在SMB伺服器上設定必要的SMB加密、以便透過SMB傳輸資料

ONTAP 9

NetApp
June 19, 2024

目錄

在SMB伺服器上設定必要的SMB加密、以便透過SMB傳輸資料

SMB加密總覽

SMB加密可在SMB伺服器上啟用或停用SMB資料傳輸功能、是一項安全性增強功能。您也可以透過共用內容設定、逐一設定所需的SMB加密設定。

根據預設、當您在儲存虛擬機器（ SVM ）上建立 SMB 伺服器時、 SMB 加密會停用。您必須讓IT能夠充分利用SMB加密所提供的增強安全性。

若要建立加密的SMB工作階段、SMB用戶端必須支援SMB加密。從Windows Server 2012和Windows 8開始的Windows用戶端支援SMB加密。

SVM上的SMB加密可透過兩種設定加以控制：

- SMB 伺服器安全選項、可在 SVM 上啟用功能
- SMB 共用屬性，可依每個共用區設定 SMB 加密設定

您可以決定是否需要加密才能存取SVM上的所有資料、或是需要SMB加密才能存取所選共用區中的資料。SVM層級的設定會取代共用層級的設定。

有效的SMB加密組態取決於兩項設定的組合、如下表所述：

啟用**SMB**伺服器**SMB**加密	共用加密資料設定已啟用	伺服器端加密行為
是的	錯	SVM中的所有共用都啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
是的	是的	無論共用層級加密為何、SVM中的所有共用都會啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
錯	是的	特定共用區已啟用共用層級加密。使用此組態、即可從樹狀結構連線進行加密。
錯	錯	未啟用加密。

不支援加密的 SMB 用戶端無法連線至需要加密的 SMB 伺服器或共用區。

對加密設定的變更會對新連線生效。現有連線不受影響。

SMB加密對效能的影響

當SMB工作階段使用SMB加密時、所有往返Windows用戶端的SMB通訊都會受到效能影響、影響用戶端和伺服器（亦即叢集上執行SVM的節點、其中包含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 加密的SMB流量中提供更好的效能。啟用SMB加密時、預設會啟用SMB加密卸載。

增強的SMB加密效能需要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加密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。

SMB加密在SMB伺服器上預設為停用。您只能在需要加密的SMB共用區或SMB伺服器上啟用SMB加密。藉由SMB加密、ONTAP 支援進一步處理解密要求、並加密每個要求的回應。因此、只有在必要時才應啟用SMB加密。

啟用或停用傳入SMB流量所需的SMB加密

如果您想為傳入的SMB流量要求SMB加密、可以在CIFS伺服器或共用層級啟用SMB加密。根據預設、不需要SMB加密。

關於這項工作

您可以在CIFS伺服器上啟用SMB加密、此功能適用於CIFS伺服器上的所有共用。如果您不希望CIFS伺服器上的所有共用都需要SMB加密、或是想要針對每個共用區的傳入SMB流量啟用必要的SMB加密、可以停用CIFS伺服器上所需的SMB加密。

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 加密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 加密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SMB加密、則必須在目的地上手動啟用CIFS伺服器SMB加密。

步驟

1. 執行下列其中一項動作：

如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能...	輸入命令...
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. 確認 CIFS 伺服器上所需的 SMB 加密已視需要啟用或停用： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 欄位隨即顯示 `true` 如果需要、會在 CIFS 伺服器和上啟用 SMB 加密 `false` 如果已停用。

範例

下列範例為SVM VS1上的CIFS伺服器啟用必要的SMB加密功能：

```
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
```

判斷用戶端是否使用加密的**SMB**工作階段連線

您可以顯示連線SMB工作階段的相關資訊、以判斷用戶端是否使用加密的SMB連線。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。

關於這項工作

SMB用戶端工作階段可以有三種加密層級之一：

- `unencrypted`

  SMB工作階段未加密。未設定儲存虛擬機器（SVM）層級或共用層級的加密。

- `partially-encrypted`

  當樹狀結構連線發生時、會啟動加密。已設定共用層級加密。未啟用SVM層級的加密。

- `encrypted`

SMB工作階段已完全加密。已啟用SVM層級的加密。共用層級加密可能已啟用、也可能未啟用。SVM層級的加密設定會取代共用層級的加密設定。

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...
針對指定SVM上的工作階段、具有指定加密設定的工作階段	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定SVM上特定工作階段ID的加密設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

範例

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、包括加密設定：

```
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
```

監控SMB加密統計資料

您可以監控SMB加密統計資料、並判斷哪些已建立的工作階段和共用連線已加密、哪些尚

未加密。

關於這項工作

。 `statistics` 進階權限層級的命令會提供下列計數器、您可以使用這些計數器來監控加密的 SMB 工作階段數目及共用連線：

計數器名稱	說明
`encrypted_sessions`	提供加密的SMB 3.0工作階段數量
`encrypted_share_connections`	提供樹狀結構連線所在的加密共用數
`rejected_unencrypted_sessions`	提供因缺乏用戶端加密功能而遭拒的工作階段設定數
`rejected_unencrypted_shares`	提供因缺乏用戶端加密功能而遭拒的共用對應數目

這些計數器可與下列統計資料物件一起使用：

- `cifs` 可讓您監控所有 SMB 3.0 工作階段的 SMB 加密。

  的輸出中包含 SMB 3.0 統計資料 `cifs` 物件： 如果您想要比較加密工作階段的數目與工作階段總數、可以比較的輸出 `encrypted_sessions` 以的輸出進行計數 `established_sessions` 計數器。

  如果您要比較加密共用連線的數目與共用連線的總數、可以比較的輸出 `encrypted_share_connections` 以的輸出進行計數 `connected_shares` 計數器。

- `rejected_unencrypted_sessions` 提供嘗試建立 SMB 工作階段的次數、該工作階段需要從不支援 SMB 加密的用戶端進行加密。
- `rejected_unencrypted_shares` 提供嘗試連線至 SMB 共用的次數、該共用需要來自不支援 SMB 加密的用戶端進行加密。

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。

3. 使用 `statistics stop` 停止收集樣本資料的命令。

4. 檢視SMB加密統計資料：

如果您要檢視下列項目的資訊...	輸入...
加密工作階段	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	加密的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共用連線
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共用連線和連線共用	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒絕未加密的工作階段	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒絕未加密的共用連線
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

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 3.0加密統計資料。

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 cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

下列命令會停止該範例的資料收集：

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

下列命令顯示節點從範例中所建立的加密SMB工作階段和已建立的SMB工作階段：

```
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
```

下列命令顯示節點從範例中拒絕的未加密SMB工作階段數目：

```
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.
```

下列命令顯示範例中節點所連線的SMB共用數和加密的SMB共用數：

```
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.
```

下列命令顯示節點從範例中拒絕的未加密SMB共用連線數目：

```
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.
```

相關資訊

判斷可用的統計資料物件和計數器

"效能監控與管理總覽"