SMBサーバを管理します。

ONTAP 9

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/smb-admin/modify-servers-task.html on December 20, 2024. Always check docs.netapp.com for the latest.

目次

SMBサーバを管理します。

SMBサーバの変更

コマンドを使用して、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`。

タスクの内容

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サーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *`example`* にコンピュータを追加するための十分な`Privileges`を備えた`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`。

  ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

- 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。

    - その他の属性を変更するには、コマンドの該当するパラメータを使用し `vserver cifs modify`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を検討する場合は、使用可能なオプションを把握しておくと役立ちます。一部のオプションは一般的なものですが、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いくつかあります。SMBサーバオプションは、オプションで制御し `vserver cifs options modify`ます。

次に、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（秒）を指定できます。アイドルセッションとは、ユーザがクライアント上でファイルやディレクトリを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サーバで使用するデフォルトの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）。そのため、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、読み取りアクセス権を持つ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して、読み取り専用属性が設定されたファイルまたはフォルダの削除をNFSクライアントに許可するかどうかを指定します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されている場合、ファイルやフォルダの削除は許可されません。UNIXの削除セマンティクスでは読み取り専用ビットが無視され、代わりに親ディレクトリの権限を使用してファイルまたはフォルダを削除できるかどうかが判断されます。デフォルトの設定はで `disabled`、NTFSの削除セマンティクスが適用されます。

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

  このオプションでは、Windows Internet Name Service（WINS）サーバアドレスのリスト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 *

  このオプションでは、ファイルの所有者ではない受信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をに設定する `true`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、このパラメータをに設定する `false`と、通常の`UNIX`ルールに従ってファイル権限が付与されます。このパラメータは、権限がに設定された`UNIX`セキュリティ形式のファイルに適用さ `mode bits`れます。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にSMBサーバが作成されているSVMでは、SMB 1.0はデフォルトで無効になっています。3.

  > SMB.3以降ではONTAP 9、SMB.3で作成された新しいONTAP 9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。セキュリティとコンプライアンスの強化に備えて、できるだけ早く新しいバージョンのSMBに移行する必要があります。詳細については、NetApp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を無効にする

と、ONTAPはSMB 3.Xも自動的に無効にします。

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っています。

- * 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。SMB 3.0をサポートするWindowsの最小バージョンは、Windows Server 2012およびWindows 8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っています。

- * SMB 3.1の有効化または無効化*

  Windows 10は、SMB 3.1をサポートする唯一のWindows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っています。

- * 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を使用すると、Windowsクライアントがコピーの実行中にファイルが変更されないモードでコピーのソースファイルを開こうとすると、コピーオフロード処理のパフォーマンスが向上します。デフォルトでは、直接コピーメカニズムが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接続でのみ有効です。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っています。

- * 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を使用して、Hyper-V over SMBソリューションを使用して格納されたデータのリモートバックアップを実行します。

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

- * シャドウ・コピーのディレクトリ階層の設定 *

  このオプションを設定すると、シャドウコピー機能を使用する場合に、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っています。

- * 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。ホームドメインは、SMBサーバのコンピュータアカウントが含まれているドメインです。

  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、その優先リストを使用してマルチドメインネームマッピングの検索が実行されます。

  デフォルトでは、マルチドメインネームマッピングの検索は有効になります。

- * ファイルシステムセクターサイズの設定 *

  このオプションでは、ONTAPがSMBクライアントに報告す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、との `512`2つの有効な値があります `4096`。デフォルト値はです `4096`。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は、この値をに設定する必要が `512`あります。

- * 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など、ダイナミックアクセス制御（DAC）を使用してSMBサーバ上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 ） *

このオプションを設定すると、認証されていないセッションのアクセス制限を指定できます。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をSMBクライアントに提供する方法を指定します。有効にすると、ONTAP 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が、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クライアントに提供されます。無効にするとONTAP、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、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役立ちます。

- * 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クライアントなどのUNIXベースのSMBクライアントが環境内にある場合は、UNIX拡張を有効にする必要があります。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検索クエリでは、8.3形式のファイル名と長いファイル名が照合されます。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リファーラルを使用します。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、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、オプションを設定して `-max-credits`SMB接続に付与するクレジット数を制限できます。デフォルト値は128です。

- * SMB マルチチャネルのサポートの有効化または無効化 *

ONTAP 9 .4以降のリリースでこのオプションを有効にする `-is-multichannel-enabled`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は、次のパラメータも指定できます。

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

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	`vserver cifs options modify -vserver` *`vserver_name options`*
advanced権限レベルで設定	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

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

SMBユーザへのUNIXグループ権限付与の設定

このオプションを設定すると、受信SMBユーザがファイルの所有者でない場合でも、ファイルまたはディレクトリにアクセスするグループ権限を付与できます。

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でも、ファイルまたはディレクトリへのアクセスを無効にしてグループ権限を取得する	`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`

匿名ユーザに対するアクセス制限の設定

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。

タスクの内容

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

匿名ユーザは、ユーザ名と詳細、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。匿名ユーザのアクセスを制御するには、次の3つのアクセス制限設定のいずれかを指定します。

値	説明
`no-restriction` （デフォルト）	匿名ユーザに対するアクセス制限を指定しません。
`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に関してファイルセキュリティをSMBクライアントに提供する方法の概要を管理します。

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で、UNIXセキュリティ形式のデータに関するファイルセキュリティをSMBクライアントに提供する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クライアントから権限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は変更できません。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。

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

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ができます。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理由はいくつかあります。

- UNIXアクセス権を変更するには、UNIXクライアントでマウントを使用する必要があります。

  UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合は、[セキュリティ]タブは使用できません。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ているように見えます。

