SMB サーバを管理します

ONTAP 9

NetApp
April 24, 2024

目次

SMB サーバを管理します

SMB サーバを変更

を使用して、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 SMBサーバを移動できます `vserver cifs modify` コマンドを実行します

このタスクについて

SMB サーバ名や管理ステータスなど、 SMB サーバのその他の属性を変更することもできます。詳細については、のマニュアルページを参照してください。

選択肢

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。

  a. SMBサーバの管理ステータスをに設定します `down`。

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

  b. ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。 `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

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

  SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限がある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 `ou=`*`example`* `ou` 内のコンテナ *`example`*.comドメイン。

  ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

- ワークグループから別のワークグループに SMB サーバを移動します。

  a. SMBサーバの管理ステータスをに設定します `down`。

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

  b. SMBサーバ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
  ```

- Active Directory ドメインからワークグループに SMB サーバを移動するには、次の手順を実行します。
  a. SMBサーバの管理ステータスをに設定します `down`。

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

  b. Active Directoryドメインからワークグループに SMBサーバを移動します。 `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切り替えるには、継続的可用性を備えた共有、シャドウコピー、 AES など、ドメインベースの機能をすべて無効にし、該当する設定がシステムによって自動的に削除されるようにする必要があります。ただし、「 EXAMPLE.COM\userName" 」などのドメインで設定された共有 ACL は正しく機能しませんが、 ONTAP で削除することはできません。このような共有 ACL は、コマンドの完了後できるだけ早く外部ツールを使用して削除してください。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ことがあります。

  - の該当するパラメータを使用して、他の属性を変更します `vserver cifs modify` コマンドを実行します

オプションを使用した**SMB**サーバのカスタマイズ

使用できる **SMB** サーバオプション

SMB サーバのカスタマイズ方法について検討する場合は、使用できるオプションを把握しておくと便利です。一部のオプションは汎用的なものですが、 SMB の特定の機能を有効にして設定するためのオプションも複数あります。SMBサーバオプションは、で制御します `vserver cifs options modify` オプション

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 セッションが切断されるまでのアイドル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 ユーザーの構成 *

  このオプションでは、 SMB サーバで使用されるデフォルトの UNIX ユーザを指定できます。ONTAP はデフォルトユーザ「 pcuser 」（ UID は 65534 ）を自動的に作成し、グループ「 pcuser 」（ GID は 65534 ）を作成して、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 は自動的に「 pcuser 」をデフォルトの UNIX ユーザとして設定します。

- * ゲスト UNIX ユーザの設定 *

  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権限付与の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、デフォルトでは無効になっています。

- * NFS クライアントからの読み取り専用ファイルの削除機能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、読み取り専用属性が設定されたファイルやフォルダの削除を NFS クライアントに許可するかどうかを指定できます。NTFS の削除では、読み取り専用属性が設定されたファイルやフォルダの削除は許可されません。UNIX の削除では読み取り専用ビットが無視され、ファイルやフォルダを削除できるかどうかは親ディレクトリの権限によって判断されます。デフォルト設定はです `disabled`これにより、NTFSの削除セマンティクスが発生します。

- * 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 ユーザーへの UNIX グループ権限の付与 *

  このオプションは、ファイルの所有者ではない CIFS ユーザにグループ権限を付与するかどうかを指定します。CIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `true`をクリックすると、ファイルに対するグループ権限が付与されます。`CIFS`ユーザが`UNIX`セキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `false`を指定すると、通常の`UNIX`ルールを適用してファイル権限が付与されます。このパラメータは、権限がに設定されている`UNIX`セキュリティ形式のファイルに適用されます `mode bits` セキュリティモードがNTFSまたはNFSv4のファイルには適用されません。デフォルト設定はです `false`。

- * 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、ネットアップ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、 ONTAP では 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 を有効または無効にします

  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 コピーオフロードの有効化または無効化 *

  ODX コピーオフロードは、対応する Windows クライアントで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 コピーオフロードの直接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、デフォルトでは無効になっています。

- * ジャンクションポイントのリパースポイントとしての使用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 サーバはジャンクションポイントをリパースポイントとして SMB クライアントに公開します。このオプションは、 SMB 2.x 接続または SMB 3.0 接続のみで有効です。このオプションはデフォルトで有効になっています。

  このオプションは SVM でのみサポートされます。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 接続ごとの最大同時操作数の設定 *

  デフォルト値は255です。

- * ローカルの Windows ユーザーとグループ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 シャドウ・コピー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 解決策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

- * シャドウ・コピーのディレクトリ階層の設定 *

  このオプションでは、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

- * マルチドメインネームマッピングの検索機能の有効化または無効化 *

  有効にすると、 UNIX ユーザが 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 Windows ドメインユーザにマッピングされている場合に（ * \joe など）、 ONTAP はホームドメインと双方向の信頼関係が確立されたすべてのドメインで、指定し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、優先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を実行するために優先リストが使用されます。

  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。

- * ファイルシステムセクターサイズの設定 *

  このオプションでは、 ONTAP から SMB クライアントに報告されるファイルシステムセクターサイズをバイト単位で設定できます。このオプションには2つの有効な値があります。 `4096` および `512`。デフォルト値はです `4096`。この値をに設定する必要がある場合があります `512` Windowsアプリケーションが512バイトのセクターサイズのみをサポートしている場合。

- * ダイナミックアクセス制御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（ restrict anonymous ） *

  このオプションでは、認証されていないセッションの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 対応のセキュリティを使用するボリューム（ UNIX セキュリティ形式のボリューム、または UNIX

対応のセキュリティを使用する mixed セキュリティ形式のボリューム）での NTFS ACL の提供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、 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 ONTAP 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 ONTAP 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 擬似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 OSX 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。

- * 略称を使用した検索のサポート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 サーバは短縮名に対して検索を実行できます。このオプションを有効にした場合の検索では、長いファイル名に加えて 8.3 形式のファイル名も照合されます。このパラメータのデフォルト値はです `false`。

- * DFS 対応の自動通知のサポート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、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以降ではを設定します `-max-credits` オプションを使用すると、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接続に付与す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 *

  を有効にします `-is-multichannel-enabled` ONTAP 9.4以降のリリースのオプションを使用すると、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に、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です `false`。

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。
- 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。このパラメータのデフォルト値は256です。

SMBサーバオプションの設定

SMBサーバオプションは、Storage Virtual Machine（SVM）でのSMBサーバの作成後にいつでも設定できます。

ステップ

1. 必要な操作を実行します。

SMBサーバオプションの設定	入力するコマンド
admin 権限レベルで設定します	`vserver cifs options modify -vserver` *`vserver_name options`*
advanced 権限レベルで設定します	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

SMBサーバオプションの設定の詳細については、のマニュアルページを参照してください `vserver cifs options modify` コマンドを実行します

SMBユーザへのUNIXグループ権限付与の設定

このオプションを使用すると、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する権限をグループに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必要に応じて設定します。

状況	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`

状況	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ようにします	`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`

匿名ユーザのアクセス制限を設定します

デフォルトでは、認証されていない匿名ユーザ（ _null ユーザ）はネットワーク上の特定の情報にアクセスできます。SMBサーバオプションを使用して、匿名ユーザに対するアクセス制限を設定できます。

このタスクについて

。 `-restrict-anonymous` SMBサーバオプションはに対応します `RestrictAnonymous` Windowsのレジストリエントリ。

匿名ユーザは、ユーザ名、詳細、アカウントポリシー、共有名など、ネットワーク上の Windows ホストから特定のタイプ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。

価値	説明
`no-restriction` （デフォルト）	匿名ユーザに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. restrict anonymousを設定します。 `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

使用できる SMB サーバオプション

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を管理します

UNIX セキュリティ形式のデータの概要で、ファイルセキュリティが **SMB** クライアントにどのように提供されるかを管理します

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。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

デフォルトでは、 ONTAP は、 UNIX セキュリティ形式のボリュームに対する UNIX アクセス権を NTFS ACL として SMB クライアントに提供します。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 アクセス権を表示および編集する。

  処理が UNIX システムで許可されていない場合、 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 システムではこの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。

- ユーザは、 Microsoft Office などの特定の Windows アプリケーションを使用して UNIX セキュリティ形式のボリューム上でファイルを編集および保存します。 ONTAP では、保存処理中に UNIX アクセス権を保持する必要があります。
- 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。

状況によっては、 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、 ONTAP は 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します。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 クライアントでのみ行うことができます。

  SMB クライアントで UNIX セキュリティ形式のボリュームがマッピングされている場合は、 Security タブを使用できません。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 がボリュームを FAT として報告する場合、アプリケーションは ACL の変更を試みません。

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に対する **NTFS ACL** の提供を有効または無効にします

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と UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）に対する NTFS ACL の SMB クライアントへの提供を有効または無効にできます。

このタスクについて

このオプションを有効にすると、 ONTAP は、 UNIX 対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダを NTFS ACL を使用するように SMB クライアントに提供します。このオプションを無効にした場合は、ボリュームが SMB クライアントに FAT ボリュームとして提供されます。デフォルトでは、NTFS ACL が SMB クライアントに提供されます。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. UNIX NTFS ACLオプションを設定します。 `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 による **UNIX** アクセス権の維持方法

UNIX アクセス権を現在持っている 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ても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、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から、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

Windows のセキュリティタブを使用して **UNIX** アクセス権を管理します

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 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、 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 アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式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。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式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したくない場合は、反映する範囲を希望の範囲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を管理します

ONTAP による SMB クライアント認証の処理

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つの認証方式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 モデルとは異なり、 SMB サーバなどの別のコンピュータとのセッションを確立する Active Directory クライアントは、直接 KDC にアクセスしてセッションのクレデンシャルを取得します。

NTLM認証

NTLM クライアント認証は、パスワードに基づく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接続を作成した場合、認証はSMBサーバによってNTLMv2を使用してローカルに行われます。

SVM ディザスタリカバリ構成での SMB サーバセキュリティ設定に関するガイドライン

IDが保持されない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（を参照） `-identity-preserve` オプションはに設定されています `false` （SnapMirror構成の場合）デスティネーションSVMでのSMBサーバセキュリティ設定の管理方法について理解しておく必要があります。

- デフォルト以外の 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。

  デスティネーション SVM 上に SMB サーバを作成した場合、すべての SMB 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。SVM のディザスタリカバリ先を初期化、更新、再同期した場合、ソース上の SMB サーバの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 サーバセキュリティ設定は手動で設定する必要があります。

  ソース SVM 上で SMB サーバセキュリティ設定をデフォルト以外にしている場合、デスティネーションが読み書き可能になったあと（ SnapMirror 関係が解除されたあと）にデスティネーション SVM 上で手動で同じ設定を行う必要があります。

SMBサーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine （ SVM ）上の SMB サーバ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正しいかどうかを確認する際に役立ちます。

このタスクについて

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。

を使用しないでください `vserver cifs security show` 一部のオプションが無効なため、ワークグループモードのSMBサーバに対してコマンドを実行します。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
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,...]` 入ることができます `-fields ?` 使用できるフィールドを決定します。

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 の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 設定に関する情報を表示します

ローカル **SMB** ユーザに対するパスワードの複雑さの要件を有効または無効にします

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。この機能は、いつでも無効にして再度有効にすることができます。

作業を開始する前に

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。

> このタスクについて
>
> を使用しないでください `vserver cifs security modify` 一部のオプションが無効なため、ワークグループモードのCIFSサーバに対してコマンドを実行します。

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	入力するコマンド
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. パスワードの複雑さの要件に関する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

CIFS サーバのセキュリティ設定に関する情報を表示する

ローカルユーザおよびローカルグループを使用した認証と許可

ローカルユーザパスワードの要件

ローカルユーザのアカウントパスワードを変更しています

CIFS サーバの Kerberos セキュリティ設定を変更します

Kerberos クロックスキュー時間の許容最大値、 Kerberos チケットの有効期間、チケットの更新日の最大数など、 CIFS サーバの Kerberos セキュリティ設定の一部を変更できます。

このタスクについて

を使用したCIFSサーバのKerberos設定の変更 `vserver cifs security modify` コマンドでは、で指定した単一のStorage Virtual Machine（SVM）の設定のみを変更できます `-vserver` パラメータActive Directory の Group Policy Object （ GPO ；グループポリシーオブジェクト）を使用すると、同一の Active Directory ドメインに属するクラスタ上の SVM すべてについて、 Kerberos セキュリティ設定を集中管理できます。

手順

1. 次の操作を 1 つ以上実行します。

状況	入力するコマンド
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します。	`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。
チケットの更新日の最大数を指定します。	`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します。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、 SVM vs1 の Kerberos セキュリティ設定を「 Kerberos Clock Skew 」に 3 分、「 Kerberos Ticket Age 」に 8 時間に変更しています。

