPO の `Take ownership of files or other objects`設定を使用して設定します。

- セキュリティ権限

  ファイル、フォルダ、Active Directoryオブジェクトなどの個々のリソースへのオブジェクト アクセスの監査オプションを指定できるユーザとグループのリストを指定します。

  `Local Policies/User Rights Assignment` GPO の `Manage auditing and security log`設定を使用して設定します。

- 通知権限の変更（トラバース チェックのバイパス）

  トラバースするディレクトリに対する権限がなくても、ディレクトリ ツリーをトラバースできるユーザとグループのリストを指定します。

ファイルやディレクトリの変更に関する通知をユーザーが受け取る場合にも、同じ権限が必要です。`Local Policies/User Rights Assignment` GPOの `Bypass traverse checking`設定を使用して設定します。

◦ レジストリ値

▪ 署名必須設定

SMB署名要求を有効にするか無効にするかを指定します。

`Security Options` GPO の `Microsoft network server: Digitally sign communications (always)`設定を使用して設定します。

◦ 匿名アクセスを制限する

匿名ユーザに対する制限を、次の3つのGPO設定で指定します。

▪ セキュリティ アカウント マネージャー (SAM) アカウントの列挙がありません：

このセキュリティ設定は、コンピュータへの匿名接続に対して付与される追加の権限を決定します。このオプションは、有効になっている場合、ONTAPでは `no-enumeration`と表示されます。

`Local Policies/Security Options` GPO の `Network access: Do not allow anonymous enumeration of SAM accounts`設定を使用して設定します。

▪ SAM アカウントと共有の列挙なし

このセキュリティ設定は、SAMアカウントと共有の匿名列挙を許可するかどうかを決定します。このオプションは、有効になっている場合、ONTAPでは `no-enumeration`として表示されます。

`Local Policies/Security Options` GPO の `Network access: Do not allow anonymous enumeration of SAM accounts and shares`設定を使用して設定します。

▪ 共有と名前付きパイプへの匿名アクセスを制限する

このセキュリティ設定は、共有およびパイプへの匿名アクセスを制限します。このオプションは、有効になっている場合、ONTAPでは `no-access`と表示されます。

`Local Policies/Security Options` GPO の `Network access: Restrict anonymous access to Named Pipes and Shares`設定を使用して設定します。

定義済みおよび適用済みのグループ ポリシーに関する情報を表示する際、 `Resultant restriction for anonymous user`出力フィールドには、匿名を制限する3つのGPO設定の結果的な制限に関する情報が表示されます。結果として生じる可能性のある制限は次のとおりです：

◦ no-access

匿名ユーザーは指定された共有および名前付きパイプへのアクセスを拒否され、SAMアカウントと共有の列挙も使用できません。この制限は、 `Network access: Restrict anonymous access to Named

Pipes and Shares`GPOが有効になっている場合に表示されます。

- `no-enumeration`

  匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAMアカウントと共有は列挙できません。この制限は、次の両方の条件に該当する場合に表示されます。

  - `Network access: Restrict anonymous access to Named Pipes and Shares`GPO は無効になっています。
  - `Network access: Do not allow anonymous enumeration of SAM accounts`または `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPO のいずれかが有効になっています。

- `no-restriction`

  匿名ユーザにはフル アクセスが付与され、列挙できます。この制限は、次の両方の条件に該当する場合に表示されます。

  - `Network access: Restrict anonymous access to Named Pipes and Shares`GPO は無効になっています。
  - `Network access: Do not allow anonymous enumeration of SAM accounts`と `Network access: Do not allow anonymous enumeration of SAM accounts and shares`の両方のGPOが無効になっています。
    - 制限付きグループ

      制限されたグループを設定して、組込みグループやユーザ定義グループのメンバーを集中管理することができます。グループ ポリシーを通して制限されたグループを適用する場合、CIFS サーバ ローカル グループのメンバーは、適用されるグループ ポリシーで定義されているメンバー リスト設定に一致するように自動的に設定されます。

      `Restricted Groups` GPO を使用して設定します。

- 集約型アクセス ポリシーの設定

  集約型アクセス ポリシーのリストを示します。集約型アクセス ポリシーと関連付けられた集約型アクセス ポリシー ルールによって、SVM上の複数のファイルに対するアクセス権が決定されます。

関連情報

- サーバー上の GPO サポートを有効または無効にする
- サーバーのファイル アクセス セキュリティについて学ぶ
- "SMBおよびNFS監査とセキュリティトレース"
- サーバーのセキュリティ設定を変更する
- BranchCacheを使用してブランチオフィスで共有コンテンツをキャッシュする方法について学習します
- ONTAP署名を使用してネットワークセキュリティを強化する方法について学習します
- バイパス トラバース チェックの設定について学ぶ
- 匿名ユーザに対するアクセス制限の設定

ONTAP SMBサーバのGPO要件

SMBサーバでグループ ポリシー オブジェクト（GPO）を使用するには、いくつかの要件を満たしている必要があります。

- クラスタにはSMBのライセンスが必要です。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サーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- SMBサーバ管理ステータスがオンである必要があります。
- GPOが設定され、SMBサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位（OU）に適用されている必要があります。
- SMBサーバでGPOのサポートが有効になっている必要があります。

