使用SMB簽署來強化網路安全性

ONTAP 9

NetApp
February 12, 2026

目錄

使用SMB簽署來強化網路安全性

瞭解如何使用 ONTAP SMB 簽署來增強網路安全性

SMB簽章有助於確保SMB伺服器與用戶端之間的網路流量不會受到影響、並可防止重播攻擊。根據預設ONTAP 、若用戶端要求、支援SMB簽署。或者、儲存管理員可以將SMB伺服器設定為需要SMB簽署。

瞭解簽署原則如何影響與 ONTAP SMB 伺服器的通訊

除了CIFS伺服器SMB簽署安全性設定之外、Windows用戶端上的兩個SMB簽署原則也會控制用戶端與CIFS伺服器之間的通訊數位簽署。您可以設定符合業務需求的設定。

用戶端SMB原則是透過Windows本機安全性原則設定來控制、這些設定是使用Microsoft管理主控台（MMC）或Active Directory GPO來設定。如需用戶端SMB簽署與安全性問題的詳細資訊、請參閱Microsoft Windows文件。

以下是Microsoft用戶端上兩種SMB簽署原則的說明：

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

  此設定可控制是否啟用用戶端的SMB簽署功能。預設為啟用。當用戶端停用此設定時、與CIFS伺服器的用戶端通訊取決於CIFS伺服器上的SMB簽署設定。

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

  此設定可控制用戶端是否需要SMB簽署才能與伺服器通訊。預設為停用。當用戶端上停用此設定時、 SMB簽署行為會根據的原則設定而定 `Microsoft network client: Digitally sign communications (if server agrees)` 以及 CIFS 伺服器上的設定。

> 如果您的環境包含設定為需要SMB簽署的Windows用戶端、則必須在CIFS伺服器上啟用SMB簽署。如果您沒有、CIFS伺服器就無法將資料提供給這些系統。

用戶端和CIFS伺服器SMB簽署設定的有效結果取決於SMB工作階段是使用SMB 1.0或SMB 2.x或更新版本。

下表摘要說明當工作階段使用SMB 1.0時的有效SMB簽署行為：

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
簽署已停用且不需要	未簽署	已簽署
簽署已啟用且不需要	未簽署	已簽署
簽署已停用且必要	已簽署	已簽署
簽署已啟用且必要	已簽署	已簽署

舊版Windows SMB 1用戶端和部分非Windows SMB 1用戶端若在用戶端上停用簽署、但CIFS伺服器上需要簽署、則可能無法連線。

下表摘要說明當工作階段使用SMB 2.x或SMB 3.0時的有效SMB簽署行為：

對於SMB 2.x和SMB 3.0用戶端、一律會啟用SMB簽署。無法停用。

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
不需要簽署	未簽署	已簽署
需要簽署	已簽署	已簽署

下表摘要說明預設的Microsoft用戶端和伺服器SMB簽署行為：

傳輸協定	雜湊演算法	可啟用/停用	可能需要/不需要	用戶端預設值	伺服器預設值	**DC**預設值
SMB 1.0	md5	是的	是的	已啟用（非必要）	已停用（非必要）	必要
SMB 2.x	HMAC SHA-256	否	是的	不需要	不需要	必要
SMB 3.0	AES-CMAC：	否	是的	不需要	不需要	必要

Microsoft 不再建議使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 群組原則設定。Microsoft 也不再建議使用 `EnableSecuritySignature` 登錄設定。這些選項只會影響 SMB 1 行為、可由取代 `Digitally sign communications (always)` 群組原則設定或 `RequireSecuritySignature` 登錄設定。您也可以從 Microsoft 部落格取得更多資訊。 The SMB 簽署基礎知識（涵蓋 SMB1 和 SMB2 ）

瞭解 ONTAP SMB 簽署對效能的影響

當SMB工作階段使用SMB簽署時、所有往返Windows用戶端的SMB通訊都會受到效能影響、這會影響用戶端和伺服器（亦即、叢集上執行SVM的節點包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 簽署的SMB流量中提供更好的效能。啟用SMB簽署時、預設會啟用SMB簽署卸載。

增強的SMB簽署效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB簽署的效能影響可能會有很大差異；您只能在網路環境中進行測試來驗證。

如果伺服器上已啟用SMB簽署、則大部分的Windows用戶端會依預設協調SMB簽署。如果您的部分Windows用戶端需要SMB保護、而且SMB簽章造成效能問題、您可以在任何不需要保護以防止重播攻擊的Windows用戶端上停用SMB簽署。如需在Windows用戶端上停用SMB簽署的相關資訊、請參閱Microsoft Windows文件。

ONTAP SMB 簽署組態建議

您可以設定SMB用戶端與CIFS伺服器之間的SMB簽署行為、以符合您的安全需求。您在CIFS伺服器上設定SMB簽署時所選擇的設定、取決於您的安全需求。

您可以在用戶端或CIFS伺服器上設定SMB簽署。設定SMB簽署時、請考慮下列建議：

如果...	建議...
您想要提高用戶端與伺服器之間通訊的安全性	啟用、讓用戶端需要 SMB 簽署 `Require Option (Sign always)` 用戶端上的安全性設定。
您希望所有SMB流量都簽署到特定的儲存虛擬機器（SVM）	設定安全性設定以要求SMB簽署、使CIFS伺服器上的SMB簽署成為必要項目。