```
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

"CIFS サーバ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"

SMBサーバの最小認証セキュリティレベルを設定する

SMB サーバの *LMCompatibilityLevel* とも呼ばれる SMB サーバの最小セキュリティレベルを設定することで、 SMB クライアントアクセスの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は、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。

このタスクについて

- 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、 admin 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。

価値	説明
`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目的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 ベースの通信用の AES 暗号化を有効または無効にします

AES 暗号化を使用して Kerberos ベースの通信のセキュリティを強化できます

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 サーバでは、 Kerberos 通信で次の暗号化タイプがサポートされます。

- AES 256
- AES 128
- DES （デス
- 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ります。その後、認証時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ます。を使用できます `-advertised-enc-types` 推奨される暗号化タイプを有効にするオプション。また、弱い暗号化タイプを無効にする場合にも使用できます。方法をご確認ください "Kerberosベースの通信の暗号化タイプを有効または無効にします"。

> 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

CIFS サーバの Kerberos セキュリティ設定の変更

Kerberos ベースの通信用の AES 暗号化を有効または無効にします

Kerberosベースの通信で最も強力なセキュリティを活用するには、SMBサーバでAES-256暗号化と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。 Active Directory （ AD ） KDC との Kerberos ベースの通信に AES 暗号化タイプを SMB サーバで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、および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バージョン	**AES**暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルトでは	はい。
9.12.1:	手動で実行する	はい。
9.11.1以前	手動で実行する	いいえ

ONTAP 9.12.1以降では、を使用してAES暗号化を有効または無効にします `-advertised-enc-types` オプション。AD KDCにアドバタイズする暗号化タイプを指定できます。デフォルト設定はです `rc4` および `des`` ただし、`AES`タイプを指定すると、`AES`暗号化が有効になります。オプションを使用して、弱い`RC4`暗号化タイプと`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` AES暗号化を有効または無効にするオプションを指定できません。また、暗号化タイプは指定できません。

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含まれる組織単位（ 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。

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（ `-identity-preserve` オプションはに設定されています `false` SnapMirrorの設定では、デフォルト以外の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。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を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 通信の **AES** 暗号化タイプの設定	入力するコマンド
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では廃止され、以降のリリースでは削除される可能性があります。

2. AES暗号化が設定どおり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 サーバを含む 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 通信の **AES** 暗号化タイプの設定	入力するコマンド
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暗号化が設定どおり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` フィールドが表示されます `true` AES暗号化が有効になっている場合と `false` 無効になっている場合。