- SMBを介したアプリケーションを使用している場合、アクセスするファイルやフォルダにNTFS ACLを設定していますが、データがUNIXセキュリティ形式のボリューム上にあると失敗する可能性があります。

  ONTAPでボリュームがFATと報告された場合、アプリケーションはACLの変更を試行しません。

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する

UNIX セキュリティ形式のデータ（ UNIX セキュリティ形式のボリュームと 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。

タスクの内容

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]タブを使用したUNIXアクセス権の管理

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。Kerberosは、ドメインユーザの認証に使用されるデフォルトの方法です。

Kerberos認証

ONTAPは、認証された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サーバまたはKerberos Key Distribution Center（KDC；キー配布センター）サービスは、Active Directoryのセキュリティ原則に関する情報を格納および取得します。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、KDCに直接接続してセッション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の共有情報に基づく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ているSVMを

作成する前に（ `-identity-preserve`SnapMirror構成でオプションがに設定されている `false`）、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を確認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。この情報を使用して、セキュリティ設定が正しいことを確認できます。

タスクの内容

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、または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。

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サーバに対してはコマンドを使用しない `vserver cifs security show`でください。

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,...]`と入力して、使用できるフィールドを指定できます `-fields ?`。

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設定に関する情報の表示

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有効化または無効化

パスワードの複雑さの要件を使用すると、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。

開始する前に

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

タスクの内容

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サーバに対してはコマンドを使用しないで `vserver cifs security modify`ください。

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`
無効にする	`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

次の例では、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ています。

```
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の表示

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

ローカルユーザのパスワードの要件

ローカルユーザアカウントのパスワードの変更

CIFSサーバのKerberosセキュリティ設定を変更します。

許可されるKerberosクロックスキューの最大時間、Kerberosチケットの有効期間、チケットを更新する最大日数など、CIFSサーバのKerberosセキュリティ設定を変更できます。

タスクの内容

コマンドによるCIFSサーバのKerberos設定の変更では `vserver cifs security modify`、パラメータで指定した単一のStorage Virtual Machine（SVM）の設定のみを変更 `-vserver`できます。Active Directoryのグループポリシーオブジェクト（GPO）を使用すると、同じActive Directoryドメインに属するクラスタ上のすべてのSVMのKerberosセキュリティ設定を一元管理できます。

手順

1. 次の操作を1つ以上実行します。

状況	入力するコマンド
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`* デフォルト設定は5分です。
Kerberosチケットの有効期間を時間単位で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` デフォルト設定は10時間です。
チケットの最大更新日数を指定します。	`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上のソケットのタイムアウトを指定します。このタイムアウトを過ぎると、すべてのKDCが到達不能としてマークされます。	`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の表示"

"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。

タスクの内容

- 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ていません。
- LMCompatibilityLevelはSMBクライアント認証にのみ適用され、管理者認証には適用されません。

最低限の認証セキュリティレベルは、サポートされている4つのセキュリティレベルのいずれかに設定できます。

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暗号化の有効化と無効化

AES暗号化を使用したKerberosベースの通信の強力なセキュリティ設定

Kerberosベースの通信による最大限のセキュリティを確保するには、SMBサーバでAES-256暗号化とAES-128暗号化を有効にします。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セッションのセットアップ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
- 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します。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。オプションを使用すると `-advertised-enc-types`、推奨される暗号化タイプを有効にしたり、弱い暗号化タイプを無効にしたりできます。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で使用できるIntel AES New Instructions（Intel AES NI）は、AESアルゴリズムを強化し、サポートされているプロセッサファミリーでのデータ暗号化を高速化します。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暗号化の有効化または無効化

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。SMBサーバでActive Directory（AD）KDCとのKerberosベースの通信にAES暗号化タイプを選択したくない場合は、AES暗号化を無効にすることができます。

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

ONTAPのバージョン	AES暗号化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	○
9.12.1	シユトウ	○
9.11.1以前	シユトウ	いいえ

ONTAP 9 .12.1以降では、AES暗号化はオプションを使用して有効または無効にでき `-advertised-enc-types`ます。このオプションを使用すると、AD KDCにアドバタイズされる暗号化タイプを指定できます。デフォルトの設定はと `des`です `rc4`が、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およびDES暗号化タイプを明示的に無効にすることもできます。AES.11.1以前でONTAP 9は、オプションを使用してAES暗号化を有効または無効にする必要があります `-is-aes-encryption-enabled`。暗号化タイプを指定することはできません。

セキュリティを強化するために、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。パスワードを変更するには、マシンアカウントを含む組織単位（OU）の管理ADクレデンシャルが必要になる場合があります。

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（SnapMirrorの設定でオプションがに設定されている `false`場合 `-identity-preserve`）、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`
無効にする	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

*注:*この `-is-aes-encryption-enabled`オプションはONTAP 9 12.1では廃止されており、今後のリリースで削除される可能性があります。

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

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の **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`
無効にする	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

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

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

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

関連情報

"ドメインユーザがDomain-Tunnelを使用するクラスタにログインできない"

SMB署名を使用したネットワークセキュリティの強化

SMB署名を使用したネットワークセキュリティの概要の強化

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ないようにします。デフォルトでは、ONTAPはクライアントから要求されたときにSMB署名をサポートします。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。

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。この設定がクライアントで無効になっている場合、クライアントのCIFSサーバとの通信は、CIFSサーバの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、のポリシー設定とCIFSサーバの設定に基づき `Microsoft network client: Digitally sign communications (if server agrees)`ます。

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	署名済み
署名が有効になっており、不要である	署名されません	署名済み
署名が無効になっており、必要です	署名済み	署名済み
署名が有効になっており、必要です	署名済み	署名済み

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	署名済み
署名が必要です	署名済み	署名済み

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	○	○	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	○	不要	不要	必須
SMB 3.0	AES-CMAC ：	いいえ	○	不要	不要	必須

Microsoftでは、または `Digitally sign communications (if server agrees)`グループポリシー設定の使用を推奨していません `Digitally sign communications (if client agrees)`。Microsoftでは、レジストリ設定の使用も推奨していません `EnableSecuritySignature`。これらのオプションはSMB 1の動作にのみ影響し、グループポリシー設定または `RequireSecuritySignature`レジストリ設定に置き換えることができます。`Digitally sign communications (always)`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、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

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、新しい暗号化オフロードアルゴリズムによって署名済みSMBトラフィックのパフォーマンスを向上させることができます。SMB署名オフロードは、SMB署名が有効になっている場合はデフォルトで有効になります。

SMB署名のパフォーマンス向上には、AES-NIオフロード機能が必要です。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できます。

ほとんどのWindowsクライアントは、サーバでSMB署名が有効になっている場合、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保護が必要な場合や、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、リプレイアタックに対する保護を必要としないWindowsクライアントで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できます。CIFSサーバでSMB署名を設定する際に選択する設定は、セキュリティ要件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署名を設定する際は、次の推奨事項を考慮してください。

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

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

複数のデータ**LIF**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サーバにはCIFSサーバのレコードエントリが複数含まれ `A`、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サーバには、次のDNSレコードエントリがあり `A`ます。

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

通常の動作では、 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（パスを使用した接続は維持したまま `O:\`）、SMB署名を使用して同じ共有に接続します `S:\`。
4. その結果、ドライブと `S:\`ドライブの両方でデータにアクセスするときにSMB署名が使用され `O:\`ます。

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

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

タスクの内容

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。

   この場合、サポートされているバージョンのONTAPで最初に設定されたSMB署名の設定は、リバートとその後のアップグレードを通じて保持されます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップする際にコマンドのオプション `snapmirror create`で選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、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。

このオプションを（非ID保持）に `false`設定する `-identity-preserve`と、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た場合は、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`
無効にする	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. 次のコマンドの出力で、フィールドの値が目的の値に設定されているかどうかを判断して、SMB署名要求が有効または無効になっていることを確認し `Is Signing Required`ます。 `vserver cifs security show -vserver vserver_name -fields is-signing-required`

例

次の例では、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の確認

CIFSサーバで接続されている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`
SVM上の特定のSession IDを使用する署名されたセッションの詳細	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

例

次のコマンドを実行すると、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
```

