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 9

NetApp
February 12, 2026

目次

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。
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`
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"

著作権に関する情報

商標に関する情報