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 サーバを含む 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
```

SMB 署名を使用してネットワークのセキュリティを強化します

SMB 署名を使用してネットワークセキュリティの概要を強化します

SMB 署名は、リプレイアタックを防止することで、 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が危険にさらされることのないようにします。デフォルト ONTAP では、クライアントから要求されたときに SMB 署名がサポートされます。ストレージ管理者は、必要に応じて、 SMB 署名を必須にするように SMB サーバを設定できます。

SMB 署名ポリシーが **CIFS** サーバとの通信に与える影響

CIFS サーバの SMB 署名セキュリティ設定に加えて、クライアントと CIFS サーバ間の通信のデジタル署名を制御する Windows クライアント上の SMB 署名ポリシーが 2 つあります。ビジネス要件に合わせて設定を行うことができます。

クライアント SMB ポリシーは、 Microsoft 管理コンソール（ MMC ）または Active Directory の GPO を使用して設定した Windows ローカルセキュリティポリシー設定で制御されます。クライアントの SMB 署名とセキュリティ問題の詳細については、 Microsoft Windows のマニュアルを参照してください。

ここでは、 Microsoft クライアントの 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。この設定をクライアントで無効にすると、クライアントの CIFS サーバとの通信は、 CIFS サーバ上の SMB 署名の設定によって異なります。

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

  この設定は、クライアントがサーバとの通信に 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。この設定がクライアントで無効になっている場合、SMB署名の動作はのポリシー設定に基づきます `Microsoft network client: Digitally sign communications (if server agrees)` およびCIFSサーバの設定。

> ご使用の環境に、 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る場合、 CIFS サーバ上の 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 SMB 署名設定の有効な結果は、 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有効な 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
署名は無効になっており、不要です	署名されません	署名
署名が有効になっており、不要である	署名されません	署名
署名が無効になっており、必要です	署名	署名
署名が有効になっており、必要です	署名	署名

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、署名がクライアントでは無効になっていて 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有効な SMB 署名の動作を示します。

SMB 2.x クライアントと SMB 3.0 クライアントでは、 SMB 署名は常に有効になります。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
署名は不要です	署名されません	署名
署名が必要です	署名	署名

次の表に、 Microsoft クライアントおよびサーバの SMB 署名のデフォルト動作を示します。

プロトコル	ハッシュアルゴリズム	有効 / 無効を切り替えられます	必須 / 不要	クライアントのデフォルト	サーバのデフォルト	**DC** のデフォルト
SMB 1.0	MD5	はい。	はい。	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい。	必要ありません	必要ありません	必須
SMB 3.0	AES-CMAC ：	いいえ	はい。	必要ありません	必要ありません	必須

Microsoftではの使用を推奨していません `Digitally sign communications (if client agrees)` または `Digitally sign communications (if server agrees)` グループポリシーの設定。Microsoftでは、の使用も推奨していません `EnableSecuritySignature` レジストリ設定。これらのオプションはSMB 1の動作にのみ影響し、で置き換えることができます `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。詳細については、Microsoftのブログを参照してください。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The SMB署名の基礎（SMB1とSMB2の両方をカバー）]

SMB 署名のパフォーマンスへの影響

SMB セッションで SMB 署名を使用すると、 Windows クライアントとのすべての SMB 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 を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、 CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、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、新しい暗号化の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が向上します。SMB 署名オフロードは、 SMB 署名が有効になっている場合にデフォルトで有効になります。

SMB 署名のパフォーマンスを向上させるには、 AES-NI オフロード機能が必要です。お使い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。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

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には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

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。一部の Windows クライアントで 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。

SMB 署名の設定に関する推奨事項

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必要がある	を有効にして、クライアントでSMB署名を必須にします `Require Option (Sign always)` クライアントのセキュリティ設定。
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 のマニュアルを参照してください。

複数のデータ **LIF** が設定されている場合の **SMB** 署名に関するガイドライン

SMB サーバで SMB 署名要求を有効または無効にするときは、 SVM に複数のデータ LIF が設定されている場合のガイドラインに注意する必要があります。

SMB サーバを設定する際に、複数のデータ LIF が設定されていることがあります。その場合、DNSサーバに複数のが含まれています `A` CIFSサーバのエントリを記録します。SMBサーバホスト名はすべて同じですが、IPアドレスはそれぞれ一意です。たとえば、2つのデータLIFが設定されているSMBサーバのDNSは次のようになります `A` レコードエントリ：

```
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、 SMB 署名要求の設定を変更すると、クライアントからの新しい接続だけが SMB 署名の設定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。クライアントに共有への既存の接続がある場合、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存の SMB 接続の両方で新しい SMB 署名の要件が適用されます。

次の例を考えてみましょう。

1. client1は、パスを使用してSMB署名を必要とせずに共有に接続します `O:\`。
2. ストレージ管理者が、 SMB 署名を要求するように SMB サーバの設定を変更したとします。
3. client1は、パスを使用してSMB署名要求で同じ共有に接続します `S:\` （パスを使用して接続を維持します `O:\`）。
4. その結果、両方でデータにアクセスするときにSMB署名が使用されます `O:\` および `S:\` ドライブ。

受信 **SMB** トラフィックの **SMB** 署名要求を有効または無効にします

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。

このタスクについて

デフォルトでは、 SMB 署名要求は無効になっています。SMB 署名要求はいつでも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）ディザスタリカバリ関係を設定する際にで選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、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を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` （ID保持）。SMB署名のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は `-identity-preserve` オプションをに設定します `false` （ID保持なし）。SMB署名の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 SMB 署名要求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。

SMB 署名要求の設定	入力するコマンド
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. での値を確認して、SMB署名要求が有効か無効かを確認します `Is Signing Required` 次のコマンドの出力のフィールドは、目的の値に設定されます。 `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
```

暗号化設定への変更は、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。

SMB セッションが署名されているかどうかを確認します

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。

表示する情報	入力するコマンド
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`

表示する情報	入力するコマンド
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です	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

例

次のコマンドを実行すると、 SVM vs1 上の署名されたセッションに関するセッション情報が表示されます。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
```

次のコマンドを実行すると、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が表示されます。

```
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を監視します

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。

このタスクについて

。 `statistics` advanced権限レベルでコマンドを実行すると、が表示されます `signed_sessions` 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カウンタ。。 `signed_sessions` カウンタには、次の統計オブジェクトがあります。

- `cifs` すべてのSMBセッションについてSMB署名を監視できます。
- `smb1` SMB 1.0セッションのSMB署名を監視できます。
- `smb2` SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

  SMB 3.0の統計はの出力に表示されます `smb2` オブジェクト。

署名されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `signed_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

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、サンプルが固定された状態になります。データ収集を停止しないと、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取得できます。この比較は、傾向を確認するのに役立ちます。

手順

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

   指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

   必要に応じて、統計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。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 署名統計情報を表示します。

表示する情報	入力するコマンド
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions

表示する情報	入力するコマンド
node_name [-node *node_name*]`	署名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 signed_sessions	established_sessions

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

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

例

次の例では、「 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
```

次のコマンドは、ノードが署名した SMB セッションと確立された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
```

次のコマンドは、 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の概要"

SMB を介したデータ転送に必要な SMB 暗号化を SMB サーバで設定します

SMB暗号化の概要

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 暗号化が提供する高度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。

暗号化された 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。Windows Server 2012 および Windows 8 以降の Windows クライアントでは、 SMB 暗号化がサポートされます。

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。

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

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。

次の表に示す 2 つの設定の組み合わせを使用すると、効果的な SMB 暗号化設定を行うことができます。

SMB サーバ **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しいです	いいえ	SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、 SMB セッション全体で暗号化が行われます。
正しいです	正しいです	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です。この設定では、 SMB セッション全体で暗号化が行われます。
いいえ	正しいです	特定の共有で共有レベルの暗号化が有効です。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 **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
いいえ	いいえ	暗号化は有効になっていません。

暗号化をサポートしていない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。

暗号化設定への変更は、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。

SMB 暗号化のパフォーマンスへの影響

SMB セッションで SMB 暗号化を使用すると、 Windows クライアントとのすべての SMB 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 を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、 CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、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、新しい暗号化の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が向上します。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に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を高めるには、 AES-NI オフロード機能が必要です。お使い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。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

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には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

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 **SMB** トラフィックの **SMB** 暗号化要求を有効または無効にします

受信 SMB トラフィックに SMB 暗号化を必須にする場合は、 CIFS サーバ上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。

このタスクについて

CIFS サーバ上で SMB 暗号化を有効にすることができます。この場合、 CIFS サーバ上のすべての共有が環境によって暗号化されます。CIFS サーバ上のすべての共有で SMB 暗号化要求を有効にしない場合、または受信 SMB トラフィックの SMB 暗号化要求を共有ごとに有効にする場合は、 CIFS サーバ上で SMB 暗号化要求を無効にすることができます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップするときににに選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、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を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` （ID保持）では、SMB暗号化のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は `-identity-preserve` オプションをに設定します `false` （ID保持なし）。SMB暗号化の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	入力するコマンド
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サーバでのSMB暗号化要求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` フィールドが表示されます `true` CIFSサーバおよびでSMB暗号化要求が有効になっている場合 `false` 無効になっている場合。

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
```

