SMB サーバのセキュリティ設定を管理します

ONTAP 9

NetApp
April 24, 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。ドメインユーザの認証に使用されるデフォルトの方法は Kerberos です。

Kerberos 認証

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

Kerberos は Active Directory のプライマリ認証サービスです。Kerberos サーバの Kerberos Key Distribution Center （ KDC ；キー配布センター）サービスは、 Active Directory に対してセキュリティプリンシパルに関する情報の格納や取得を行います。NTLM モデルとは異なり、 SMB サーバなどの別のコンピュータとのセッションを確立する Active Directory クライアントは、直接 KDC にアクセスしてセッションのクレデンシャルを取得します。

NTLM認証

NTLM クライアント認証は、パスワードに基づくユーザ固有のシークレットを共有し、チャレンジ - 応答プロトコルを使用して行われます。

ユーザがローカルのWindowsユーザアカウントを使用してSMB接続を作成した場合、認証はSMBサーバによってNTLMv2を使用してローカルに行われます。

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

IDが保持されないディザスタリカバリデスティネーションとして設定されたSVMを作成する前に（を参照） `-identity-preserve` オプションはに設定されています `false` （SnapMirror構成の場合）デスティネーションSVMでのSMBサーバセキュリティ設定の管理方法について理解しておく必要があります。

- デフォルト以外の SMB サーバセキュリティ設定はデスティネーションにレプリケートされません。

  デスティネーション SVM 上に SMB サーバを作成した場合、すべての SMB サーバセキュリティ設定はデフォルト値に設定されます。SVM のディザスタリカバリ先を初期化、更新、再同期した場合、ソース上の SMB サーバのセキュリティ設定はデスティネーションにレプリケートされません。

- デフォルト以外の SMB サーバセキュリティ設定は手動で設定する必要があります。

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

SMBサーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine （ SVM ）上の SMB サーバセキュリティ設定に関する情報を表示できます。この情報は、セキュリティ設定が正しいかどうかを確認する際に役立ちます。

このタスクについて

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

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

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した SVM のすべてのセキュリティ設定	`vserver cifs security show -vserver` *`vserver_name`*
SVM の特定のセキュリティ設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 入ることができます `-fields ?` 使用できるフィールドを決定します。

例

次の例は、 SVM vs1 のすべてのセキュリティ設定を表示します。

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

Vserver: vs1

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

表示される設定は、実行中の ONTAP のバージョンによって異なります。

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

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

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

関連情報

GPO 設定に関する情報を表示します

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

パスワードの複雑さの要件を有効にすると、 Storage Virtual Machine （ SVM ）上のローカル SMB ユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この機能は、いつでも無効にして再度有効にす

ることができます。

作業を開始する前に

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

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

手順

1. 次のいずれかを実行します。

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

2. パスワードの複雑さの要件に関するセキュリティ設定を確認します。 `vserver cifs security show -vserver` *`vserver_name`*

例

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

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

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

関連情報

CIFS サーバのセキュリティ設定に関する情報を表示する

ローカルユーザおよびローカルグループを使用した認証と許可

ローカルユーザパスワードの要件

ローカルユーザのアカウントパスワードを変更しています

CIFS サーバの Kerberos セキュリティ設定を変更します

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

このタスクについて

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

手順

1. 次の操作を 1 つ以上実行します。

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

2. Kerberos セキュリティ設定を確認します。

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

例

次の例では、 SVM vs1 の Kerberos セキュリティ設定を「 Kerberos Clock Skew 」に 3 分、「 Kerberos Ticket Age 」に 8 時間に変更しています。

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

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

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

関連情報

"CIFS サーバのセキュリティ設定に関する情報を表示する"

"サポートされる GPO"

"CIFS サーバへのグループポリシーオブジェクトの適用"

SMBサーバの最小認証セキュリティレベルを設定する

SMB サーバの *LMCompatibilityLevel* とも呼ばれる SMB サーバの最小セキュリティレベルを設定することで、 SMB クライアントアクセスのビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルは、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。