ONTAP SMBサーバでGPOサポートを有効または無効にする

CIFSサーバでグループ ポリシー オブジェクト（GPO）のサポートを有効または無効にできます。CIFSサーバでGPOのサポートを有効にすると、グループ ポリシー（CIFSサーバ コンピュータ オブジェクトを含む組織単位に適用されるポリシー）に定義されている該当するGPOがCIFSサーバに適用されます。

タスク概要

GPOはワークグループ モードのCIFSサーバでは有効にできません。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
GPOを有効にする	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOを無効にする	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. GPO サポートが目的の状態であることを確認します（：） `vserver cifs group-policy show -vserver +vserver_name_`

   ワークグループ モードの CIFS サーバーのグループ ポリシー ステータスは「disabled」と表示されます。

例

次の例は、Storage Virtual Machine（SVM）vs1でGPOサポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

関連情報

サポートされているGPOについて学ぶ

GPOのサーバ要件

SMBサーバ上のGPOの更新について学ぶ

SMBサーバのGPO設定を手動で更新する

GPO設定に関する情報の表示

SMBサーバでのGPOの更新方法

ONTAP SMBサーバ上のGPOの更新について学ぶ

デフォルトでは、ONTAPはグループ ポリシー オブジェクト（GPO）の変更を90分に1回取得して適用します。セキュリティ設定は16時間に1回更新されます。ONTAPで自動的に更新される前にGPOを更新し、新しいGPOポリシー設定を適用するには、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーします。

- デフォルトで、すべてのGPOを90分に1回確認し、必要に応じて更新。

  この間隔は構成可能であり、 `Refresh interval`および `Random offset` GPO 設定を使用して設定できます。

  ONTAPは、GPOの変更がないかどうかをActive Directoryに照会します。Active Directoryに記録されているGPOのバージョン番号がCIFSサーバ上のGPOのバージョン番号より大きい場合、ONTAPは新しいGPOを取得して適用します。バージョン番号が同じ場合、CIFSサーバ上のGPOは更新されません。

- セキュリティ設定のGPOを16時間に1回更新。

  ONTAPは、変更の有無にかかわらず、16時間に1回セキュリティ設定のGPOを取得して適用します。

  > デフォルト値の16時間は、現在のONTAPバージョンでは変更できません。これはWindowsクライアントのデフォルト設定です。

- ONTAPコマンドを使用して手動ですべてのGPOを更新。

  このコマンドは、Windows の `gpupdate.exe`/force`コマンドをシミュレートします。

関連情報

SMBサーバのGPO設定を手動で更新する

ONTAP SMBサーバのGPO設定を手動で更新する

CIFSサーバのグループ ポリシー オブジェクト（GPO）設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

手順

1. 適切な処理を実行します。

アップデートしたい場合...	コマンドを入力してください...
変更したGPO設定	`vserver cifs group-policy update -vserver vserver_name`
すべてのGPO設定	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

関連情報

SMBサーバ上のGPOの更新について学ぶ

ONTAP SMB GPO 構成に関する情報を表示する

Active Directoryで定義されているグループ ポリシー オブジェクト（GPO）設定およびCIFSサーバに適用されているGPO設定に関する情報を表示できます。

タスク概要

CIFSサーバが属しているドメインのActive Directoryで定義されているすべてのGPO設定に関する情報を表示できます。また、CIFSサーバに適用されているGPO設定に関する情報のみを表示することもできます。

手順

1. 次のいずれかの操作を実行し、GPO設定に関する情報を表示します。

すべてのグループ ポリシー設定に関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy show-defined -vserver vserver_name`
CIFS対応のStorage Virtual Machine（SVM）に適用されている	`vserver cifs group-policy show-applied -vserver vserver_name`