クライアントが暗号化 **SMB** セッションを使用して接続しているかどうかを確認します

接続中の SMB セッションに関する情報を表示して、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、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。

このタスクについて

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

- `unencrypted`

  SMB セッションは暗号化されません。Storage Virtual Machine （ SVM ）レベルの暗号化も共有レベルの暗号化も設定されません。

- `partially-encrypted`

  ツリー接続が行われると、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りません。

- `encrypted`

  SMB セッションは完全に暗号化されます。SVM レベルの暗号化が有効です。共有レベルの暗号化は、有効になる場合とならない場合があります。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。

表示する情報	入力するコマンド
指定した SVM のセッションで、指定した暗号化設定を使用するセッション	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定した SVM 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

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

```
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
```

SMB 暗号化統計情報を監視する

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。

このタスクについて

。 `statistics` advanced権限レベルでコマンドを実行すると次のカウンタが表示され、暗号化されたSMBセッションおよび共有接続の数を監視できます。

カウンタ名	説明
`encrypted_sessions`	暗号化された SMB 3.0 セッションの数
`encrypted_share_connections`	ツリー接続が行われた暗号化された共有の数
`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を示します
`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使用できます。

- `cifs` すべてのSMB 3.0セッションについてSMB暗号化を監視できます。

  SMB 3.0の統計はの出力に表示されます `cifs` オブジェクト。 暗号化されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `encrypted_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

  暗号化された共有接続数を共有接続の合計数と比較する場合は、の出力を比較します `encrypted_share_connections` の出力でカウンタに設定します `connected_shares` カウンタ。

- `rejected_unencrypted_sessions` 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セッションの確立が試行された回数を示します。
- `rejected_unencrypted_shares` 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が必要なSMB共有への接続が試行された回数を示します。

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、サンプルが固定された状態になります。データ収集を停止しないと、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取得できます。この比較は、傾向を確認するのに役立ちます。

手順

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

   指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

   必要に応じて、統計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。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 暗号化統計情報を表示します。

表示する情報	入力するコマンド
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

表示する情報	入力するコマンド
`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*]`
暗号化されていないセッションは	`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
`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、オプションのを指定します `-node` パラメータ

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

使用可能な統計オブジェクトと統計カウンタの確認

"パフォーマンスの監視と管理の概要"

セキュアな **LDAP** セッション通信

LDAP の署名と封印の概念

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、シークレットキーのテクノロジを使用して、 LDAP ペイロードデータの整合性を確認します。封印は、 LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。

SVMでCIFSトラフィックに対するLDAPの署名と封印が `-session-security-for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

CIFS サーバで **LDAP** の署名と封印を有効にする

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

作業を開始する前に

AD サーバ管理者に問い合わせて、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver` *`vserver_name`* `-session-security -for-ad-ldap {none|sign|seal}`

   署名を有効にできます (`sign`、データ整合性）、署名と封印 (`seal`、データ整合性と暗号化）、またはどちらでもない `none`、署名または封印なし）。デフォルト値はです `none`。

2. LDAPの署名と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がネーム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、で対応する設定を有効にする必要があります `-session-security` のオプション `vserver services name-service ldap client modify` コマンドを実行します

LDAP over TLS を設定する

自己署名ルート **CA** 証明書のコピーをエクスポートします

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。

作業を開始する前に

Active Directory 証明書サービスがすでにインストールされ、 CIFS サーバが属してい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"

ステップ

1. 内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 `.pem` テキスト形式。

   "Microsoft TechNet ライブラリ： technet.microsoft.com"

完了後

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"

自己署名ルート **CA** 証明書を **SVM** にインストールします

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。

このタスクについて

LDAP over TLS が有効な場合、 SVM 上の ONTAP LDAP クライアントでは、 ONTAP 9.0 および 9.1 の破棄された証明書はサポートされません。

ONTAP 9.2 以降では、 TLS 通信を使用する ONTAP 内のすべてのアプリケーションで、 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。OCSP が LDAP over TLS に対して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. 証明書を開きます `.pem` ファイルテキストエディタを使用して、で始まる行を含めて証明書をコピーします `-----BEGIN CERTIFICATE-----` で終わる `-----END CERTIFICATE-----`をクリックし、コマンドプロンプトのあとに証明書を貼り付けます。

   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`

サーバで **LDAP over TLS** を有効にします

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 以降では、 Active Directory （ AD ）とネームサービスの両方の LDAP 接続で、 LDAP チャネルバインド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封印に設定されている場合にのみ、 LDAP 接続でチャネルバインドを試行します。ADサーバとのLDAPチャネルバインディングを無効または再度有効にするには、を使用します `-try-channel-binding-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します

詳細については、以下を参照してください。

- "LDAPの概要"
- "2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"。

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行います。 `vserver cifs security modify -vserver *vserver_name* -use-start-tls-for-ad-ldap true`
2. LDAP over TLSのセキュリティ設定が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がネーム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、も変更する必要があります `-use-start-tls` オプションを使用します `vserver services name-service ldap client modify` コマンドを実行します

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

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。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。

作業を開始する前に

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 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。

このタスクについて

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 セッションでの同時接続数は、導入している NIC によって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

  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 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 で接続を確立できます。

また、次のパラメータを変更することもできます（ 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有効にする場合は、クライアントの設定に対して同等の調整を行う必要があります。これには、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. ONTAP が SMB マルチチャネルセッションを報告していることを確認します。 `vserver cifs session show` *`options`*
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を設定する

デフォルトの UNIX ユーザを設定する

ユーザに対する他のマッピングの試行がすべて失敗した場合や、 UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトの UNIX ユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする必要がある場合は、デフォルト UNIX ユーザを設定しないでください。

このタスクについて

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、デフォルトで、デフォルト UNIX ユーザへのユーザマッピングが有効になっていることを意味します。デフォルトの 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 ）用に設定されているネームサービスデータベース内に存在する必要があります。このオプションを null 文字列に設定すると、どのユーザも UNIX デフォルトユーザとして CIFS サーバにアクセスできません。つまり、 CIFS サーバにアクセスするためには、各ユーザがパスワードデータベースにアカウントを持つ必要があります。

ユーザがデフォルトの UNIX ユーザアカウントを使用して CIFS サーバに接続するには、次の前提条件を満たす必要があります。

- ユーザが認証されていること。
- ユーザが、 CIFS サーバのローカル Windows ユーザデータベース、 CIFS サーバのホームドメイン、信頼できるドメイン（ CIFS サーバでマルチドメインネームマッピング検索が有効な場合）のいずれかにあること
- ユーザ名が明示的に null 文字列にマッピングされることはありません。

手順

1. デフォルトの UNIX ユーザを設定します。

状況	入力するコマンド
デフォルトの UNIX ユーザ「 pcuser 」を使用する	`vserver cifs options modify -default -unix-user pcuser`
別の UNIX ユーザアカウントをデフォルトユーザとして使用します	`vserver cifs options modify -default -unix-user` *`user_name`*
デフォルトの UNIX ユーザを無効にします	`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 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「 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 **UNIX** ユーザを設定します

