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

ONTAP 9

NetApp
December 20, 2024

目次

SMBを介したデータ転送でのSMBサーバでのSMB暗号化要求の設定

SMBアンコウカノカイヨウ

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

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

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

SVMでのSMB暗号化は、次の2つの設定によって制御されます。

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

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

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

SMB サーバ **SMB** 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しい	正しくない	SVMのすべての共有でサーバレベルの暗号化が有効になっています。この設定では、SMBセッション全体で暗号化が行われます。
正しい	正しい	共有レベルの暗号化に関係なく、SVMのすべての共有でサーバレベルの暗号化が有効になります。この設定では、SMBセッション全体で暗号化が行われます。
正しくない	正しい	特定の共有で共有レベルの暗号化が有効になっている。この設定では、ツリー接続から暗号化が行われます。
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`
指定した SVM の特定のセッション ID の暗号化設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

例

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

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

SMB暗号化統計の監視

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

タスクの内容

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

カウンタ名	説明
`encrypted_sessions`	暗号化されたSMB 3.0セッションの数
`encrypted_share_connections`	ツリー接続が行われた暗号化された共有の数を示します。
`rejected_unencrypted_sessions`	クライアントの暗号化機能がないために拒否されたセッションセットアップの数
`rejected_unencrypted_shares`	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

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

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

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

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

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

手順

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

   パラメータを指定しない場合は `-sample-id`、サンプルIDが自動的に生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id`はテキスト文字列です。同じCLIセッションでパラメータを指定せずにこのコマンドを実行すると、 `-sample-id`以前のデフォルトサンプルが上書きされます。

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

3. サンプルのデータ収集を停止するには、コマンドを使用し `statistics stop`ます。
4. SMB暗号化統計を表示します。

表示する情報	入力するコマンド
暗号化されたセッション	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	暗号化されたセッションと確立されたセッション
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	暗号化された共有接続

表示する情報	入力するコマンド
`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"

著作権に関する情報

商標に関する情報