例

次の例は、FlexVolを備えたCIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
```

```
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

次の例は、CIFS対応のSVM vs1に適用されているGPO設定を表示します。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
------------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

```
    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

関連情報

サーバー上の GPO サポートを有効または無効にする

ONTAP SMB 制限グループ GPO に関する情報を表示する

Active Directoryでグループ ポリシー オブジェクト（GPO）として定義されている制限されたグループ、およびCIFSサーバに適用されている制限されたグループに関する詳細情報を表示できます。

タスク概要

デフォルトでは、次の情報が表示されます。

- グループ ポリシー名
- グループ ポリシー バージョン
- リンク

  グループ ポリシーが設定されているレベルを示します。次の値が出力されます。

  - `Local`グループ ポリシーが ONTAP で設定されている場合
  - `Site`グループ ポリシーがドメイン コントローラのサイト レベルで設定されている場合
  - `Domain`ドメイン コントローラでドメイン レベルでグループ ポリシーが設定されている場合
  - `OrganizationalUnit`グループ ポリシーがドメイン コントローラの組織単位（OU）レベルで設定されている場合
  - `RSOP`さまざまなレベルで定義されたすべてのグループ ポリシーから派生したポリシーの結果セット
- 制限されたグループ名
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ
- 制限されたグループが追加されているグループの一覧

  グループは、このリストのグループ以外のグループのメンバーになることもできます。

手順

1. 次のいずれかの操作を実行し、制限されたグループのすべてのGPOに関する情報を表示します。

すべての制限されたグループ **GPO** に関する情報を表示する場合：	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサーバに適用されている	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryドメインで定義されている、制限された

グループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

次の例は、CIFS対応のSVM vs1に適用されている、制限されたグループのGPOに関する情報を表示します。

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

関連情報

ONTAP SMB集中アクセスポリシーに関する情報を表示する

Active Directoryで定義されている集約型アクセス ポリシーに関する詳細情報を表示できます。また、グループ ポリシー オブジェクト（GPO）を介してCIFSサーバに適用されている集約型アクセス ポリシーに関する情報も表示できます。

タスク概要

デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ポリシーの名前
- SID
- 概要
- 作成日時
- 更新日時
- メンバー ルール

ワークグループ モードのCIFSサーバについては、GPOをサポートしていないため情報は表示されません。

手順

1. 次のいずれかの操作を実行し、集約型アクセス ポリシーに関する情報を表示します。

すべての集中アクセス ポリシーに関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
CIFSサーバに適用されている	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

例

次の例は、Active Directoryで定義されているすべての集約型アクセス ポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されているすべての集約型アクセス ポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                   SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- GPO設定に関する情報の表示
- 集約型アクセス ポリシー ルールに関する情報の表示

ONTAP SMB集中アクセスポリシールールに関する情報を表示する

Active Directoryで定義されている集約型アクセス ポリシーに関連付けられた集約型アクセス ポリシー ルールに関する詳細情報を表示できます。また、集約型アクセス ポリシーのGPO（グループ ポリシー オブジェクト）を介してCIFSサーバに適用されている集約型アクセス ポリシー ルールに関する情報も表示できます。

タスク概要

定義されているか適用されている集約型アクセス ポリシー ルールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ルールの名前
- 概要
- 作成日時
- 更新日時
- 現在の権限
- 推奨される権限
- ターゲット リソース

集約型アクセス ポリシーに関連付けられているすべての集約型アクセス ポリシー ルールに関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサーバに適用されている	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

例

次の例は、Active Directoryで定義されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例は、クラスタ上でStorage Virtual Machine（SVM）に適用されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- GPO設定に関する情報の表示
- 集約型アクセス ポリシーに関する情報の表示

ONTAPコマンドでSMBサーバコンピュータアカウントのパスワードを管理する

パスワードの変更、リセット、無効化、および自動更新スケジュールの設定に使用するコマンドについて説明します。また、パスワードを自動的に更新するようにSMBサーバでスケジュールを設定することもできます。

状況	使用するコマンド
ONTAPがADサービスと同期しているときにドメインアカウントのパスワードを変更する	`vserver cifs domain password change`
ONTAPがADサービスと同期されていない場合にドメインアカウントのパスワードをリセットする	`vserver cifs domain password reset`
SMBサーバにコンピュータ アカウント パスワードの自動変更を設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
SMBサーバのコンピュータ アカウント パスワードの自動変更を無効にする	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

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

ドメイン コントローラ接続の管理

ONTAP SMB検出サーバに関する情報を表示する

CIFSサーバで検出されたLDAPサーバおよびドメイン コントローラに関する情報を表示できます。

手順

1. 検出されたサーバーに関連する情報を表示するには、次のコマンドを入力します： `vserver cifs domain discovered-servers show`

例

次の例は、SVM vs1で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

- サーバのリセットと再検出
- サーバーの停止または起動

ONTAP SMBサーバをリセットして再検出する

CIFSサーバでサーバをリセットおよび再検出すると、CIFSサーバは、LDAPサーバおよびドメイン コントローラに関して保存されている情報を破棄します。サーバの情報を破棄したあと、CIFSサーバはそれらの外部サーバに関する最新の情報を再取得します。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します： `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 新しく再検出されたサーバーに関する情報を表示します `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

例

次の例は、Storage Virtual Machine（SVM、旧Vserver）vs1のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

関連情報

- 検出されたサーバに関する情報の表示
- サーバーの停止または起動

ONTAP SMB ドメイン コントローラ検出を管理する

ONTAP 9.3以降では、ドメイン コントローラ（DC）の検出に使用するデフォルト プロセスを変更できます。ローカル サイトまたは優先DCのプールに検出対象を制限できるため、環境によってはパフォーマンスの向上につながります。

タスク概要

デフォルトでは、動的な検出プロセスによって、使用可能なすべてのDC（優先DCを含む）、ローカル サイト内のすべてのDC、およびすべてのリモートDCが検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用するDCのプールが決まっている場合、またはリモートDCが不適切またはアクセスできない場合、検出方法を変更することができます。

ONTAP 9.3 以降のリリースでは、 `cifs domain discovered-servers`コマンドの `discovery-mode`パラメータを使用して、次のいずれかの検出オプションを選択できます：

- ドメイン内のすべてのDCを検出します。
- ローカル サイト内のDCだけを検出します。

  SMB サーバーの `default-site`パラメータは、sites-and-services 内のサイトに割り当てられていない LIF でこのモードを使用するように定義できます。

- サーバの検出は実行せず、優先DCのみを使用するようにSMBサーバを設定します。

  このモードを使用するには、最初にSMBサーバに対して優先DCを定義する必要があります。

開始する前に

advanced権限レベルが必要です。

手順

1. 必要な検出オプションを指定します： `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

`mode`パラメータのオプション：

- `all`

  使用可能なすべてのDCを検出します（デフォルト）。

- `site`

  DCの検出対象をサイトに制限します。

- `none`

  優先DCのみを使用し、検出は実行しません。

優先 ONTAP SMB ドメイン コントローラを追加する

ONTAPでは、DNSを介してドメイン コントローラが自動的に検出されます。必要に応じて、特定のドメインに対する優先ドメイン コントローラのリストにドメイン コントローラを追加することができます。

タスク概要

優先ドメイン コントローラ リストがすでに特定のドメインに存在する場合、新しいリストが既存のリストに統合されます。

手順

1. 優先ドメイン コントローラのリストに追加するには、次のコマンドを入力します：+ `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred -dc IP_address, …+`