ゲスト UNIX ユーザを設定すると、信頼されていないドメインからログインしたユーザがゲスト UNIX ユーザにマッピングされ、 CIFS サーバに接続できるようになります。ただし、信頼されていないドメインのユーザの認証を失敗にする場合は、ゲスト UNIX ユーザ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による CIFS サーバへの接続は許可されません（ゲスト UNIX アカウントは設定されません）。

このタスクについて

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- 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、ローカルデータベースのどちらか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。
- このオプションを null 文字列に設定すると、ゲスト UNIX ユーザは無効になります。
- 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。
- ゲストユーザとしてログインしたユーザは、自動的に CIFS サーバの BUILTIN\guests グループのメンバーになります。
- 「 homedirs-public 」オプションは、認証されたユーザにのみ適用されます。ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
ゲスト UNIX ユーザを設定します	`vserver cifs options modify -guest -unix-user` *`unix_name`*
ゲスト UNIX ユーザを無効にします	`vserver cifs options modify -guest -unix-user ""`

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

2. ゲストUNIXユーザ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 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「 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           : -
   ```

Administrators グループをルートにマッピングします

環境内のクライアントがすべて CIFS クライアントで、 Storage Virtual Machine （ 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 root 権限を持つ Windows アカウントが少なくとも 1 つ必要です。 十分なユーザ権限がないため、この SVM を管理できません。

このタスクについて

ただし、ストレージシステムがNTFS専用としてセットアップされている場合は `/etc` ディレクトリには、AdministratorsグループがONTAP 構成ファイルにアクセスできるようにするファイルレベルのACLが設定されています。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 必要に応じて、 Administrators グループをルートにマッピングする CIFS サーバオプションを設定します。

状況	作業
管理者グループメンバーをルートにマッピングします	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` がなくても、Administratorsグループ内のすべてのアカウントはrootとみなされます `/etc/usermap.cfg` アカウントをrootにマッピングするエントリ。Administrators 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する場合、 UNIX クライアントからファイルを表示するときに、ファイルはルートによって所有されます。
Administrators グループメンバーのルートへのマッピングを無効にします	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Administratorsグループ内のアカウントがrootにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行できます。

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`

SMB セッションを介して接続しているユーザのタイプに関する情報を表示します

SMB セッションを介して接続しているユーザのタイプに関する情報を表示できます。これは、適切なタイプのユーザのみが Storage Virtual Machine （ SVM ）上の SMB セッションを介して接続していることを確認するのに役立ちます。

このタスクについて

SMB セッションを介して接続できるユーザのタイプは次のとおりです。

- `local-user`

  ローカル CIFS ユーザとして認証されている

- `domain-user`

  ドメインユーザとして（ CIFS サーバのホームドメインまたは信頼できるドメインから）認証されている

- `guest-user`

  ゲストユーザとして認証されています

- `anonymous-user`

  匿名ユーザまたは null ユーザとして認証されています

手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。 `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タイプ情報を表示する対象	入力するコマンド
指定したユーザ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}`	特定のユーザの場合

例

次のコマンドを実行すると、ユーザ「 iepubs\user1 」によって確立された SVM vs1 上のセッションのユーザタイプに関するセッション情報が表示されます。

```
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
```

Windows クライアントの過剰なリソース消費を制限するコマンドオプション

をクリックします `vserver cifs options modify` コマンドを使用すると、Windowsクライアントのリソース消費を制御できます。ファイルオープン、セッションオープン、変更通知要求が異常に多い場合など、正常な範囲を超えてリソースを消費しているクライアントがある場合に便利です。

には次のオプションがあります `vserver cifs options modify` Windowsクライアントのリソース消費を制御するコマンドが追加されました。これらのオプションの最大値を超えると、要求は拒否され、 EMS メッセージが送信されます。これらのオプションで設定された上限の 80% に達したときにも 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`

同じユーザが接続ごとに開いたセッションの最大数

- `-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の最大数（別名 *change notifier*）

デフォルトの制限および現在の設定を表示する方法については、マニュアルページを参照してください。

ONTAP 9.4 以降では、 SMB バージョン 2 以降を実行しているサーバで、クライアントからサーバに SMB 接続で送信できる未処理要求（ _SMB クレジット _ ）の数を制限することができます。SMB クレジットの管理はクライアント側で開始され、サーバ側で制御されます。

SMB接続で許可できる未処理要求の最大数は、で制御されます `-max-credits` オプション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** リースでクライアントのパフォーマンスを向上

従来の **oplock** および **oplock** リースの概要でクライアントのパフォーマンスを向上

便宜的 oplock と oplock リースでは、先読み、あと書き、ロックの各情報を SMB クライアント側でキャッシングできるよう、特定のファイル共有シナリオでそのクライアントを有効にします。これにより、クライアントは、目的のファイルへのアクセス要求をサーバに定期的に通知しなくても、ファイルの読み書きを実行できます。これにより、ネットワークトラフィックが軽減され、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し、保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティで、を使用します `vserver cifs share create` 共有の作成時にコマンドを実行するか、またはを実行します `vserver share properties` 作成後のコマンド。
- qtreeプロパティ。を使用します `volume qtree create` コマンドを使用してqtreeを作成するか、コマンドを使用します `volume qtree oplock` 作成後のコマンド。

oplock を使用するときの書き込みキャッシュデータ消失に関する考慮事項

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可能性があ

ります。

- データ損失の可能性

  データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります。

  - 接続は SMB 1.0 を使用して確立されます。
  - ファイルに対して排他的な oplock を使用している場合
  - oplock を解除するか、ファイルを閉じるように指示された場合
  - 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲットシステムにエラーが発生した場合

- エラー処理および書き込みの完了

  キャッシュ自体にはエラー処理がありません。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と、書き込みは常に完了します。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、書き込みは完了していると仮定する必要があります。これは、完了していない場合、データが失われるためです。

SMB 共有の作成時に oplock を有効または無効にします

oplock を使用すると、クライアントによって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が向上します。Storage Virtual Machine （ SVM ）上にある SMB 共有では、 oplock が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。oplock は共有ごとに有効または無効にできます。

このタスクについて

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. 該当する操作を実行します。

状況	作業
共有の作成時に共有で oplock を有効にします	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のみを設定する場合は、です `oplocks`、 `browsable`および `changenotify` 有効にすると、を指定する必要はありません `-share-properties` SMB共有を作成するときのパラメータ。デフォルト以外の共有プロパティを組み合わせて使用する場合は、を指定する必要があります `-share-properties` パラメータに指定し、その共有に使用する共有プロパティのリストを指定します。
共有の作成時に共有で oplock を無効にします	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、共有の作成時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、を指定することはできません `oplocks` プロパティ。

関連情報

既存の SMB 共有で oplock を有効または無効にします

oplock ステータスを監視しています

ボリュームおよび **qtree** で **oplock** を有効または無効にするためのコマンド

oplock を使用すると、クライアントによって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が向上します。ボリュームや qtree の oplock を有効または無効にするためのコマンドを理解しておく必要があります。また、いつボリュームおよび qtree で oplock を有効または無効に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。

- ボリュームの作成時に oplock を無効に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できます。
- SVM の qtree では oplock を有効にできます。

  oplock モードの設定は、すべてのボリュームのデフォルトの qtree である qtree ID 0 のプロパティです。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 設定を継承します。この設定はデフォルトで有効になっています。ただし、新しい qtree に oplock 設定を指定すると、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 を有効にします	`volume qtree oplocks` を使用 `-oplock-mode` パラメータをに設定します `enable`
ボリュームまたは qtree の oplock を無効にします	`volume qtree oplocks` を使用 `-oplock-mode` パラメータをに設定します `disable`

関連情報

oplock ステータスを監視しています

既存の **SMB** 共有で **oplock** を有効または無効にします

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できます。

このタスクについて

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。

ステップ

1. 該当する操作を実行します。

状況	作業
既存の共有を変更して、共有で oplock を有効にします	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。 新しく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。
既存の共有を変更して共有で oplock を無効にします	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です。

例

次のコマンドは、 Storage Virtual Machine （ SVM 、旧 Vserver ） vs1 上の「 Engineering 」という名前の共有の 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 ステータスを監視しています

既存の SMB 共有に対する共有プロパティの追加または削除

oplock ステータスを監視します

oplock ステータスについて、情報を監視、表示できます。この情報を使用して、 oplock が設定されたファイル、 oplock のレベルや oplock の状態レベル、 oplock リースの使用の有無を確認できます。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、情報を確認することもできます。

このタスクについて

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 ）およびロックのタイプ（ 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 リースが許可されている場合は、 Open Group ID

を参照してください `vserver oplocks show` 各パラメータの詳細な概要 のマニュアルページ

手順

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

例

次のコマンドは、すべてのロックに関するデフォルトの情報を表示します。表示されたファイルのoplockは、で許可されています `read-batch` oplockレベル：