このタスクについて

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

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

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

手順

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

関連情報

Kerberos ベースの通信用の AES 暗号化を有効または無効にします

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

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

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

- AES 256
- AES 128
- DES （デス
- RC4-HMAC

Kerberos 通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、 SVM の Kerberos 通信で AES

暗号化を有効にする必要があります。

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

ONTAP 9.12.1以降では、Active Directory（AD）KDCにアドバタイズする暗号化タイプを指定できます。を使用できます `-advertised-enc-types` 推奨される暗号化タイプを有効にするオプション。また、弱い暗号化タイプを無効にする場合にも使用できます。方法をご確認ください "Kerberosベースの通信の暗号化タイプを有効または無効にします"。

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

関連情報

CIFS サーバの Kerberos セキュリティ設定の変更

Kerberos ベースの通信用の AES 暗号化を有効または無効にします

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

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

ONTAPバージョン	**AES**暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルトでは	はい。
9.12.1:	手動で実行する	はい。
9.11.1以前	手動で実行する	いいえ

ONTAP 9.12.1以降では、を使用してAES暗号化を有効または無効にします `-advertised-enc-types` オプション。AD KDCにアドバタイズする暗号化タイプを指定できます。デフォルト設定はです `rc4` および `des`` ただし、`AES`タイプを指定すると、`AES`暗号化が有効になります。オプションを使用して、弱い`RC4`暗号化タイプと`DES`暗号化タイプを明示的に無効にすることもできます。`ONTAP 9.11.1`以前では、 `-is-aes-encryption-enabled` AES暗号化を有効または無効にするオプションを指定できません。また、暗号化タイプは指定できません。

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

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（ `-identity-preserve` オプションはに設定されています `false` SnapMirrorの設定では、デフォルト以外のSMBサーバセキュリティ設定はデスティネーションにレプリケートされません。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を手動で有効にする必要があります。

例 **1.** 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
無効	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

注： `-is-aes-encryption-enabled` オプションはONTAP 9.12.1では廃止され、以降のリリースでは削除される可能性があります。

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の **AES** 暗号化タイプの設定	入力するコマンド
有効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
無効	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

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

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

SMB 署名を使用してネットワークのセキュリティを強化します

SMB 署名を使用してネットワークセキュリティの概要を強化します

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

SMB 署名ポリシーが CIFS サーバとの通信に与える影響

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

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

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

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

  この設定は、クライアントの SMB 署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定をクライアントで無効にすると、クライアントの CIFS サーバとの通信は、 CIFS サーバ上の SMB 署名の設定によって異なります。

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

  この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB署名の動作はのポリシー設定に基づきます `Microsoft network client: Digitally sign communications (if server agrees)` およびCIFSサーバの設定。

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

クライアントと CIFS サーバの SMB 署名設定の有効な結果は、 SMB セッションで SMB 1.0 が使用されるか SMB 2.x 以降が使用されるかによって異なります。

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

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は無効になっており、不要です	署名されません	署名
署名が有効になっており、不要である	署名されません	署名
署名が無効になっており、必要です	署名	署名
署名が有効になっており、必要です	署名	署名

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

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

SMB 2.x クライアントと SMB 3.0 クライアントでは、 SMB 署名は常に有効になります。無効にすることはできません。

クライアント	**ONTAP —** 署名は不要	**ONTAP —** 署名が必要
署名は不要です	署名されません	署名
署名が必要です	署名	署名

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

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

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

SMB 署名のパフォーマンスへの影響

SMB セッションで SMB 署名を使用すると、 Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（ SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

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

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、署名済み SMB トラフィックのパフォーマンスが向上します。SMB 署名オフロードは、 SMB 署名が有効になっている場合にデフォルトで有効になります。

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

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

ネットワーク、 ONTAP 9 のバージョン、 SMB のバージョン、および SVM の実装方法に応じて SMB 署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

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

SMB 署名の設定に関する推奨事項

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

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

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

Windows クライアントのセキュリティ設定の詳細については、 Microsoft のマニュアルを参照してください。

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

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

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

ようになります A レコードエントリ：

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

通常の動作では、 SMB 署名要求の設定を変更すると、クライアントからの新しい接続だけが SMB 署名の設定変更の影響を受けます。ただし、この動作には例外があります。クライアントに共有への既存の接続がある場合、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存の SMB 接続の両方で新しい SMB 署名の要件が適用されます。

