將部署失敗從FMC升級為FTD後，疑難排解Sftunnel通訊問題

目錄

問題

將部署推送到多個防火牆威脅防禦(FTD)裝置的嘗試失敗，部署失敗發生率介於8%和20%之間。FMC日誌未提供導致這些失敗的明確原因。

環境

- 思科安全防火牆Firepower(FMC)
- FMC和FTD通過MPLS路徑進行通訊
- FMC和FTD之間的sftunnel/management流量不進行防火牆檢查
- FMC和FTD之間用於安全通道通訊的足夠頻寬
- 已注意到部署失敗

解析

此工作流提供全面和詳細的過程，用於識別和解決從FMC到與sftunnel進程通訊問題相關的FTD裝置的部署故障。每個步驟都詳細介紹，包括示例命令輸出以示說明。

以超級超級使用者身份訪問FTD CLI

若要執行進階診斷和程式操作，請登入FTD裝置CLI並將許可權提升到root。

```
> expert
device$ sudo su
Password:
root@device:/Volume/home/admin#
```

檢查FTD sftunnel狀態

運行`sftunnel_status.pl`指令碼以檢查sftunnel進程的運行狀況和通訊狀態。

```
root@device:/Volume/home/admin# sftunnel_status.pl
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERIPADDRESS
```

```
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERUUID
```

指示RPC狀態故障的輸出示例：

```
peer UUID did not reply at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 309.
Retry rpc status poll at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 315.
**RPC STATUS****PEERIP*************
RPC status :Failed
**RPC STATUS****PEERIP*************
RPC status :Failed
```

確保最近沒有對FMC或FTD管理進行IP地址或網路更改，因為這將需要手動更改FMC System/Configuration/Management Interfaces頁面或FTD CLISH上的IP地址，具體取決於需要更改的裝置。

FTD CLISH上的管理IP位址變更範例：

```
> configure network ipv4 manual IPADDRESS NETMASK GATEWAYIP
> show network
```

確定sftunnel進程的當前進程ID(PID)

要監視和驗證sftunnel進程，請使用pmtool檢索其PID。

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

輸出示例：

```
sftunnel      Running     PID: 12345
```

重新啟動sftunnel進程並驗證PID更改

重新啟動sftunnel進程以重置其通訊狀態。重新啟動後，重新運行PID檢查以確認新進程處於活動狀態。

```
root@device:/Volume/home/admin# pmtool restartbyid sftunnel
```

經過一段短暫的時間後，再次檢查進程狀態：

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

示例輸出（PID必須與前面不同）：

```
sftunnel      Running     PID: 67890
```

等待2分鐘，讓安全通道程式穩定並嘗試從FMC到受影響的FTD進行新部署

請等待大約兩分鐘，以便sftunnel進程完全重新初始化並重新建立通訊。然後，啟動從FMC到FTD的新部署。

示例部署指令碼：

```
===============TRANSACTION INFO===============
Device UUID: PEERUUID
Transaction ID: 4075925334520
Selected policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrusion
Out-of-date policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrus
Deployment Type: Full Deployment
================================================================
```

如果成功，則部署完成，且不會出現錯誤，並且會在FTD上更新策略。

重新啟動後驗證sftunnel和RPC通訊

成功部署後，再次使用`sftunnel_status.pl`確認sftunnel進程和RPC狀態是否正常。

```
root@device:/Volume/home/admin# sftunnel_status.pl
```

指示成功的輸出示例：

```
**RPC STATUS****PEERIP*************
  'ipv4_1' => 'PEERIP',
  'uuid' => 'PEERUUID',
  'ipv6' => 'IPv6 is not configured for management',
```

```
  'active' => 1,
  'ip' => 'PEERIP',
  'last_changed' => 'Thu Nov 13 23:22:43 2025',
  'name' => 'PEERNAME',
  'uuid_gw' => ''
```

對所有受影響的FTD重複sftunnel重新啟動程式

如果多個FTD受到影響，請針對每個受影響的裝置執行上述步驟以恢復部署功能。

頻寬和連線驗證

運行bandwidth_analyzer.pl —size SIZEINMB -p PEERIP，確保FMC和FTD之間具有足夠的頻寬和基本網路連線。思科文檔建議至少使用5 Mbps的吞吐量建立穩定的管理連線。

頻寬分析輸出示例：

```
======== Bandwidth Analysis Result  ========
$VAR1 = {
          'PEERIP' => [
                                {
                                  'download' => '3.81 Mbps'
                                },
                                {
                                  'upload' => '4.24 Mbps'
                                },
                                {
                                  'rpcStatus' => 'Up'
                                }
                              ]
        };
```

原因

部署失敗的根本原因可能是由於：

- 特定FTD或FMC裝置上的sftunnel程式故障。
- 管理TLS流量的干擾（例如來自中間防火牆檢查的干擾），導致對RPC狀態檢查的錯誤響應。
- 網路更改（例如IP地址更改、遷移或裝置新增）會導致裝置之間無法連線。

在受影響的FTD/FMC上重新啟動sftunnel程式可以還原正確的通訊並允許從FMC成功部署策略。

否則，請通過驗證IP地址和清除網路路徑來確保裝置之間的正確連線。

相關內容

- 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）。