```
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 `/data2/data2_2/intro.pptx`。を使用してファイルにoplockリースが許可されています `batch` IPアドレスがのクライアントに対するoplockレベル `10.3.1.3`：

> 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 oplock を有効または無効にします

ボリュームおよび qtree で oplock を有効または無効にするためのコマンド

SMB サーバへのグループポリシーオブジェクトの適用

SMB サーバへのグループポリシーオブジェクトの適用の概要の説明を参照してください

SMBサーバは、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は、Active Directory環境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す。GPO を使用して、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。

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

情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次の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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

"SMB および NFS の監査とセキュリティトレース"

サポートされる GPO

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設定：

  オブジェクトへのアクセス：集約型アクセスポリシーのステージング

  次の設定を含む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のタイプを指定します。

  - 監査しないでください
  - 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。

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

  > 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 対応の SVM のグループポリシーの更新間隔

を使用して設定します `Registry` GPO：

- グループポリシーの更新間隔のランダムオフセット

  を使用して設定します `Registry` GPO：

- BranchCache のハッシュの発行

  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。

  - 共有ごと
  - all-shares
  - 無効 を使用して設定します `Registry` GPO：

- BranchCache のハッシュバージョンサポート

  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 1.7
  - BranchCache バージョン 1.7
  - BranchCacheバージョン1および2 を使用して設定します `Registry` GPO：

> 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

    - ログオンイベントを監査します

      次の設定を含む監査対象となるログオンイベントの種類を指定します。

      - 監査しないでください
      - 成功イベントのみ監査
      - 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 を使用して設定します `Audit logon events` を設定します `Local Policies/Audit Policy` GPO：

> 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。

    - オブジェクトへのアクセスを監査する

      次の設定を含む監査対象となるオブジェクトアクセスの種類を指定します。

- 監査しないでください
- 成功イベントのみ監査
- 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 を使用して設定します `Audit object access` を設定します `Local Policies/Audit Policy` GPO：

> 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。

- ログの保持方法

  次の設定を含む監査ログの保持方法を指定します。

  - ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
  - イベントログを上書きしない（手動でログを消去） を使用して設定します `Retention method for security log` を設定します `Event Log` GPO：

- 最大ログサイズ

  監査ログの最大サイズを指定します。

  を使用して設定します `Maximum security log size` を設定します `Event Log` GPO：

> 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 を通して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。

を使用して設定します `File System` GPO：

> 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同期の最大許容誤差を分単位で指定します。

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

- チケットの有効期間

  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。

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

- チケットの更新の有効期間

  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。

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

- ユーザ権限の割り当て（権限）

  - 所有権を取得します

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

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

  - 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。

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

  - 通知権限の変更（トラバースチェックのバイパス）

    ユーザとグループがトラバースするディレクトリに対する権限を持っていなくても、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通知を受け取るユーザにも同じ権限が必要です。を使用して設定します `Bypass traverse checking` を設定します `Local Policies/User Rights Assignment` GPO：

- レジストリ値

  - 署名要求設定

    SMB 署名要求が有効になっているか無効になっているかを示します。

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

- restrict anonymous （匿名の制限

  匿名ユーザの制限内容に次の 3 つの GPO 設定を指定します。

  - Security Account Manager （ SAM ）アカウントを列挙しない：

    このセキュリティ設定は、コンピュータへの匿名接続に付与される追加の権限を決定します。こ

のオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

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

- SAM アカウントと共有は列挙しません

  このセキュリティ設定で、匿名による SAM アカウントと共有の列挙を許可するかどうかを決定します。このオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

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

- 共有と名前付きパイプへの匿名アクセスを制限します

  共有とパイプへの匿名アクセスを制限します。このオプションはと表示されます `no-access` ONTAP （有効になっている場合）。

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

  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場合は、 `Resultant restriction for anonymous user` Outputフィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示されます。表示される可能性がある制限結果は、次のとおりです。

- `no-access`

  匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、 SAM アカウントと共有を列挙できません。この制限結果は、の場合に表示されます `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが有効になっている。

- `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適用されます。

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
  - またはをクリックします `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が有効になっている。

- `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適用されます。

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
  - 両方とも `Network access: Do not allow anonymous enumeration of SAM accounts` および `Network access: Do not allow anonymous enumeration of SAM accounts`

`and shares` GPOが無効になっている。

- 制限されたグループ

  制限されたグループを設定して、組み込みまたはユーザ定義のグループのメンバーシップを一元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シップは、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。

を使用して設定します `Restricted Groups` GPO：

- 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指定します。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限が決定されます。

関連情報

CIFS サーバ上で GPO サポートを有効または無効にします

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

"SMB および NFS の監査とセキュリティトレース"

CIFS サーバの Kerberos セキュリティ設定の変更

BranchCache を使用したブランチオフィスでの SMB 共有のコンテンツのキャッシュ

SMB 署名を使用したネットワークセキュリティの強化

トラバースチェックのバイパスの設定

匿名ユーザのアクセス制限を設定します

SMB サーバで GPO を使用するための要件

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。

- クラスタで SMB のライセンスが有効になっている必要があります。SMBライセンスはに含まれています。 "ONTAP One"。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 ドメインに参加している必要があります。
- SMB サーバ管理ステータスがオンになっている必要があります。
- 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。

CIFS サーバ上で GPO のサポートを有効または無効にします

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 サーバ上で 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。

このタスクについて

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	入力するコマンド
GPOs を有効にします。	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOs 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になってい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

サポートされる GPO

CIFSサーバでGPOを使用するための要件

CIFS サーバでの GPO の更新方法

CIFS サーバ上の GPO 設定を手動で更新します

GPO 設定に関する情報を表示します

SMBサアハテノGPOノコウシンホウホウ

CIFS サーバでの GPO の更新方法の概要

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 時間ごとに更新されます。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。

- デフォルトでは、すべての GPO を 90 分に 1 回確認し、必要に応じて更新。

  この間隔は設定可能で、を使用して設定できます `Refresh interval` および `Random offset` GPO設定。

  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、ウィンドウをシミュレートします `gpupdate.exe`/force`コマンド。

関連情報

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバの Group Policy Object （ GPO ；グループポリシーオブジェクト）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。

ステップ

1. 適切な操作を実行します。

更新する項目	入力するコマンド
GPO 設定が変更されました	`vserver cifs group-policy update -vserver` *`vserver_name`*

更新する項目	入力するコマンド
すべての GPO 設定	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

関連情報

CIFS サーバでの GPO の更新方法

GPO 設定に関する情報を表示します

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。

このタスクについて

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するか、または 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ができます。

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。

情報を表示するグループポリシー設定	入力するコマンド
Active Directory で定義されています	`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、 vs1 という CIFS 対応の 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

CIFS サーバ上で GPO サポートを有効または無効にします

制限されたグループの **GPO** に関する詳細情報を表示します

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。

このタスクについて

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
- グループポリシーのバージョン
- リンク

  グループポリシーを設定するレベルを指定します。出力される値は次のとおりです。

- `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` グループポリシーがドメインコントローラのドメインレベルで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一連のポリシー