次の例を考えてみましょう。

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

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

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

このタスクについて

デフォルトでは、 SMB 署名要求は無効になっています。SMB 署名要求はいつでも有効または無効にできます。

> 次の状況では、 SMB 署名はデフォルトで無効になりません。
>
> 1. SMB 署名要求が有効になっており、クラスタが SMB 署名をサポートしていないバージョンの ONTAP にリバートされた。
> 2. その後、クラスタが SMB 署名をサポートするバージョンの ONTAP にアップグレードされた。
>
> このような場合は、サポートされているバージョンの ONTAP で最初に行われた SMB 署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係を設定する際にで選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

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

を設定した場合は `-identity-preserve` オプションをに設定します `false` （ID保持なし）。SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションの CIFS サ

ーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 署名要求を有効にしている場合は、デスティネーション SVM で SMB 署名要求を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

SMB 署名要求の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. での値を確認して、SMB署名要求が有効か無効かを確認します `Is Signing Required` 次のコマンドの出力のフィールドは、目的の値に設定されます。 `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

例

次の例は、 SVM vs1 で SMB 署名要求を有効にします。

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

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

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

SMB セッションが署名されているかどうかを確認します

CIFS サーバで接続中の SMB セッションに関する情報を表示できます。この情報を使用して、 SMB セッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した Storage Virtual Machine （ SVM ）上の署名されたすべてのセッション	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
SVM 上の指定したセッション ID を持つ署名されたセッションの詳細です	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

例

次のコマンドを実行すると、 SVM vs1 上の署名されたセッションに関するセッション情報が表示されます。デフォルトのサマリー出力には ' Is Session Signed 出力フィールドは表示されません

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

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報が表示されます。

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

関連情報

SMB 署名済みセッションの統計の監視

SMB 署名済みセッションの統計を監視します

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

このタスクについて

。 `statistics` advanced権限レベルでコマンドを実行すると、が表示されます `signed_sessions` 署名済みSMBセッションの数を監視するために使用できるカウンタ。。 `signed_sessions` カウンタには、次の統計オブジェクトがあります。

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

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

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

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

ば、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

手順

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

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

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

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

表示する情報	入力するコマンド
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	署名されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

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

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

例

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

次のコマンドは、 advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

次のコマンドは、ノードが署名した SMB セッションと確立されたセッションをサンプルから表示します。

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

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

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

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

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

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

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

次のコマンドは、 admin 権限レベルに戻ります。

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

関連情報

SMB セッションが署名されているかどうかの確認

"パフォーマンスの監視と管理の概要"

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

SMB暗号化の概要

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

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

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

SVM での SMB 暗号化は、次の 2 つの設定によって制御されます。

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

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

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

SMB サーバ **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しいです	いいえ	SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、 SMB セッション全体で暗号化が行われます。
正しいです	正しいです	共有レベルの暗号化には関係なく SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、 SMB セッション全体で暗号化が行われます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
いいえ	正しいです	特定の共有で共有レベルの暗号化が有効です。この設定では、ツリー接続から暗号化が行われます。
いいえ	いいえ	暗号化は有効になっていません。

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

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

SMB 暗号化のパフォーマンスへの影響

SMB セッションで SMB 暗号化を使用すると、 Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（ SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

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

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、暗号化された SMB トラフィックのパフォーマンスが向上します。SMB 暗号化オフロードは、 SMB 暗号化が有効になっている場合にデフォルトで有効になります。

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

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

ネットワーク、 ONTAP 9 のバージョン、 SMB のバージョン、および SVM の実装方法に応じて SMB 暗号化のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

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

受信 SMB トラフィックの SMB 暗号化要求を有効または無効にします

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

このタスクについて

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

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップするときにに選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