   `-vserver vserver_name`ストレージ仮想マシン（SVM）名を指定します。

   `-domain domain_name` 指定されたドメイン コントローラが属するドメインの完全修飾 Active Directory 名を指定します。

   `-preferred-dc IP_address,...` は、優先ドメイン コントローラの 1 つ以上の IP アドレスを、優先順位に従ってコンマ区切りのリストとして指定します。

例

次のコマンドは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを確立するために使用する優先ドメイン コントローラのリストに、ドメイン コントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先されるドメイン コントローラの管理用コマンド

優先SMBドメインコントローラを管理するためのONTAPコマンド

優先ドメイン コントローラを追加、表示、削除するコマンドについて説明します。

状況	使用するコマンド
優先ドメイン コントローラを追加する	`vserver cifs domain preferred-dc add`
優先ドメイン コントローラを表示する	`vserver cifs domain preferred-dc show`
優先ドメイン コントローラを削除する	`vserver cifs domain preferred-dc remove`

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

関連情報

優先ドメイン コントローラの追加

ONTAP SMBドメイン コントローラへの暗号化接続を有効にする

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ことができます。

タスク概要

ONTAPでは、 `-encryption-required-for-dc-connection`オプションが `true`に設定されている場合、ドメイン コントローラ（DC）通信の暗号化が必要です。デフォルトは `false`です。このオプションが設定されている場合、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。

暗号化されたDC通信が必要な場合、ONTAPはSMB3接続のみをネゴシエートするため、 `-smb2-enabled-for-dc-connections`オプションは無視されます。DCがSMB3と暗号化をサポートしていない場合、ONTAPは接続しません。

手順

1. DC 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`

非Kerberos環境でストレージにアクセスするためのnullセッションの使用

ONTAP SMB nullセッションを使用して、非**Kerberos**環境でストレージにアクセスします。

ヌル セッション アクセスは、ストレージ システム データなどのネットワーク リソースや、ローカル システムで実行されるクライアント ベースのサービスに対する権限を提供します。ヌル セッションは、クライアント プロセスが「system」アカウントを使用してネットワーク リソースにアクセスしたときに発生します。ヌル セッション設定は、Kerberos 以外の認証に固有です。

ONTAP SMB ストレージ システムがヌル セッション アクセスを提供する仕組みを学びます

nullセッション共有には認証が必要ないため、nullセッション アクセスが必要なクライアントはそのIPアドレスがストレージ システムにマッピングされている必要があります。

デフォルトでは、マッピングされていないnullセッション クライアントは、共有の列挙など一部のONTAPシステム サービスにはアクセスできますが、ストレージ システム データへのアクセスは制限されます。

> ONTAPは、 `-restrict-anonymous`オプションを使用して`Windows RestrictAnonymous`レジストリ設定値をサポートしています。これにより、マッピングされていない`null`ユーザがシステム リソースを表示またはアクセスできる範囲を制御できます。たとえば、共有の列挙と`IPC$`共有（非表示の名前付きパイプ共有）へのアクセスを無効にできます。 `vserver cifs options modify`、 `vserver cifs options show`、および `–restrict-anonymous`オプションの詳細については、"ONTAPコマンド リファレンス"を参照してください。

別途設定がない限り、ヌル セッションを介してストレージ システムへのアクセスを要求するローカル プロセスを実行しているクライアントは、「everyone」などの非制限グループのメンバーとしてのみ機能します。ヌル セッションへのアクセスを特定のストレージ システム リソースに制限するには、すべてのヌル セッション クライアントが属するグループを作成することをお勧めします。このグループを作成することで、ストレージ システムへのアクセスを制限し、ヌル セッション クライアントにのみ適用されるストレージ システム リソースの権限を設定できます。

ONTAPは、 `vserver name-mapping`コマンドセットにマッピング構文を提供し、nullユーザセッションを使用してストレージシステムリソースへのアクセスを許可するクライアントのIPアドレスを指定します。nullユーザのグループを作成した後、ストレージシステムリソースへのアクセス制限と、nullセッションにのみ適用されるリソース権限を指定できます。nullユーザは匿名ログオンとして識別されます。nullユーザはどのホームディレクトリにもアクセスできません。

マッピングされたIPアドレスからストレージシステムにアクセスするヌルユーザーには、マッピングされたユーザー権限が付与されます。ヌルユーザーがマッピングされたストレージシステムへの不正アクセスを防ぐため、適切な予防措置を講じてください。最大限の保護を実現するには、ストレージシステムとヌルユーザーによるストレージシステムアクセスを必要とするすべてのクライアントを別のネットワークに配置し、IPアドレスの「spoofing」の可能性を排除してください。

関連情報

ONTAP SMBファイルシステム共有へのアクセス権をNULLユーザーに付与する

nullセッション クライアントによるストレージ システム リソースへのアクセスを許可するには、nullセッション クライアントにグループを割り当てて、nullセッション クライアントのIPアドレスを記録し、ストレージ システム上の、nullセッションを使用したデータ アクセスを許可するクライアント リストにそのIPアドレスを追加します。

手順

1. `vserver name-mapping create`コマンドを使用して、IP修飾子を使用して、nullユーザを任意の有効なWindowsユーザにマッピングします。

   次のコマンドは、有効なホスト名 google.com を持つ user1 に null ユーザーをマッピングします：

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   次のコマンドは、null ユーザーを有効な IP アドレス 10.238.2.54/32 を持つ user1 にマッピングします：

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. `vserver name-mapping show`コマンドを使用して名前のマッピングを確認します。

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1        -                10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. `vserver cifs options modify –win-name-for-null-user`コマンドを使用して、Windowsメンバーシップをnullユーザーに割り当てます。

   このオプションは、null ユーザに有効な名前マッピングがある場合にのみ適用されます。

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. `vserver cifs options show`コマンドを使用して、nullユーザとWindowsユーザまたはグループのマッピングを確認します。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

SMBサーバ用のNetBIOSエイリアスの管理

ONTAP SMBサーバのNetBIOSエイリアスの管理について学習します

NetBIOSエイリアスはSMBサーバの別名で、SMBクライアントがSMBサーバに接続する際に使用できます。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サーバに統合した場合に、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ことができます。

SMBサーバの作成時、または作成後いつでも、NetBIOSエイリアスのリストを指定できます。リストにはいつでもNetBIOSエイリアスを追加または削除できます。SMBサーバにはNetBIOSエイリアス リスト内のどの名前を使用しても接続できます。

関連情報

NetBIOS over TCP接続に関する情報の表示

ONTAP SMBサーバーにNetBIOSエイリアスリストを追加する

エイリアスを使用してSMBクライアントをSMBサーバに接続する場合、NetBIOSエイリアスのリストを作成するか、NetBIOSエイリアスの既存のリストにNetBIOSエイリアスを追加します。

タスク概要

- NetBIOSエイリアス名は15文字以内にする必要があります。
- SMBサーバには最大200個までのNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

手順

1. NetBIOSエイリアスを追加します：+ `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - カンマ区切りのリストを使用して、1つ以上のNetBIOSエイリアスを指定できます。
   - 指定された NetBIOS エイリアスが既存のリストに追加されます。

◦ 現在のリストが空である場合、NetBIOSエイリアスの新しいリストが作成されます。

2. NetBIOS エイリアスが正しく追加されたことを確認します： `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

関連情報

- SMBサーバーのリストからNetBIOSエイリアスを削除します
- SMBサーバーのNetBIOSエイリアスリストを表示する

ONTAP SMBサーバーのリストからNetBIOSエイリアスを削除します

CIFSサーバーに特定のNetBIOSエイリアスが必要ない場合は、リストからそれらのNetBIOSエイリアスを削除できます。また、リストからすべてのNetBIOSエイリアスを削除することもできます。

タスク概要

カンマ区切りのリストを使用して、複数のNetBIOSエイリアスを削除できます。 `-netbios-aliases`パラメータの値として `-`を指定することで、CIFSサーバー上のすべてのNetBIOSエイリアスを削除できます。

手順

1. 次のいずれかを実行します。

削除したい場合...	入力する内容
リストからの特定のNetBIOSエイリアス	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
リスト内のすべてのNetBIOSエイリアス	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 指定されたNetBIOSエイリアスが削除されたことを確認します： `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_2, ALIAS_3
```