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

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

関連情報

SMB署名済みセッションの統計の監視

SMB署名済みセッションの統計の監視

SMBセッションの統計を監視して、確立されたセッションのうち、署名されているセッションと署名されていないセッションを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`と、署名済みSMBセッションの数を監視するためのカウンタが提供され `signed_sessions`ます。この `signed_sessions`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。

  オブジェクトの出力にはSMB 3.0の統計が表示され `smb2`ます。

署名されたセッションの数をセッションの総数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `signed_sessions`。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなけれ

ば、サンプルからデータを表示できます。データ収集を停止すると、固定サンプルが表示されます。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、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+ `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]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、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セッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以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. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。
4. SMB署名統計を表示します。

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
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、オプションのパラメータを指定します `-node`。

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

例

次の例は、vs1というStorage Virtual Machine（SVM）について、SMB 2.xとSMB 3.0の署名統計を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
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、ノードごとに署名されたSMBセッションと確立された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|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
```

次のコマンドは、node2の署名済み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でのSMBサーバでのSMB暗号化要求の設定

SMBアンコウカノカイヨウ

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

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

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

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

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

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

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

SMB サーバ **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	正しくない	SVMのすべての共有でサーバレベルの暗号化が有効になっています。この設定では、SMBセッション全体で暗号化が行われます。
正しい	正しい	共有レベルの暗号化に関係なく、SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
正しくない	正しい	特定の共有で共有レベルの暗号化が有効になっている。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
正しくない	正しくない	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、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行しているクラスタノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワークトラフィックの量に変化はありませんが、クライアントとサーバの両方でCPU使用率が増加したことを示しています。

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、新しい暗号化オフロードアルゴリズムにより、暗号化されたSMBトラフィックのパフォーマンスを向上させることができます。SMB暗号化オフロードは、SMB暗号化が有効になっている場合はデフォルトで有効になります。

SMB暗号化のパフォーマンスを強化するには、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できます。

SMB暗号化は、SMBサーバではデフォルトで無効になっています。SMB暗号化は、暗号化を必要とするSMB共有またはSMBサーバでのみ有効にしてください。SMB暗号化では、ONTAPは要求を復号化し、要求ごとに応答を暗号化する追加の処理を実行します。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**暗号化要求の有効化または無効化

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。

タスクの内容

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コマンドのオプション `snapmirror create`で選択した値 `-identity-preserve`によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

このオプションを（ID保持）に `true`設定する `-identity-preserve`と、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。

このオプションを（非ID保持）に `false`設定する `-identity-preserve`と、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`
無効にする	`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`フィールドには、CIFSサーバでSMB暗号化要求が有効になっているかどうかと、SMB暗号化要求が無効になっているかどうか`false`が表示されます `true`。

例

次の例では、SVM vs1の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
```

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。

タスクの内容

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暗号化統計の監視

SMB暗号化の統計を監視して、確立されたセッションと共有接続のうち、暗号化されているものと暗号化されていないものを確認できます。

タスクの内容

advanced権限レベルでコマンドを実行する `statistics`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を示します。
rejected_unencrypted_sessions	クライアントの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の数
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

- `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。

  オブジェクトの出力にはSMB 3.0の統計が表示され `cifs`ます。暗号化されたセッション数をセッションの合計数と比較する場合は、カウンタの出力とカウンタの出力 `established_sessions`を比較できます `encrypted_sessions`。

