SMBサーバのセキュリティ設定の管理

ONTAP 9

NetApp
February 12, 2026

目次

SMBサーバのセキュリティ設定の管理

ONTAP SMBクライアント認証の処理について学ぶ

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

Kerberos認証

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

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

NTLM認証

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

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

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

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

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

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

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

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

ONTAP SMB サーバのセキュリティ設定に関する情報を表示します

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

タスク概要

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

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

手順

1. 次のいずれかを実行します。

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

例

次の例は、SVM vs1のすべてのセキュリティ設定を表示します。

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

Vserver: vs1

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

表示される設定は、実行中のONTAPバージョンによって異なります。

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

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

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

関連情報

GPO設定に関する情報の表示

ローカルSMBユーザのONTAPパスワードの複雑さを設定する

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

開始する前に

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

タスク概要

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

手順

1. 次のいずれかを実行します。

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

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

例

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

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

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

関連情報

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

ONTAP SMBサーバのKerberosセキュリティ設定を変更する

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

タスク概要

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

手順

1. 次の操作を1つ以上実行します。

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

2. Kerberosセキュリティ設定を確認します。

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

例

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

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

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

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

関連情報

"サーバーのセキュリティ設定に関する情報を表示する"

"サポートされるGPO"

"CIFSサーバへのグループ ポリシー オブジェクトの適用"

ONTAP SMBサーバの最小認証セキュリティレベルを設定する

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

タスク概要

- ワークグループ モードのSMBサーバでは、NTLM認証のみがサポートされます。Kerberos認証はサポートされません。
- LMCompatibilityLevelはSMBクライアント認証にのみ適用され、管理者認証には適用されません。

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

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

手順

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

関連情報

Kerberosベースの通信用にAES暗号化を設定する

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

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

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

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

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

SMBサーバを作成すると、ドメイン コントローラによってActive Directoryにコンピュータ マシン アカウントが作成されます。この時点で、KDCは特定のマシン アカウントの暗号化機能を認識するようになっています。これ以降は、認証の際にクライアントがサーバに提示するサービス チケットを暗号化するために特定の暗号化タイプが選択されます。

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

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

関連情報

サーバーのセキュリティ設定を変更する

ONTAP SMB Kerberosベースの通信にAES暗号化を設定する

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

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

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

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

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

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

例 **1.** 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

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

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

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

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

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

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

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

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

関連情報

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

SMB署名を使用したネットワーク セキュリティの強化

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

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

でSMB署名を必須にするように設定できます。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ONTAP SMB署名のパフォーマンスへの影響について学ぶ

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

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

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

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

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

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

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

ONTAP SMB署名設定の推奨事項

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

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

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

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

複数のデータLIFに対するONTAP SMB署名設定について学習します

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

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

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

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

次の例を考えてみましょう。

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

受信**SMB**トラフィック用の**ONTAP**署名を設定する

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

タスク概要

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

次の状況では、SMB署名はデフォルトで無効になりません。

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

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

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

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

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

手順

1. 次のいずれかを実行します。

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

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

例

次の例は、SVM vs1でSMB署名要求を有効にします。

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

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

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

関連情報

- "snapmirror create"

ONTAPSMBセッションが署名されているかどうかを確認する

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

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

手順

1. 次のいずれかを実行します。

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

例

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

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

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

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

関連情報

SMB署名済みセッションの統計の監視

ONTAP SMB署名セッション統計を監視する

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

タスク概要

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

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

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

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

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

手順

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

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

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

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

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

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

4. 次のコマンドによりSMB署名統計を表示します。

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

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

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

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

例

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

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

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

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

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

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

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

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

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

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

次のコマンドで、admin権限レベルに戻ります。

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

関連情報

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

SMB経由のデータ転送でのSMBサーバのSMB暗号化要求の設定

ONTAP SMB暗号化について学ぶ

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

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

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

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

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

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

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

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

SMB サーバの SMB 暗号化が有効	共有暗号化データ設定が有効	サーバー側の暗号化の動作
False	True	共有ごとに共有レベルの暗号化が有効になります。この設定では、ツリー接続から暗号化が行われます。
False	False	暗号化はすべて無効になります。

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

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

ONTAP SMB暗号化のパフォーマンスへの影響について学ぶ

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

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

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

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

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

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

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

受信トラフィックのONTAP SMB暗号化を有効または無効にする

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

タスク概要

CIFSサーバーでSMB暗号化を有効にすると、CIFSサーバー上のすべての共有に適用されます。CIFSサーバー

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

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

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

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

手順

1. 次のいずれかを実行します。

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

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

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

例

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

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

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

関連情報

- "snapmirror create"

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

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

タスク概要

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

- `unencrypted`

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

- `partially-encrypted`

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

- `encrypted`

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

手順

1. 次のいずれかを実行します。

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

...に関する情報を表示する場合	コマンドを入力してください...
指定されたSVM上の特定のセッションIDの暗号化設定	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

例

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

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

ONTAP SMB暗号化統計を監視する

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

タスク概要

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

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

これらのカウンタでは、次の統計オブジェクトを利用できます。

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

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

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

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

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

手順

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

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

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

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

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

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

4. SMB暗号化統計情報を表示します。

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

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

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

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

例

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

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

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

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

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

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

2 entries were displayed
```

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

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

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

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

1 entry was displayed.
```

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

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

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

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

2 entries were displayed.
```

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

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

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

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

1 entry was displayed.
```

関連情報

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

LDAPセッションの通信の保護

ONTAP SMB LDAP署名とシーリングについて学ぶ

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会に対するLDAPセッション セキュリティを有効にすることができます。Storage Virtual Machine（SVM）のCIFSサーバ セキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

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

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

ONTAP SMBサーバでLDAP署名とシーリングを有効にする

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

開始する前に

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

手順

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

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

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

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

LDAP over TLSの設定

ONTAP SMB SVMの自己署名ルートCA証明書をエクスポートする

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

す。

開始する前に

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

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

手順

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

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

終了後の操作

SVMに証明書をインストールします。

関連情報

"Microsoft TechNetライブラリ"

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

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

タスク概要

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

手順

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

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

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

関連情報

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

ONTAP SMBサーバで**LDAP over TLS**を有効にする

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

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

詳細については、以下を参照してください。

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

手順

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

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

著作権に関する情報

商標に関する情報