ONTAP SMBサーバのNetBIOSエイリアス リストを表示する

NetBIOSエイリアスのリストを表示できます。これは、SMBクライアントがCIFSサーバへの接続に使用できる名前を確認するときに役立ちます。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合は	入力する内容
CIFSサーバのNetBIOSエイリアス	`vserver cifs show -display-netbios -aliases`
NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報	`vserver cifs show -instance`

次の例は、CIFSサーバのNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例は、NetBIOSエイリアスのリストを含む詳細なCIFSサーバ情報を表示します。

```
vserver cifs show -instance
```

```
                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    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: ALIAS_1, ALIAS_2,
ALIAS_3
```

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

関連情報

- NetBIOS エイリアス リストをサーバに追加する
- サーバを管理するためのコマンド

ONTAP SMBクライアントがNetBIOSエイリアスを使用して接続されているかどうかを確認する

SMBクライアントがNetBIOSエイリアスを使用して接続しているかどうか、また使用されている場合はどのNetBIOSエイリアスが接続に使用されているかを確認できます。これは、接続に関する問題のトラブルシューティングに役立ちます。

タスク概要

SMB接続に関連付けられたNetBIOSエイリアス（存在する場合）を表示するには、 `-instance`パラメータを使用する必要があります。CIFSサーバー名またはIPアドレスを使用してSMB接続を確立した場合、`NetBIOS Name`フィールドの出力は `-（ハイフン）になります。