  暗号化された共有接続の数を共有接続の総数と比較するには、カウンタの出力とカウンタの出力 `connected_shares`を比較します `encrypted_share_connections`。

- `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、固定サンプルが表示されます。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、傾向を特定するのに役立ちます。

手順

1. 権限レベルをadvancedに設定します。+ `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`*`]`

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、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セッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以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. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。
4. SMB暗号化統計を表示します。

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
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`

表示する情報	入力するコマンド
暗号化された共有接続と接続された共有	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒否された非暗号化セッション	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された非暗号化共有接続
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

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

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暗号化統計情報を監視する方法を示しています。

次のコマンドは、advanced権限レベルに移行します。

```
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セッションと確立されたSMBセッション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、接続されているSMB共有と暗号化されたSMB共有の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共有接続の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）サーバへのクエリに

対して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`。

CIFSトラフィックに対するLDAPの署名と封印は、コマンドのオプションを `vserver cifs security modify`使用して`SVM`で有効にします `-session-security-for-ad-ldap`。

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。

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(`sign`、データ整合性）、署名と封印(`seal`、データの整合性と暗号化を有効にすることができます。また、 `none`署名と封印のどちらも有効にしないことも可能です。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、コマンドのオプション `vserver services name-service ldap client modify`で対応する設定を有効にする必要があります。 `-session-security`

LDAP over TLSの設定

自己署名ルート**CA**証明書のコピーをエクスポートする

LDAP over SSL/TLSを使用してActive Directory通信を保護するには、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、ASCIIテキストファイルに変換する必要があります。ONTAPでは、このテキストファイルを使用して証明書をStorage Virtual Machine（SVM）にインストールします。

開始する前に

CIFSサーバが属しているドメイン用にActive Directory証明書サービスがインストールされ、設定されている必要があります。Active Director証明書サービスのインストールと設定については、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. ドメインコントローラのルートCA証明書をテキスト形式で取得します `.pem`。

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

終了後

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**にインストールする

LDAPサーバへのバインド時にTLSを使用したLDAP認証が必要な場合は、最初に自己署名ルートCA証明書をSVMにインストールする必要があります。

タスクの内容

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、オンライン証明書ステータスプロトコル（OCSP）を使用してデジタル証明書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. 証明書ファイルをテキストエディタで開き `.pem`、で始まる行とで終わる `-----END CERTIFICATE-----`行を含めて証明書をコピーし `-----BEGIN CERTIFICATE-----`、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たことを確認します。 `security certificate show -vserver vserver_name`

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。

10.1以降では、**ONTAP 9**チャネルバインドが**Active Directory**（**AD**）接続とネームサービス**LDAP**接続の両方で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のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。**AD**サーバとの**LDAP**チャネルバインディングを無効または再度有効にするには、コマンドでパラメータを `**vserver cifs security modify**`使用し `**-try-channel-binding-for-ad-ldap**`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"です。

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 `true`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、コマンドを使用してオプションを `vserver services name-service ldap client modify`変更する必要もあります。 `-use-start-tls`

パフォーマンスと冗長性を確保するための**SMB**マルチチャネルの設定

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。

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。

タスクの内容

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 *

クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

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

  クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数の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`

  マルチチャネルセッションごと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、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

  マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

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
```

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する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の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のWindowsユーザからUNIXユーザへのマッピングの設定

デフォルトの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。

タスクの内容

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している必要があります。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ユーザを無効にする	`vserver cifs options modify -default -unix-user ""`

