對Catalyst交換機上與Azure雲伺服器的安全外殼連線進行故障排除

目錄

簡介

本文檔介紹當思科交換機無法使用Secure Shell連線到Microsoft Blob儲存時，如何識別和解決問題。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解思科交換器上的安全檔案傳輸通訊協定(SFTP)操作和設定
- 熟悉安全殼層(SSH)通訊協定及其交涉階段
- 瞭解用於SFTP訪問的Microsoft Blob儲存服務配置
- 閱讀和解釋交換機系統日誌/調試消息的經驗
- 針對思科交換機和外部SFTP服務之間的網路連線和協定相容性的基本故障排除

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 產品系列：Catalyst 9300 系列交換器
- 軟體版本:Cisco IOS® XE 17.9.5
- 技術：LAN 交換
- 到Azure雲平台的SSH連線

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Microsoft Blob儲存現在提供SFTP訪問，支援從思科交換機等網路裝置傳輸檔案。將裝置配置備份到非現場雲端儲存（如Microsoft Blob）是災難恢復和操作連續性的常見做法。SFTP利用SSH協定實現安全檔案傳輸。它需要成功的SSH協商、金鑰交換以及開啟安全資料通道的能力。本地SFTP伺服器可以採用標準或受良好支援的協定實施，而基於雲的服務（如Microsoft Blob SFTP）可能會引入可能影響成功檔案傳輸的相容性或協定協商差異。要解決此類互操作性問題，需要對系統日誌/調試輸出進行仔細分析，並採用系統方法隔離協定、配置或環境原因。

問題

當嘗試將配置從思科交換機備份到Microsoft Blob儲存SFTP端點時，備份在SSH協商完成之後失敗。到本地SFTP伺服器的備份成功而沒有出現問題，這表明交換機SFTP客戶端在其他情況下可以正常工作。

症狀：

- 交換機使用Microsoft Blob SFTP成功完成SSH金鑰交換和身份驗證。
- 備份在通道開啟階段失敗，導致檔案傳輸無法進行。
- Syslog/debug消息指示SFTP寫入操作期間失敗。

在故障期間記錄的相關調試/系統日誌輸出：

<#root>

```
Feb 12 14:05:03.272: ssh2_calculate_modulus_length: modulus len 32
Feb 12 14:05:03.280:  SSH: Signature verification successful
Feb 12 14:05:03.280: SSH2: kex_derive_keys complete
Feb 12 14:05:03.281: SSH2 CLIENT 0: SSH2_MSG_NEWKEYS sent
```

```
Feb 12 14:05:03.281: SSH2 CLIENT 0: waiting for SSH2_MSG_NEWKEYS
Feb 12 14:05:03.288: SSH2 CLIENT 0: SSH2_MSG_NEWKEYS received
Feb 12 14:05:03.330: SSH2 CLIENT 0:

Channel open failed, reason = 1

Feb 12 14:05:03.331: SSH CLIENT0: Session disconnected - error 0x00
Feb 12 14:05:03.332:

SFTP write_process: sftp_write failed err 1545

Feb 12 14:05:03.332: SFTP ifs_write: ndent stat (2) 3
```

日誌中的主要觀察結果：

- SSH金鑰交換和簽名驗證成功。
- 故障發生在SSH通道開啟階段：通道開啟失敗，原因= 1。
- SFTP寫入過程失敗（錯誤1545），會話在之後立即斷開。

解決方案

通過增加Catalyst 9300交換機上的SSH視窗大小配置以滿足Azure雲伺服器要求來解決此問題。Azure雲伺服器要求的SSH視窗大小大於在17.10.1 Cisco IOS XE版本之前的思科交換機上配置的預設值。

步驟1.配置SSH視窗大小

將SSH視窗大小配置為至少為16384的值。建議的最大值是65536，以避免對低端裝置產生過多的CPU影響：

```
<#root>

device(config)#

ip ssh window-size 65536
```

執行此命令後，您將收到以下警告消息：

```
%% Warning: This cli may have impact on CPU. So, use only for SCP
Please configure ip tcp window-size<> with same value, for this CLI to work
```

步驟2.配置TCP視窗大小

配置TCP視窗大小以匹配SSH視窗大小值：

<#root>

```
device(config)#

ip tcp window-size 65536
```

組態驗證

實施兩次配置更改後，交換機和Azure雲伺服器之間的SSH連線正常工作，允許成功進行SFTP備份操作。

附註：從Cisco IOS XE Dublin 17.10.1開始，預設啟用SSH批次資料傳輸模式，預設視窗大小為128 KB。雖然支援的最大SSH視窗大小值是131072，但建議使用最大值65536來最大程度降低對低端裝置的CPU影響。

注意：Azure雲伺服器所需的最小視窗大小為16384。SSH和TCP視窗大小必須配置為匹配值，解決方案才能有效工作。

原因

此問題的根本原因是在Cisco Catalyst 9300交換機上配置的預設SSH視窗大小與Microsoft Azure雲伺服器的最小SSH視窗大小要求之間不匹配。預設情況下，思科交換機使用SSH視窗大小值8912，該值對於要求最小視窗大小至少為16384的Azure雲伺服器來說是不夠的。這種不相容將阻止建立SFTP檔案傳輸所需的SSH通道，即使初始SSH身份驗證和金鑰交換過程已成功完成。

相關資訊

- 思科支援助理
- 思科全球聯絡
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。