SMBサーバのセキュリティ設定を管理します。

ONTAP 9

NetApp
December 20, 2024

目次

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。

SMB署名ポリシーがCIFSサーバとの通信に与える影響

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

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

ここでは、 Microsoft クライアントの 2 つの SMB 署名ポリシーについて説明します。

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

  この設定は、クライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定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。

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。
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
```

クライアントが暗号化された**SMB**セッションを使用して接続中かどうかの確認

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`

表示する情報	入力するコマンド
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

カウンタ名	説明
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*]`
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`

サーバで **LDAP over TLS** を有効にします

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

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**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`

著作権に関する情報

商標に関する情報