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

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

手順

1. 次のいずれかを実行します。

CIFS サーバでの受信 **SMB** トラフィックの **SMB** 暗号化要求の設定	入力するコマンド
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. CIFSサーバでのSMB暗号化要求が必要に応じて有効または無効になっていることを確認します。 `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   。 `is-smb-encryption-required` フィールドが表示されます `true` CIFSサーバおよびでSMB暗号化要求が有効になっている場合 `false` 無効になっている場合。

例

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

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

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

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

接続中の SMB セッションに関する情報を表示して、クライアントが暗号化された SMB 接続を使用しているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

このタスクについて

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

- `unencrypted`

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

- `partially-encrypted`

  ツリー接続が行われると、暗号化が開始されます。共有レベルの暗号化が設定されています。SVM レベルの暗号化は有効になりません。

- `encrypted`

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

手順

1. 次のいずれかを実行します。

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

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 暗号化統計情報を監視する

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

このタスクについて

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

カウンタ名	説明
`encrypted_sessions`	暗号化された SMB 3.0 セッションの数

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
rejected_unencrypted_sessions	クライアントに暗号化機能がないために拒否されたセッションセットアップ数を示します
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

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

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

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

- rejected_unencrypted_sessions SMB暗号化をサポートしていないクライアントから暗号化を必要とするSMBセッションの確立が試行された回数を示します。
- rejected_unencrypted_shares SMB暗号化をサポートしていないクライアントから暗号化が必要なSMB共有への接続が試行された回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

手順

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

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

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

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

表示する情報	入力するコマンド
暗号化されたセッション	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	暗号化されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	暗号化された共有接続
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
暗号化された共有接続と接続された共有	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
暗号化されていないセッションは	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された暗号化されていない
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

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

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

例

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

次のコマンドは、 advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

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

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

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

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

2 entries were displayed
```

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

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

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

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

1 entry was displayed.
```

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

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

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

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

2 entries were displayed.
```

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

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

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

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

1 entry was displayed.
```

関連情報

使用可能な統計オブジェクトと統計カウンタの確認

"パフォーマンスの監視と管理の概要"

セキュアな LDAP セッション通信

LDAP の署名と封印の概念

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

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

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

CIFS サーバで LDAP の署名と封印を有効にする

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

作業を開始する前に

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

手順

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

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

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

> SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、で対応する設定を有効にする必要があります `-session-security` のオプション `vserver services name-service ldap client modify` コマンドを実行します

LDAP over TLS を設定する

自己署名ルート **CA** 証明書のコピーをエクスポートします

Active Directory 通信の保護に LDAP over SSL/TLS を使用するには、まず Active Directory 証明書サービスの自己署名ルート CA 証明書のコピーを証明書ファイルにエクスポートし、それを ASCII テキストファイルに変換する必要があります。ONTAP は、

このテキストファイルを使用して証明書を Storage Virtual Machine （ SVM ）にインストールします。

作業を開始する前に

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

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

ステップ

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

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

完了後

SVM に証明書をインストールします。

関連情報

"Microsoft TechNet ライブラリ"

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

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

このタスクについて

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

ONTAP 9.2 以降では、 TLS 通信を使用する ONTAP 内のすべてのアプリケーションで、 Online Certificate Status Protocol （ OCSP ）を使用してデジタル証明書のステータスを確認できます。OCSP が LDAP over TLS に対して有効になっている場合、失効した証明書は拒否され、接続は失敗します。

手順

1. 自己署名ルート CA 証明書をインストールします。

   a. 証明書のインストールを開始します。 `security certificate install -vserver vserver_name -type server-ca`

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

   b. 証明書を開きます `.pem` ファイルテキストエディタを使用して、で始まる行を含めて証明書をコピーします `-----BEGIN CERTIFICATE-----` で終わる `-----END CERTIFICATE-----`をクリックし、コマンドプロンプトのあとに証明書を貼り付けます。

   c. 証明書が正しく表示されることを確認します。

   d. Enter キーを押してインストールを完了します。

2. 証明書がインストールされていることを確認します。 `security certificate show -vserver vserver_name`

サーバで **LDAP over TLS** を有効にします

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

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

詳細については、以下を参照してください。

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

手順

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

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