手順

1. 次のうち必要な操作を実行します。

NetBIOS 情報を表示する場合：	入力する内容
SMB 接続	`vserver cifs session show -instance`
指定された NetBIOS エイリアスを使用した接続：	`vserver cifs session show -instance -netbios-name` *netbios_name*

次の例は、セッションID 1のSMB接続に使用されているNetBIOSエイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

SMBサーバに関するその他のタスクの管理

ONTAP SMBサーバを停止または起動する

ユーザがSMB共有を介してデータにアクセスしていない間に作業を行う場合は、SVM上のCIFSサーバを停止すると便利です。SMBアクセスを再開するときは、CIFSサーバを起動します。CIFSサーバを停止することによって、Storage Virtual Machine（SVM）で許可されているプロトコルを変更できます。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
CIFSサーバを停止する	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFSサーバを起動する
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground`コマンドをフォアグラウンドで実行するかバックグラウンドで実行するかを指定します。このパラメータを入力しない場合は `true`に設定され、コマンドはフォアグラウンドで実行されます。

2. `vserver cifs show`コマンドを使用して、CIFSサーバーの管理ステータスが正しいことを確認します。

例

次のコマンドは、SVM vs1のCIFSサーバを起動します。

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

関連情報

- 検出されたサーバに関する情報の表示
- サーバのリセットと再検出

ONTAP SMBサーバーを別のOUに移動する

CIFSサーバのcreateプロセスでは、別の組織単位（OU）を指定しないかぎり、セットアップ時のデフォルトのOUであるCN=Computersが使用されます。CIFSサーバはセットアップ後でも別のOUに移動できます。

手順

1. Windows サーバーで、**Active Directory** ユーザーとコンピューター ツリーを開きます。
2. Storage Virtual Machine（SVM）のActive Directoryオブジェクトを見つけます。
3. オブジェクトを右クリックし、*移動*を選択します。
4. SVMに関連付けるOUを選択します。

結果

選択したOUに、SVMオブジェクトが移動します。

ONTAP SMBサーバを移動する前にダイナミックDNSドメインを変更する

SMBサーバを別のドメインに移動する際に、SMBサーバのDNSレコードがActive Directoryに統合されたDNSサーバによってDNSに動的に登録されるようにするには、SMBサーバを移動する前にStorage Virtual Machine（SVM）上の動的DNS（DDNS

）を変更する必要があります。

開始する前に

新しいドメイン（SMBサーバ コンピュータ アカウントの移動先）のサービス ロケーション レコードを含むDNSドメインを使用するよう、SVM上のDNSネーム サービスを変更する必要があります。セキュアDDNSを使用している場合は、Active Directoryに統合されたDNSネーム サーバを使用する必要があります。

タスク概要

DDNS（SVM上で設定されている場合）はデータLIFのDNSレコードを新しいドメインに自動的に追加しますが、元のドメインのDNSレコードは元のDNSサーバから自動的には削除されません。手動で削除する必要があります。

SMBサーバを移動する前にDDNSの変更を完了するには、次のトピックを参照してください。

"ダイナミック DNS サービスを構成する"

ONTAP SMB SVMをActive Directoryドメインに参加させる

`vserver cifs modify`コマンドを使用してドメインを変更することで、既存のSMBサーバを削除せずに、Storage Virtual Machine（SVM）をActive Directoryドメインに参加させることができます。現在のドメインに再参加することも、新しいドメインに参加することもできます。

開始する前に

- SVM にはすでに DNS 構成が存在している必要があります。
- SVM の DNS 構成は、ターゲット ドメインに対応できる必要があります。

  DNSサーバに、ドメインLDAPおよびドメイン コントローラ サーバのサービス ロケーション レコード（SRV）が格納されている必要があります。

タスク概要

- Active Directoryドメインの変更を続行するには、CIFSサーバーの管理ステータスを `down`に設定する必要があります。
- コマンドが正常に完了すると、管理ステータスは自動的に `up`に設定されます。"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。
- ドメインに参加する場合、このコマンドが完了するまでに数分かかることがあります。

手順

1. SVMをCIFSサーバ ドメインに参加させます。 `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

`vserver cifs modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-modify.html["ONTAPコマンド リファレンス"^]を参照してください。新しいドメインのDNSを再設定する必要がある場合は、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+dns+modify["ONTAPコマンド リファレンス"^]の`vserver dns modify`の詳細を参照してください。

SMBサーバのActive Directoryマシン アカウントを作成するには、 *example*.comドメイン内の `ou=*example* ou`コンテナにコンピュータを追加するための十分な権限を持つWindowsアカウントの名前とパスワードを指定する必要があります。

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。

2. CIFSサーバが目的のActive Directoryドメイン内にあることを確認します： `vserver cifs show`

例

次の例では、SVM vs1上のSMBサーバ「CIFSSERVER1」が、keytab認証を使用してexample.comドメインに参加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