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

2. デフォルトのUNIXユーザ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**ユーザの設定

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）。

タスクの内容

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。

- ホームドメイン、信頼できるドメイン、またはローカルデータベースのドメインコントローラに対してCIFSサーバがユーザを認証できない場合、このオプションが有効になっていると、CIFSサーバはそのユーザをゲストユーザとみなして、指定したUNIXユーザにユーザをマッピングします。
- 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ユーザの設定	`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           : -
   ```

ルートへの**Administrators**グループのマッピング

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。

タスクの内容

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`、ディレクトリにファイルレベルのACLがあり、Administratorsグループはこのを使用してONTAP構成ファイルにアクセスできます。

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	そしたら...。
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`アカウントをrootにマッピングするエントリがない場合でも、Administratorsグループ内のすべてのアカウントはrootとみなされ `/etc/usermap.cfg`ます。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する

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。

タスクの内容

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

コマンドのオプションを `vserver cifs options modify`使用すると、Windowsクライアントのリソース消費を制御できます。これは、ファイルオープン、セッションオープン、Change Notify要求が異常に多い場合など、通常の範囲を超えてリソースを消費するクライアントがある場合に役立ちます。

Windowsクライアントのリソース消費を制御するために、コマンドに次のオプション `vserver cifs options modify`が追加されました。いずれか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に設定されている制限の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ツリーあたりの同一ファイルに対する最大オープン数

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

接続ごとに同じユーザが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*）

デフォルトの制限と現在の設定を表示するには、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によって開始され、サーバによって制御されます。

SMB接続で許可できる未処理要求の最大数は、オプションで制御され `-max-credits`ます。このオプションのデフォルト値は128です。

従来の**oplock**および**oplock**リースでクライアントパフォーマンスを向上

従来の**oplock**および**oplock**リースでクライアントパフォーマンスを向上させる方法の概要

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。クライアントは、対象のファイルへのアクセスが必要であることをサーバに定期的に通知することなく、ファイルの読み取りや書き込みを行うことができます。これにより、ネットワークトラフィックが軽減され、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リースを使用すると、クライアントが自身を起点とする複数のSMBオープンでクライアントのキャッシュ状態を取得して保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティ。共有の作成時にコマンドを使用するか、 `vserver share properties`作成後にコマンドを使用し `vserver cifs share create`ます。
- qtreeプロパティ。qtreeの作成時にコマンドを使用するか、 `volume qtree oplock`作成後にコマンドを使用し `volume qtree create`ます。

oplockを使用する場合の書き込みキャッシュデータ損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を持っていて、別のプロセスがそのファイルを開こうとすると、最初のプロセスが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しなければならないことがあります。その

後、クライアントはoplockを放棄してファイルにアクセスする必要があります。このフラッシュ中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

  キャッシュ自体にエラー処理機能はなく、アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行う場合、書き込みは必ず完了します。キャッシュがネットワークを介してターゲットシステムに書き込みを行う場合、書き込みが完了していないとデータが失われるため、書き込みが完了したと想定する必要があります。

SMB共有の作成時にoplockを有効または無効にする

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、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が有効になります。場合によっては、oplockの無効化が必要になることがあります。oplockは共有ごとに有効または無効にできます。

タスクの内容

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、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	そしたら...。
共有の作成時に共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` 共有でデフォルトの共有プロパティ（、、、 `changenotify`）のみを有効にする場合 `oplocks`は、 `browsable`SMB共有の作成時にパラメータを指定する必要はありません `-share-properties`。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、パラメータとその共有に使用する共有プロパティのリストを指定する必要があります `-share-properties`。
共有の作成時に共有でoplockを無効にする	次のコマンドを入力します。 `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` oplockを無効にする場合は、共有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、プロパティは指定しないで `oplocks`ください。

関連情報

既存のSMB共有でのoplockの有効化と無効化

oplockステータスの監視

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

oplockを使用すると、クライアントがファイルをロックしてコンテンツをローカルにキャッシュできるため、ファイル操作のパフォーマンスが向上します。ここでは、ボリュームまたはqtreeでoplockを有効または無効にするコマンドについて説明します。また、ボリュームおよびqtreeでoplockを有効または無効にできるタイミングについても把握しておく必要があります。

- ボリュームでは、oplockがデフォルトで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に含まれるデフォルトの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（デフォルトで有効）を継承します。ただし、新しいqtreeでoplock設定を指定した場合は、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でoplockを有効にする	`volume qtree oplocks`パラメータがに設定されている `enable`場合 `-oplock-mode`
ボリュームまたはqtreeでoplockを無効にする	`volume qtree oplocks`パラメータがに設定されている `disable`場合 `-oplock-mode`

関連情報

oplockステータスの監視

既存の**SMB**共有での**oplock**の有効化または無効化

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。状況によっては、oplockの無効化が必要になることがあります。また、以前に共有でoplockを無効にしたことがある場合は、oplockを再度有効にすることもできます。

タスクの内容

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。既存の共有では、oplockをいつでも有効または無効にできます。

ステップ

1. 該当する操作を実行します。

状況	そしたら...。
既存の共有を変更して共有でoplockを有効にする	次のコマンドを入力します。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` 追加する共有プロパティをカンマで区切って追加指定できます。 新しく追加したプロパティは、既存の共有プロパティ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を無効にする	次のコマンドを入力します。 `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 削除する共有プロパティをカンマで区切って追加指定できます。 削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しない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キヨウユウノサクセイシノoplockノユウコウカトムコウカ

oplockステータスの監視

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ステータスを監視する

oplockステータスに関する情報を監視および表示できます。この情報を使用して、oplockが設定されているファイル、oplockレベルとoplock状態レベル、およびoplockリースが使用されているかどうかを確認できます。また、手動での解除が必要になる可能性があるロックに関する情報を確認することもできます。

タスクの内容

すべてのoplockに関する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、指定したクライアントIPアドレスまたは指定したパスを持つロックのみを出力に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）とタイプ（oplock）
- ロックの状態
- oplockレベル
- 接続状態とSMBの有効期限
- oplockリースが許可されている場合のOpen Group ID

各パラメータの詳細については、のマニュアルページを参照して `vserver oplocks show`ください。

手順

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

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にはoplockレベルが設定されてい `read-batch`ます。

```
cluster1::> vserver locks show

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

次の例は、パス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`。このファイルでは、IPアドレスがのクライアントに対してoplockレベルで`10.3.1.3`oplockリースが許可されてい `batch`ます。