- 制限されたグループ名です
- 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リスト

  グループは、ここに記載されている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。

ステップ

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。

情報を表示する制限されたグループのすべての **GPO**	入力するコマンド
Active Directory で定義されています	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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

集約型アクセスポリシーに関する情報を表示します

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。

このタスクについて

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
- 説明
- 作成時間
- 修正日時
- 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。

ステップ

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。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directory で定義されています	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFS サーバに適用されます	`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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

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。

このタスクについて

定義および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 名です
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 修正日時
- 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た、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directory で定義されています	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

SMBサーバコンピュータアカウントパスワードの管理用コマンド

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。SMBサーバでスケジュールを設定して自動的に更新することもできます。

状況	使用するコマンド
ドメインアカウントのパスワードを変更またはリセットします。パスワードがわかっている場合	`vserver cifs domain password change`
ドメインアカウントパスワードをリセットします。パスワードがわからない場合	`vserver cifs domain password reset`
コンピュータアカウントパスワードの自動変更を行うために SMB サーバを設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
SMBサーバでのコンピュータアカウントパスワードの自動変更の無効化	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

詳細については、各コマンドのマニュアルページを参照してください。

ドメインコントローラ接続を管理します

検出されたサーバに関する情報を表示します

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。

ステップ

1. 検出されたサーバに関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

サーバのリセットおよび再検出

CIFS サーバを停止または起動しています

サーバをリセットおよび再検出します

CIFS サーバでサーバのリセットと再検出を行うと、 LDAP サーバおよびドメインコントローラに格納されている情報が CIFS サーバに破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。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. 再検出されたサーバ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を表示する

CIFS サーバを停止または起動しています

ドメインコントローラの検出を管理します

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。サイトまたは優先 DC のプールに検出を制限できるため、環境によってはパフォーマンスの向上につながります。

このタスクについて

デフォルトでは、任意の優先 DC 、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 を含めて、使用可能なすべての 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は、検出方法を変更できます。

ONTAP 9.3以降のリリースでは、 `discovery-mode` のパラメータ `cifs domain discovered-servers` コマンドでは、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 が検出されます。
- ローカルサイト内の DC だけが検出されます。

  。 `default-site` SMBサーバのパラメータは、sites-and-servicesで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。

ステップ

1. 目的の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}`

   のオプション `mode` パラメータ：

   - `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。

優先ドメインコントローラを追加する

ONTAP は DNS を介してドメインコントローラを自動的に検出します。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。

このタスクについて

指定したドメインに優先ドメインコントローラリストがすでに存在する場合、新しいリストが既存のリストに統合されます。

ステップ

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` Storage Virtual Machine（SVM）名を示します。

   `-domain domain_name` 指定し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*` はい。 優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、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管理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

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの追加、表示、削除を行う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`

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

優先ドメインコントローラの追加

ドメインコントローラへの **SMB2** 接続を有効にします

ONTAP 9.1 以降では、 SMB バージョン 2.0 からドメインコントローラへの接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、 SMB2 がデフォルトで有効になります。

このタスクについて

。 `smb2-enabled-for-dc-connections` コマンドオプションを使用すると、使用しているONTAP のリリースに応じたシステムデフォルトが有効になります。ONTAP 9.1 のシステムデフォルトでは、 SMB 1.0 が有効、 SMB 2.0 が無効になります。ONTAP 9.2 のシステムデフォルトでは、 SMB 1.0 が有効になり、 SMB 2.0 が有効になります。ドメインコントローラは、最初に SMB 2.0 をネゴシエートし、失敗した場合は SMB 1.0 を使用します。

SMB 1.0 は、 ONTAP からドメインコントローラに対して無効にすることができます。ONTAP 9.1 では、SMB 1.0 を無効にした場合、ドメインコントローラと通信するために SMB 2.0 を有効にする必要があります。

詳細情報：

- "有効なSMBのバージョンの確認"。
- "サポートされる SMB のバージョンと機能"。

> 状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true`ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

手順

1. SMBセキュリティ設定を変更する前に、有効になっているSMBのバージョンを確認します。 `vserver cifs security show`
2. リストを下にスクロールして SMB のバージョンを確認します。
3. を使用して、該当するコマンドを実行します `smb2-enabled-for-dc-connections` オプション

SMB2 の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

ドメインコントローラへの暗号化接続を有効にします

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。

このタスクについて

ONTAP では、ドメインコントローラ（DC）通信の暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`;デフォルトはです `false`。このオプションを設定すると、 SMB3 でのみ暗号化がサポートされるため、 SMB3 プロトコルのみが使用されます。

暗号化されたDC通信が必要な場合は、を参照してください `-smb2-enabled-for-dc-connections` ONTAP はSMB3接続のみをネゴシエートするため、この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。

ステップ

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** 環境のストレージにアクセスするには、 **null** セッションを使用します

非 **Kerberos** 環境でストレージにアクセスする場合は、 **null** セッションを使用します

null セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスに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へのアクセスを提供します。null セッションは、クライアントプロセスが「システム」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するときに発生します。null セッション設定は非 Kerberos 認証に固有です。

ストレージシステムによる null セッションアクセスの実現方法

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、でWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous` オプションこれにより、マッピングされていない null ユーザが表示またはアクセスできるシステムリソースの範囲を制御できます。たとえば、共有の一覧や 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` および `vserver cifs options show` の詳細については、のマニュアルページを参照してください `-restrict-anonymous` オプション

特に設定がないかぎり、 null セッションでストレージシステム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 」などの制限のないグループのみのメンバーとなります。null セッションアクセスを選択したストレージシステムリソースに制限するには、すべての null セッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限したり、null セッションクライアントのみに適用されるストレージシステムリソース権限を設定したりできます。

ONTAP には、マッピング構文が用意されています `vserver name-mapping` nullユーザセッションを使用した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アドレスを指定するコマンドセット。null ユーザ用のグループを作成したら、 null セッションのみに適用されるストレージシステムリソースのアクセス制限および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みなされます。null ユーザは、ホームディレクトリに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すべての null ユーザには、マッピングされたユーザ権限が付与されます。null ユーザにマッピングされたストレージシステムへの不正なアクセスを防止するため、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要な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「 SVM 」の問題を解消します。

関連情報

匿名ユーザのアクセス制限を設定します

null ユーザにファイルシステム共有へのアクセスを許可します

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使用する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. を使用します `vserver name-mapping create` 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するコマンド。

   次のコマンドは、有効なホスト名 google.com で user1 に null ユーザ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、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。

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

2. を使用します `vserver name-mapping show` コマンドを入力してネーム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. を使用します `vserver cifs options modify –win-name-for-null-user` nullユーザにWindowsメンバーシップを割り当てるコマンド。

   このオプションは、 null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

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

4. を使用します `vserver cifs options show` コマンドを使用して、nullユーザのWindowsユーザまたはグループへ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 サーバの NetBIOS エイリアスを管理します

SMB サーバ用の NetBIOS エイリアスの概要を管理します

NetBIOS エイリアスは、 SMB クライアントが SMB サーバに接続するときに使用でき

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

SMB サーバの作成時または SMB サーバ作成後の任意の時点で、 NetBIOS エイリアスのリストを指定できます。リストへの NetBIOS エイリアスの追加や削除は、いつでも行うことができます。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 接続に関する情報を表示する

SMBサーバにNetBIOSエイリアスのリストを追加する

エイリアスを使用してSMBサーバに接続できるようにするには、NetBIOSエイリアスのリストを作成するか、既存のNetBIOSエイリアスのリストにNetBIOSエイリアスを追加します。