ONTAP SMB NetBIOS over TCP接続に関する情報を表示します。

NetBIOS over TCP（NBT）接続に関する情報を表示できます。この情報は、NetBIOSに関連する問題のトラブルシューティングに役立ちます。

手順

1. `vserver cifs nbtstat`コマンドを使用して、NetBIOS over TCP 接続に関する情報を表示します。

IPv6経由のNetBIOSネーム サービス（NBNS）はサポートされていません。

例

次の例は、「cluster1」に表示される NetBIOS ネーム サービス情報を示しています：

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1           00               wins          58
         CLUSTER_1           20               wins          58
         4 entries were displayed.
```

SMBサーバーを管理するためのONTAPコマンド

SMBサーバを作成、表示、変更、停止、開始、削除するコマンドについて説明します。また、サーバのリセットと再検出、マシン アカウント パスワードの変更またはリセット、マシン アカウント パスワードのスケジュール変更、NetBIOSエイリアスの追加や削除を行うコマンドもあります。

状況	使用するコマンド
SMBサーバーを作成する	`vserver cifs create`
SMBサーバに関する情報を表示する	`vserver cifs show`
SMBサーバを変更する	`vserver cifs modify`
SMBサーバを別のドメインに移動する	`vserver cifs modify`

SMBサーバを停止する	`vserver cifs stop`
SMBサーバを起動する	`vserver cifs start`
SMBサーバを削除する	`vserver cifs delete`
SMBサーバ用にサーバをリセットおよび再検出する	`vserver cifs domain discovered-servers reset-servers`
SMBサーバのマシン アカウント パスワードを変更する	`vserver cifs domain password change`
SMBサーバのマシン アカウント パスワードをリセットする	`vserver cifs domain password change`
SMBサーバのマシン アカウントの自動パスワード変更をスケジュールする	`vserver cifs domain password schedule modify`
SMBサーバ用のNetBIOSエイリアスを追加する	`vserver cifs add-netbios-aliases`
SMBサーバ用のNetBIOSエイリアスを削除する	`vserver cifs remove-netbios-aliases`

`vserver cifs`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"^]をご覧ください。

関連情報

"SMBサーバを削除したときにローカル ユーザとローカル グループが受ける影響"

ONTAP SMB NetBios ネーム サービスを有効にする

ONTAP 9以降では、NetBiosネーム サービス（NBNS、Windows Internet Name Service [WINS]とも呼ばれる）がデフォルトで無効になります。以前のリリースでは、WINSがネットワークで有効かどうかに関係なく、CIFS対応Storage Virtual Machine（SVM）が名前登録のブロードキャストを送信していました。NBNSが必須の構成でのみこのブロードキャストが送信されるようにするには、新しいCIFSサーバに対してNBNSを明示的に有効にする必要があります。

開始する前に

- すでにNBNSを使用しているシステムをONTAP 9にアップグレードした場合、このタスクを実行する必要はありません。NBNSはそれまでと同様に機能します。
- NBNSはUDP（ポート137）経由で有効になります。
- IPv6経由のNBNSはサポートされていません。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. CIFSサーバでNBNSを有効にします。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. admin権限レベルに戻ります。

