SMB署名を使用したネットワークセキュリティの強化

ONTAP 9

NetApp
December 20, 2024

目次

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"

著作権に関する情報

商標に関する情報