このタスクについて

- 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
   ```

   - 1 つ以上の NetBIOS エイリアスをカンマで区切って指定します。
   - 指定した 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

NetBIOS エイリアスリストからの NetBIOS エイリアスの削除

CIFS サーバの NetBIOS エイリアスのリストを表示する

NetBIOS エイリアスリストから NetBIOS エイリアスを削除します

CIFS サーバで特定の NetBIOS エイリアスが不要な場合、その NetBIOS エイリアスをリストから削除できます。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。

このタスクについて

複数の NetBIOS エイリアスを削除するには、カンマで区切って指定します。を指定すると、CIFSサーバ上のすべてのNetBIOSエイリアスを削除できます - をの値として指定します `-netbios-aliases` パラメータ

手順

1. 次のいずれかを実行します。

削除する項目	入力するコマンド
リスト内の特定の 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. 指定した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
```

CIFS サーバの NetBIOS エイリアスのリストを表示します

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場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
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 CIFS サーバの詳細情報の一部として表示します。

```
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
```

詳細については、コマンドのマニュアルページを参照してください。

関連情報

CIFS サーバへの NetBIOS エイリアスのリストの追加

CIFS サーバの管理用コマンド

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を確認します

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、および使

用している場合はその NetBIOS エイリアスを確認できます。これは、接続の問題のトラブルシューティングを行う場合に役立ちます。

このタスクについて

を使用する必要があります `-instance` SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するためのパラメータ。CIFSサーバの名前またはIPアドレスを使用してSMB接続を確立している場合は、の出力が表示されます `NetBIOS Name` フィールドはです `-` （ハイフン）。

ステップ

1. 必要な操作を実行します。

表示する **NetBIOS** 情報	入力するコマンド
SMBセツソク	`vserver cifs session show -instance`
指定した NetBIOS エイリアスを使用する接続：	`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
```

その他の SMB サーバタスクを管理します

CIFS サーバを停止または起動します

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には、 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	入力するコマンド
CIFS サーバを停止します	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFS サーバを起動します
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

   `-foreground` コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定します。省略した場合、このパラメータはに設定されます `true`コマンドはフォアグラウンドで実行されます。

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

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を表示する

サーバのリセットおよび再検出

CIFS サーバを別の OU に移動します

CIFS サーバの create プロセスでは、別の OU を指定しないかぎり、セットアップ時にデフォルトの Organizational Unit （ OU ；組織単位） 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 * （ * Move * ）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。

SMB サーバを移動する前に、 SVM 上の動的 DNS ドメインを変更します

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。

作業を開始する前に

SMB サーバコンピュータアカウントを含む新しいドメイン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には、 SVM で 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。

このタスクについて

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。

"動的 DNS サービスを設定する"

SVM を Active Directory ドメインに追加します

を使用してドメインを変更すると、既存のSMBサーバを削除することなくStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify` コマンドを実行します現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

作業を開始する前に

- SVM の DNS 設定が完了している必要があります。
- SVM の DNS 設定がターゲットドメインを提供できる必要があります。

  DNS サーバには、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 ）が含まれている必要があります。

このタスクについて

- Active Directory ドメインの変更を続行するには、 CIFS サーバの管理ステータスを「所有」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。
- ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

手順

1. SVMをCIFSサーバドメインに追加します。 `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

   詳細については、のマニュアルページを参照してください `vserver cifs modify` コマンドを実行します新しいドメイン用にDNSを再設定する必要がある場合は、のマニュアルページを参照してください `vserver dns modify` コマンドを実行します

   SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限がある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 `ou= example ou` 内のコンテナ *example*.comドメイン。

   ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

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 上にある SMB サーバ「 CIFSSERVER1 」を keytab 認証を使用して example.com ドメインに追加します。

```
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
```

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。これは、 NetBIOS に関連する問題のトラブルシューティングを行う場合に役立ちます。

ステップ

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

> 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 」について表示される NetBIOS ネームサービスの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サーバの管理用コマンド

作成、表示、変更、停止、開始、 およびSMBサーバを削除しています。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 エイリアスの追加または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 サーバを作成	`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	`vserver cifs stop`
SMB サーバを起動	`vserver cifs start`
SMBサーバを削除する	`vserver cifs delete`
SMBサーバ用のサーバのリセットと再検出	`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のスケジュールを設定する	`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サーバのNetBIOSエイリアスを削除する	`vserver cifs remove-netbios-aliases`

詳細については、各コマンドのマニュアルページを参照してください。

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"

NetBIOS ネームサービスを有効にします

ONTAP 9 以降では、 NetBIOS ネームサービス（ NBNS 、 Windows Internet Name Service または WINS と呼ばれることもあります）はデフォルトで無効になっていま

す。以前は、 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。

作業を開始する前に

- 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 サービスに IPv6 を使用します

IPv6 を使用するための要件

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 ライセンスの要件：

SMB のライセンスがあれば、 IPv6 を使用するために特別なライセンスは必要ありません。SMBライセンスはに含まれています。 "ONTAP One"。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 ONTAP 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。

SMB アクセスと CIFS サービスでの IPv6 のサポート

CIFS サーバで 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。次に、 Microsoft Windows クライアントおよびサーバによる IPv6 のサポートについて説明します。

- Windows 7 、 Windows 8 、 Windows Server 2008 、 Windows Server 2012 以降では、 SMB ファイル共有と、 DNS 、 LDAP 、 CLDAP 、 Kerberos サービスなどの Active Directory 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 および Windows Server 2008 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 共有に接続できます。

ONTAPがサポートするWindowsクライアントに関する最新情報については、を参照してください。 "互換性マトリックス"。

NT ドメインは IPv6 ではサポートされません。

その他の CIFS サービスもサポートされます

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、 および以前のバージョン
- 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が可能です
- NAS のマルチプロトコルの監査
- FPolicy の
- 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）

ネームサービスおよび認証サービスのサポート

次のネームサービスとの通信が 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サアハ
- NISサーバ

CIFS サーバが IPv6 を使用して外部サーバに接続する方法

要件に対応した設定を作成するには、 CIFS サーバが外部サーバへの接続を確立するときに IPv6 がどのように使用されるかを確認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を試行する場合、選択する送信元アドレスは宛先アドレスと同じタイプでなければなりません。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 アドレスを持つデータ 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 アドレスを持つデータ 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は、 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が適切かどうかと、 IPv6 または IPv4 のデータ LIF または管理 LIF が使用可能かどうかに応じて、いずれかのタイプが使用されます。 動的サーバ検出は、ドメインコントローラとその関連サービス（ LSA 、 NETLOGON 、 Kerberos 、 LDAP など）の検出に使用されます。

- 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。必要に応じて、 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にするため、 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、 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サアハセツソク

  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。必要に応じて、 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にするため、 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、 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。必要に応じて、NISサーバへの接続で引き続きIPv4アドレスを使用できるように、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、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

SMB での IPv6 の有効化（クラスタ管理者のみ）

IPv6 SMB セッション情報の監視および表示

SMB での IPv6 の有効化（クラスタ管理者のみ）

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。

ステップ

1. IPv6を有効にします。 `network options ipv6 modify -enabled true`

   クラスタでの IPv6 の有効化と IPv6 LIF の設定の詳細については、 _ ネットワーク管理ガイド _ を参照してください。

   IPv6 が有効になっている。SMB アクセス用の IPv6 データ LIF を設定できます。

関連情報

IPv6 SMB セッション情報の監視および表示

"Network Management の略"

SMB で IPv6 を無効にします

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、 ONTAP は IPv6 を無効にします。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る必要があります。

クラスタでの IPv6 の無効化の詳細については、 _ ネットワーク管理ガイド _ を参照してください。

関連情報

"Network Management の略"

IPv6 SMB セッション情報を監視および表示します

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。この情報は、 IPv6 SMB セッションに関する他の有用な情報と同様、 IPv6 を使用して接続するクライアントを決定する上で役に立ちます。

ステップ

1. 必要な操作を実行します。

確認する項目	入力するコマンド
Storage Virtual Machine （ SVM ）への SMB セッションは、 IPv6 を使用して接続されます	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
特定の LIF アドレスにより、 SMB セッションに IPv6 を使用します	`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。