如需設定Windows用戶端安全性設定的詳細資訊、請參閱Microsoft文件。

瞭解多重資料生命的 ONTAP SMB 簽署組態

如果您在SMB伺服器上啟用或停用必要的SMB簽署、您應該瞭解SVM多重資料生命量組態的準則。

設定SMB伺服器時、可能會設定多個資料生命量。如果是、則 DNS 伺服器包含多個 `A` 記錄 CIFS 伺服器的項目、所有項目都使用相同的 SMB 伺服器主機名稱、但每個項目都有唯一的 IP 位址。例如、已設定兩個資料生命期的 SMB 伺服器可能具有下列 DNS `A` 記錄項目：

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

正常情況是、變更必要的SMB簽署設定後、只有來自用戶端的新連線會受到SMB簽署設定的變更影響。不過、這種行為有例外。在某種情況下、用戶端與共用有現有的連線、而用戶端會在變更設定之後、建立新的連線至同一個共用區、同時維持原始連線。在這種情況下、新的和現有的SMB連線都會採用新的SMB簽署要求。

請考慮下列範例：

1. Client1 連接到共享區、而不需要使用路徑簽署 SMB `O:\`。
2. 儲存管理員會修改SMB伺服器組態、以要求SMB簽署。
3. Client1 會使用路徑連線到具有必要 SMB 簽署的同一個共用區 `S:\` （同時使用路徑維持連線 `O:\`）。

4. 結果是在存取兩者的資料時、會使用 SMB 簽署 `O:\` 和 `S:\` 磁碟機。

為傳入的 SMB 流量設定 ONTAP 簽署

您可以啟用必要的SMB簽署、強制要求用戶端簽署SMB訊息。如果啟用ONTAP 、僅當SMB訊息具有有效的簽名時、才會接受該訊息。如果您想要允許SMB簽署、但不需要SMB簽署、可以停用必要的SMB簽署。

關於這項工作

預設會停用必要的SMB簽署。您可以隨時啟用或停用所需的SMB簽署。

> 在下列情況下、預設不會停用SMB簽署：
>
> 1. 啟用必要的SMB簽署、叢集將還原為ONTAP 不支援SMB簽署的版本。
> 2. 叢集隨後會升級至ONTAP 支援SMB簽署的版本的支援。
>
>   在這種情況下、原本設定在支援版本ONTAP 的支援版本上的SMB簽署組態會透過還原及後續升級來保留。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 簽署安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 簽署安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用必要的SMB簽署、則必須在目的地SVM上手動啟用必要的SMB簽署。

步驟

1. 執行下列其中一項動作：

如果您想要**SMB**簽署...	輸入命令...
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 判斷中的值是否已啟用或停用必要的 SMB 簽署 `Is Signing Required` 下列命令輸出中的欄位設定為所需的值： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

範例

下列範例可為SVM VS1啟用必要的SMB簽署：

```
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
```

對加密設定的變更會對新連線生效。現有連線不受影響。

相關資訊

- "SnapMirror建立"

判斷 ONTAP SMB 工作階段是否已簽署

您可以在CIFS伺服器上顯示連線SMB工作階段的相關資訊。您可以使用此資訊來判斷SMB工作階段是否已簽署。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
指定儲存虛擬機器（SVM）上的所有簽署工作階段	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
在SVM上具有特定工作階段ID的已簽署工作階段詳細資料	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

範例

下列命令會顯示SVM VS1上已簽署工作階段的相關工作階段資訊。預設的摘要輸出不會顯示「Is Session Signed」（已簽署的工作階段）輸出欄位：

```
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
```

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括工作階段是否已簽署：

```
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
```

相關資訊

監控SMB簽署的工作階段統計資料

監控 ONTAP SMB 簽署的工作階段統計資料

您可以監控SMB工作階段統計資料、並判斷哪些已建立的工作階段已簽署、哪些尚未簽署。

關於這項工作

。 `statistics` 進階權限層級的命令提供 `signed_sessions` 可用來監控已簽署 SMB 工作階段數量的計數器。。 `signed_sessions` 下列統計資料物件可使用計數器：

- `cifs` 可讓您監控所有 SMB 工作階段的 SMB 簽署。
- `smb1` 可讓您監控 SMB 1.0 工作階段的 SMB 簽署。
- `smb2` 可讓您監控 SMB 2.x 和 SMB 3.0 工作階段的 SMB 簽署。

  的輸出中包含 SMB 3.0 統計資料 `smb2` 物件：

如果您想要比較已簽署工作階段的數目與工作階段總數、您可以比較的輸出 `signed_sessions` 以的輸出進行計數 `established_sessions` 計數器。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

   如"指令參考資料ONTAP"需詳細 `statistics start`資訊，請參閱。
3. 使用 `statistics stop` 停止收集樣本資料的命令。

   詳細了解 `statistics stop`在"指令參考資料ONTAP" 。
4. 檢視SMB簽署統計資料：

如果您要檢視下列項目的資訊...	輸入...
已簽署的工作階段	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	已簽署的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

   如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。
5. 返回管理權限層級：
   `set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 2.x和SMB 3.0簽署統計資料。

下列命令會移至進階權限層級：

```
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
```

下列命令會啟動新範例的資料收集：

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

下列命令會停止範例的資料收集：

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

下列命令會顯示已簽署的SMB工作階段、以及範例中各節點所建立的SMB工作階段：

```
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
```

以下命令顯示節點2的簽署SMB工作階段：

```
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
```

下列命令會移回管理權限層級：

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

相關資訊

- 判斷SMB工作階段是否已簽署
- "效能監控與管理總覽"

版權資訊

商標資訊