詳細情報を表示する場合は、oplockと共有ロックの情報を個別に出力します。この例は、oplockセクションの出力のみを示しています。

```
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キヨウユウノサクセイシノoplockノユウコウカトムコウカ

既存のSMB共有でのoplockの有効化と無効化

ボリュームおよびqtreeでoplockを有効または無効にするコマンド

SMBサーバへのグループポリシーオブジェクトの適用

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

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UUID（Universally Unique Identifier）のリスト

関連情報

ダイナミックアクセス制御（DAC）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。

- 監査ポリシーの詳細設定：

  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。

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

  > 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

GPOを使用して設定し `Registry`ます。

- グループポリシーの更新間隔のランダムオフセット

  GPOを使用して設定し `Registry`ます。

- 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ています。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
  - Disabled GPOを使用して設定します `Registry`。

- 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 GPOを使用して設定されます `Registry`。

> 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のログオン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
      - 障害イベントの監査
      - GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit logon events`。

        > 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、監査対象のオブジェクトアクセス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
- 障害イベントの監査
- GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit object access`。

> 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
  - GPOの設定を `Event Log`使用して設定されたイベントログを上書きしないでください（ログを手動でクリア） `Retention method for security log`。
- 最大ログサイズ

  監査ログの最大サイズを指定します。

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

> 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を介してファイルセキュリティが適用されるファイルまたはディレクトリのリストを指定します。

GPOを使用して設定し`File System`ます。

> SVM内にファイルシステムセキュリティGPOを設定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値を分単位で指定します。

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

- 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。

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

- チケットの更新の有効期間

  ユーザチケット更新の最大有効期間を日数で指定します。

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

- ユーザ権限の割り当て（権限）

  - 所有権の取得

    セキュリティ保護可能なオブジェクトの所有権を取得する権限を持つユーザおよびグループのリストを指定します。

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

  - 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、個 々 のリソース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。

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

  - 通知権限の変更（トラバースチェックのバイパス）

    ユーザとグループにトラバースするディレクトリに対する権限がない場合でも、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。

  ユーザがファイルおよびディレクトリの変更通知を受信するには、同じ権限が必要です。GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Bypass traverse checking`。

- 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。

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

- restrict anonymous （匿名の制限

  匿名ユーザに対する制限を指定します。次の3つのGPO設定が含まれます。

  - 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対して許可される追加の権限を決定します。このオプションが有効になっている場合は、ONTAPでと表示され `no-enumeration`ます。

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

- 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は、SAMアカウントと共有の匿名列挙を許可するかどうかを指定します。このオプションが有効になっている場合は、ONTAPでと表示され `no-enumeration`ます。

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

- 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。このオプションが有効になっている場合は、ONTAPでと表示され `no-access`ます。

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

  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、出力フィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示 `Resultant restriction for anonymous user`されます。考えられる制限は次のとおりです。

° `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。この制限は、GPOが有効になっている場合に発生し `Network access: Restrict anonymous access to Named Pipes and Shares`ます。

° `no-enumeration`

匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAMアカウントと共有を列挙することはできません。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- `Network access: Do not allow anonymous enumeration of SAM accounts`または `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPO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、列挙を使用できます。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- GPOと `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOの両方 `Network access: Do not allow anonymous enumeration of SAM accounts`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、組み込みグループまたはユーザ定義グループのメンバーシップを一元管理できます。グループポリシーを使用して制限されたグループを適用すると、CIFSサーバローカルグループのメンバーシップは、適用されたグループポリシーで定義されているメンバーシップリストの設定に一致するように自動的に設定されます。

  GPOを使用して設定し `Restricted Groups`ます。

- 集約型アクセスポリシーの設定

  集約型アクセスポリシーのリストを指定します。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サーバでのGPOサポートの有効化と無効化

ダイナミックアクセス制御（DAC）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

匿名ユーザに対するアクセス制限の設定

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、システムが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"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMBサーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- SMBサーバ管理ステータスがオンである必要があります。
- GPOが設定され、SMBサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位（OU）に適用されている必要があります。
- SMBサーバでGPOのサポートが有効になっている必要があります。

CIFSサーバ上でのGPOサポートの有効化と無効化

CIFSサーバでGroup Policy Object（GPO；グループポリシーオブジェクト）のサポート

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

タスクの内容

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
GPOを有効にする	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOを無効にする	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. GPOサポートが目的の状態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

次の例では、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サーバでのGPO設定の手動更新

GPO設定に関する情報の表示

SMBサアハテノGPOノコウシンホウホウ

CIFSサアハテノGPOノコウシンノカイヨウ

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分ごとに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を更新して新しいGPOポリシー設定を適用する場合は、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーできます。

- デフォルトでは、すべてのGPOが90分ごとに検証され、必要に応じて更新されます。

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

  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は16時間ごとに更新されます。

  ONTAPは、変更の有無にかかわらず、16時間ごとに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、すべてのGPOを手動で更新できます。

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

関連情報

CIFSサーバでのGPO設定の手動更新

CIFSサーバでのGPO設定の手動更新

CIFSサーバのGroup Policy Object（GPO；グループポリシーオブジェクト）設定をすぐに更新する場合は、設定を手動で更新できます。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する

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

タスクの内容

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ことも、CIFSサーバに適用されているGPO設定に関する情報のみを表示することもできます。

手順

1. 次のいずれかの操作を実行して、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デテイギ	`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、CIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

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

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
```

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

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
```

```
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

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

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

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
```

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

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
```

```
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

関連情報

CIFSサーバでのGPOサポートの有効化と無効化

制限されたグループの**GPO**に関する詳細情報を表示する

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

タスクの内容

デフォルトでは、次の情報が表示されます。

- グループポリシー名
- グループポリシーバージョン
- リンク

  グループポリシーが設定されているレベルを指定します。指定可能な出力値は次のとおりです。

- `Local`グループポリシーがONTAPで設定されている状況
- `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Organizational Unit（OU；組織単位）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
- 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、ここにリスト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ができます。

ステップ

1. 次のいずれかの操作を実行して、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デテイギ	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`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
```

次の例では、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する

Active Directoryで定義されている集約型アクセスポリシーに関する詳細情報を表示できます。また、Group Policy Object（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に関する情報も表示できます。

タスクの内容

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
- 更新日時
- メンバールール

ワークグループモードのCIFSサーバはGPOをサポートしていないため表示されません。

ステップ

1. 次のいずれかの操作を実行して、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デテイギ	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFSサアハニテキヨウ	`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

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

GPO設定に関する情報の表示

集約型アクセスポリシールールに関する情報の表示

集約型アクセスポリシールールに関する情報を表示する

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。また、集約型アクセスポリシーのGPO（グループポリシーオブジェクト）を介してCIFSサーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

タスクの内容

定義済み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
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 更新日時
- 現在の権限
- 推奨される権限
- ターゲットリソース

集約型アクセスポリシーに関連付けられた、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デテイギ	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`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ている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、クラスタ上の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ている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

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

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
ONTAPがADサービスと同期されている場合のドメインアカウントパスワードの変更	`vserver cifs domain password change`
ONTAPがADサービスと同期されていない場合のドメインアカウントパスワードのリセット	`vserver cifs domain password reset`
SMBサーバでコンピュータアカウントパスワードの自動変更を設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
SMBサーバ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の管理