```
set -privilege admin
```

SMBアクセスとSMBサービスでのIPv6の使用

ONTAP の IPv6 に関する SMB 要件について学ぶ

SMBサーバでIPv6を使用する前に、この機能をサポートするONTAPおよびSMBのバージョンとライセンスの要件について確認しておく必要があります。

ONTAPのライセンス要件

SMBライセンスがある場合、IPv6に特別なライセンスは必要ありません。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プロトコルのバージョン

- SVMについては、すべてのバージョンのSMBプロトコルでIPv6がサポートされます。

IPv6経由のNetBIOSネーム サービス（NBNS）はサポートされていません。

ONTAP SMBアクセスおよびCIFSサービスによるIPv6のサポートについて学習します

CIFSサーバ上でIPv6を使用する場合は、ONTAPによるSMBアクセスやCIFSサービスとのネットワーク通信でのIPv6のサポートについて確認しておく必要があります。

Windowsクライアントおよびサーバのサポート

ONTAPでは、IPv6をサポートするWindowsサーバおよびクライアントをサポートしています。Microsoft Windowsクライアントおよびサーバによる IPv6のサポートは次のとおりです。

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012、およびそれ以降のリリースでは、SMBファイル共有とActive Directoryサービス（DNS、LDAP、CLDAP、Kerberosなどのサービス）の両方でIPv6がサポートされます。

  IPv6アドレスが設定されている場合、Windows 7、Windows Server 2008、およびそれ以降のリリースでは、Active Directoryサービスに対してデフォルトでIPv6が使用されます。IPv6接続によるNTLM認証とKerberos認証の両方がサポートされます。

  ONTAPでサポートされるWindowsクライアントでは、いずれもIPv6アドレスを使用してSMB共有にアクセスできます。

ONTAPがサポートするWindowsクライアントの最新情報については、"Interoperability Matrix"を参照してください。

NTドメインはIPv6ではサポートされません。

その他の**CIFS**サービスのサポート

ONTAPでは、SMBファイル共有とActive Directoryサービスに加え、以下に対してもIPv6をサポートしています。

- クライアント側のサービス：オフライン フォルダ、移動プロファイル、フォルダ リダイレクト、以前のバージョン機能など
- サーバ側のサービス：動的ホーム ディレクトリの有効化（ホーム ディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODXコピー オフロード、自動ノード リファーラル、以前のバージョン機能など
- ファイル アクセス管理用のサービス：Windowsのローカル ユーザやローカル グループを使用したアクセス制御と権限の管理、CLIを使用したファイル権限や監査ポリシーの設定、セキュリティ トレース、ファイル ロックの管理、SMBアクティビティの監視など
- NASのマルチプロトコルの監査
- FPolicy
- 共有の継続的な可用性、監視プロトコル、およびリモートVSS（Hyper-V over SMB構成で使用）

ネーム サービスと認証サービスのサポート

次のネーム サービスを使用した通信がIPv6でサポートされます。

- ドメイン コントローラ
- DNSサーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

ONTAP SMBサーバがIPv6を使用して外部サーバに接続する方法を学びます

要件に対応した設定を作成するためには、CIFSサーバから外部サーバへの接続時にIPv6

がどのように使用されるかを理解しておく必要があります。

- 送信元アドレスの選択

  外部サーバへの接続では、送信元アドレスに接続先アドレスと同じタイプのアドレスを選択する必要があります。たとえば、IPv6アドレスに接続する場合、CIFSサーバをホストするStorage Virtual Machine（SVM）には、送信元アドレスとして使用するIPv6アドレスが割り当てられたデータLIFまたは管理LIFが必要です。同様に、IPv4アドレスに接続する場合、SVMには、送信元アドレスとして使用するIPv4アドレスが割り当てられたデータLIFまたは管理LIFが必要です。

- DNSを使用して動的に検出されるサーバの場合、サーバ検出は次のように実行されます。
  - クラスターでIPv6が無効になっている場合は、IPv4サーバ アドレスのみが検出されます。
  - クラスタでIPv6が有効になっている場合、IPv4とIPv6の両方のサーバアドレスが検出されます。アドレスが属するサーバの適合性と、IPv6またはIPv4のデータLIFまたは管理LIFの可用性に応じて、どちらかのタイプが使用される場合があります。動的サーバ検出は、ドメインコントローラと、LSA、NETLOGON、Kerberos、LDAPなどの関連サービスを検出するために使用されます。

- DNSサーバへの接続

  SVMがDNSサーバに接続するときにIPv6を使用するかどうかは、DNSネーム サービスの設定によって決まります。IPv6アドレスを使用するようにDNSサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要な場合はDNSサーバへの接続に引き続きIPv4アドレスが使用されるよう、DNSネーム サービスの設定でIPv4アドレスを使用できます。DNSネーム サービスの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

- LDAPサーバへの接続

  SVMがLDAPサーバに接続するときにIPv6を使用するかどうかは、LDAPクライアントの設定によって決まります。IPv6アドレスを使用するようにLDAPクライアントが設定されている場合は、IPv6を使用して接続が確立されます。必要な場合は、LDAPサーバへの接続に引き続きIPv4アドレスが使用されるよう、LDAPクライアントの設定でIPv4アドレスを使用できます。LDAPクライアントの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  > LDAPクライアントの設定は、UNIXユーザ、グループ、およびネットグループのネーム サービス用にLDAPを設定するときに使用されます。

- NISサーバへの接続

  SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネーム サービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要な場合はNISサーバへの接続に引き続きIPv4アドレスが使用されるよう、NISネーム サービスの設定でIPv4アドレスを使用できます。NISネーム サービスの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。

  > NISネーム サービスは、UNIXユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

関連情報

- サーバーのIPv6を有効にする
- IPv6セッションに関する情報を監視および表示する

ONTAP SMBサーバでIPv6を有効にする

IPv6ネットワークはクラスタのセットアップ時には有効になりません。SMBでIPv6を使用するには、クラスタのセットアップ後にクラスタ管理者がIPv6を有効にする必要があります。クラスタ管理者がIPv6を有効にすると、IPv6はクラスタ全体で有効になります。

手順

1. IPv6を有効にする： `network options ipv6 modify -enabled true`

   IPv6が有効になります。SMBアクセス用のIPv6データLIFを設定できます。

関連情報

- IPv6セッションに関する情報を監視および表示する
- "System Managerを使用してネットワークを視覚化する"
- "クラスタでIPv6を有効にする"
- "network options ipv6 modify"

ONTAP SMBサーバのIPv6を無効にする方法について

クラスタでIPv6を有効にするにはネットワーク オプションを使用しますが、同じコマンドを使用してSMBでのIPv6を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後にIPv6を有効にしたインターフェイスを無効にすると、IPv6は無効になります。IPv6を有効にしたインターフェイスの管理については、クラスタ管理者と連絡を取り合う必要があります。

関連情報

- "System Manager を使用して ONTAP ネットワークを視覚化する"

IPv6 ONTAP SMBセッションに関する情報を監視および表示する

IPv6ネットワークで接続されているSMBセッション情報を監視および表示できます。IPv6 SMBセッションに関する情報を確認できる以外にも、IPv6を使用して接続しているクライアントを特定するのに役立ちます。

手順

1. 次のうち必要な操作を実行します。

...かどうかを判断したい場合	コマンドを入力してください...
Storage Virtual Machine（SVM）へのSMBセッションがIPv6を使用して接続しているかどうか	`vserver cifs session show -vserver` *`vserver_name`* `-instance`

...かどうかを判断したい場合	コマンドを入力してください...
指定したLIFアドレスのSMBセッションでIPv6を使用しているかどうか	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* は、データ LIF の IPv6 アドレスです。

著作権に関する情報

商標に関する情報