検出されたサーバに関する情報を表示する

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

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サーバの停止と起動

サーバのリセットと再検出

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

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 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

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

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

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

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

関連情報

検出されたサーバに関する情報の表示

CIFSサーバの停止と起動

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。これにより、検出対象をサイトまたは優先DCのプールに限定できます。これにより、環境によってはパフォーマンスが向上する可能性があります。

タスクの内容

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

ONTAP 9 .3以降のリリースでは `discovery-mode`、コマンドのパラメータを `cifs domain discovered-servers`使用して次の検出オプションのいずれかを選択できます。

- ドメイン内のすべてのDCが検出されます。
- ローカルサイトのDCだけが検出されます。

  SMBサーバのパラメータは、 `default-site`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。

- サーバ検出は実行されず、優先DCのみを使用してSMBサーバを設定します。

  このモードを使用するには、まずSMBサーバの優先DCを定義する必要があります。

開始する前に

advanced権限レベルが必要です。

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}`

   パラメータのオプション `mode`：

   - `all`

     使用可能なすべてのDCを検出します（デフォルト）。

   - `site`

     DC検出をサイトに限定します。

   - `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の追加

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1つ以上のドメインコントローラを追加できます。

タスクの内容

指定したドメインの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は、新しいリストが既存のリストにマージされます。

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*`、…には、優先ドメインコントローラの1つ以上のIPアドレスを優先順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を追加、表示、削除するコマンドについて説明します。

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

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**接続を有効にする

SMB.1以降では、ONTAP 9バージョン2.0からドメインコントローラへの接続を有効にすることができます。この処理は、ドメインコントローラでSMB 1.0を無効にしている場合に必要です。ONTAP 9 .2以降では、SMB2がデフォルトで有効になっています。

タスクの内容

コマンドオプションを使用すると、 `smb2-enabled-for-dc-connections`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では有効になり、SMB 2.0では無効になります。ONTAP 9 .2のシステムデフォルトは、SMB 1.0では有効、SMB 2.0では有効です。ドメインコントローラが最初にSMB 2.0をネゴシエートできない場合は、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SMB 1.0が無効になっている場合は、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。

詳細については以下を参照してください。

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

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

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. オプションを使用して、該当するコマンドを実行し `smb2-enabled-for-dc-connections`ます。

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`
無効にする	`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する

ONTAP 9 .8以降では、ドメインコントローラへの接続を暗号化するように指定できます。

タスクの内容

このオプションをに設定 `true`すると、ONTAPでドメインコントローラ（DC）通信の暗号化が必要になります `-encryption-required-for-dc-connection`。デフォルトはです。 `false`暗号化はONTAP 3でしかサポートされないため、このオプションを設定するとSMB3プロトコルのみがSMB-DC接続に使用されます。

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

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**環境で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。

Kerberos以外の環境でストレージにアクセスする場合に**null**セッションを使用する概要

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提供方法

nullセッション共有は認証を必要としないため、nullセッションアクセスを必要とするクライアントは、ストレージシステム上でIPアドレスをマッピングする必要があります。

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、共有の列挙などの特定の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では、オプションを使用してWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous`。これにより、マッピングされていないnullユーザがシステムリソースを表示またはアクセスできる範囲を制御できます。たとえば、共有の列挙とipc$共有（非表示の名前付きパイプ共有）へのアクセスを無効にすることができます。オプションの詳細については、 `vserver cifs options modify`および `vserver cifs options show`のマニュアルページを参照して `–restrict-anonymous`ください。

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、nullセッションクライアントにのみ適用されるストレージシステムリソース権限を設定できます。

ONTAPのコマンドセットでは `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アドレスを指定できます。nullユーザ用のグループを作成したら、nullセッションにのみ適用されるストレージシステムリソースおよびリソース権限に対するアクセス制限を指定できます。nullユーザは匿名ログオンとして識別されます。nullユーザはどのホームディレクトリにもアクセスできません。

マッピングされたIPアドレスからストレージシステムにアクセスするすべての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アクセスを防止するために、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

匿名ユーザに対するアクセス制限の設定

nullユーザにファイルシステム共有へのアクセスを許可する

nullセッションクライアントによるストレージシステムリソースへのアクセスを許可するには、nullセッションクライアントが使用するグループを割り当て、nullセッションクライアントのIPアドレスを記録して、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のリストに追加します。

手順

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

   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. コマンドを使用し `vserver name-mapping show`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. コマンドを使用し `vserver cifs options modify –win-name-for-null-user`て、nullユーザにWindowsメンバーシップを割り当てます。

   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. コマンドを使用し `vserver cifs options show`て、nullユーザがWindowsユーザまたはグループにマッピングされていることを確認します。

   ```
   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エイリアスの管理の概要

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、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。

NetBIOSエイリアスのリストは、SMBサーバの作成時、またはSMBサーバの作成後にいつでも指定できます。リストにNetBIOSエイリアスを追加または削除することはいつでもできます。SMBサーバには、NetBIOSエイリアスリスト内の任意の名前を使用して接続できます。

関連情報

NetBIOS over TCP接続に関する情報の表示

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。

タスクの内容

- NetBIOSエイリアス名は15文字以内で指定します。
- 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。
   - NetBIOSエイリアスのリストが現在空の場合は、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の表示

NetBIOSエイリアスリストからNetBIOSエイリアスを削除する

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。

タスクの内容

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。パラメータの値に `-netbios -aliases` 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 `-`。

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のリスト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（CIFSサーバの詳細情報の一部）	`vserver cifs show -instance`

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

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

```
Vserver: vs1

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

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

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

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

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の確認

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、接続の問題をトラブルシューティングするときに役立ちます。

タスクの内容

SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するには、パラメータを使用する必要があります `-instance`。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、フィールドの出力 `NetBIOS Name`は（ハイフン）になります `-`。

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、Session ID 1とのSMB接続に使用される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サーバタスクの管理

CIFSサーバの停止または起動

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タスクを実行する場合は、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することもできます。

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サーバを停止する	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFSサーバを起動する
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground`コマンドをフォアグラウンド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。こ

のパラメータを入力しない場合、このパラメータはに設定され `true`、フォアグラウンドでコマンドが実行されます。

2. コマンドを使用して、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`。

例

次のコマンドは、SVM vs1でCIFSサーバを起動します。

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

cluster1::> vserver cifs show -vserver vs1

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

関連情報

検出されたサーバに関する情報の表示

サーバのリセットおよび再検出

別のOUへのCIFSサーバの移動

CIFSサーバの作成プロセスでは、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組織単位（OU）CN=Computersが使用されます。CIFSサーバはセットアップ後に別の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オブジェクトを探します。
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オブジェクトが配置されます。

SMBサーバ移動前にSVM上の動的DNSドメインを変更する

SMBサーバを別のドメインに移動するときに、Active Directory統合DNSサーバでSMBサーバのDNSレコードが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）の動的DNS（DDNS）を変更する必要がありま

す。

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。

タスクの内容

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サービスの設定"

SVMのActive Directoryドメインへの参加

コマンドを使用してドメインを変更すると、既存のSMBサーバを削除せずにStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify`。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。

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サーバと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。

タスクの内容

- 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、コマンドのマニュアルページを参照して `vserver cifs modify`ください。新しいドメイン用にDNSを再設定する必要がある場合は、コマンドのマニュアルページを参照して `vserver dns modify`ください。

   SMBサーバ用のActive Directoryマシンアカウントを作成するには、.comドメイン内のコンテナ *example*`にコンピュータを追加するための十分なPrivilegesを備えた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。

ONTAP 9 .7以降では、権限のあるWindowsアカウントの名前とパスワードを指定する代わりに、keytabファイルのURIをAD管理者から提供することができます。URIを受け取ったら、コマンドのパラメータ `vserver cifs`にそのURIを含め `-keytab-uri`ます。

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する

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

ステップ

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

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

例

次の例は、「 cluster1 」について表示される 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サーバを停止する	`vserver cifs stop`
SMBサーバを起動する	`vserver cifs start`
SMBサーバを削除する	`vserver cifs delete`
SMBサーバ用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のローカルユーザとローカルグループへの影響"

NetBIOSネームサービスを有効にする

ONTAP 9以降では、NetBIOSネームサービス（NBNS、Windowsインターネットネームサービスまたは 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になっている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。このようなブロードキャストをNBNSが必要な構成に限定するには、新しいCIFSサーバに対してNBNSを明示的に有効にする必要があります。

開始する前に

- すでにNBNSを使用していて、ONTAP 9にアップグレードする場合は、このタスクを実行する必要はありません。NBNSは以前と同様に機能します。
- NBNSはUDP（ポート137）でイネーブルになっています。
- 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を使用する

IPv6の使用要件

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のライセンス要件

SMBのライセンスがある場合、IPv6に特別なライセンスは必要ありません。SMBライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMBプロトコルのバージョン

- SVMについては、ONTAPで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ます。次に、Microsoft Windowsクライアントおよびサーバの IPv6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Active Directoryサービス（DNS、LDAP、CLDAP、Kerberosの各サービス）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サービスにデフォルトでIPv6が使用されます。IPv6接続を介した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クライアントの最新情報については、を参照して"Interoperability Matrix"ください。

NTドメインはIPv6ではサポートされていません。

その他の**CIFS**サービスのサポート

ONTAPでは、SMBファイル共有とActive Directoryサービスに加えて、次の項目に対しても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（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODXコピーオフロード、自動ノードリファーラル、以前のバージョン機能など
- ファイルアクセス管理サービス（Windowsのローカルユーザおよび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と監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、SMBアクティビティの監視など）
- NASのマルチプロトコルの監査
- FPolicy
- 共有の継続的可用性、監視プロトコル、およびリモートVSS（Hyper-V over SMB構成で使用）

ネームサービスと認証サービスのサポート

IPv6では、次のネームサービスとの通信がサポートされます。

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

CIFSサーバでのIPv6を使用した外部サーバへの接続方法

要件に応じ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際に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

  外部サーバに接続しようとする場合、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ある必要が

あります。たとえば、IPv6アドレスに接続する場合、CIFSサーバをホストするStorage Virtual Machine（SVM）には、ソース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、ソース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たサーバの場合、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、および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、どちら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サーバへの接続で引き続きIPv4アドレスを使用できるように、DNSネームサービスの設定でIPv4アドレスを使用できます。DNSネーム サービスの設定時には、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。
- LDAPサーバへの接続

  SVMがLDAPサーバに接続するときにIPv6を使用するかどうかは、LDAPクライアントの設定によって異なります。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サーバへの接続で引き続きIPv4アドレスを使用できるように、LDAPクライアント設定で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完了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が有効になっています。SMBアクセス用のIPv6データLIFを設定できます。

関連情報

IPv6 SMBセッション情報の監視および表示

"ネットワーク管理"

SMBでのIPv6の無効化

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が有効なインターフェイスの管理については、クラスタ管理者に問い合わせてください。

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

"ネットワーク管理"

IPv6 SMBセッションに関する情報を監視および表示する

IPv6ネットワークを使用して接続されているSMBセッションに関する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その他の有用な情報と同様に、IPv6を使用して接続しているクライアントを特定する場合に役立ちます。

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る	`vserver cifs session show -vserver` *`vserver_name`* `-instance`

確認する項目	入力するコマンド
IPv6は、指定したLIFアドレスを介したSMBセッションに使用されます。	`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。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。