排除Talos連線狀態故障

目錄

簡介

本文檔介紹如何解決安全防火牆FMC和FDM上的TALOS連線問題。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆裝置管理員(FDM)

- 思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

FMC 7.6.0或7.7.0版
FDM 7.6.0或7.7.0版
FTD 7.6.0或7.7.0版

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

思科安全防火牆管理中心(FMC)依靠客戶端證書與Cisco Talos威脅情報服務建立安全連線。此驗證對於FMC成功下載關鍵更新(包括URL信譽資料庫(URLDB)、輕量級安全包(LSP)和其他增強資料)至關重要。

在正常操作條件下，此證書在軟體安裝過程中預配置，並設計為在其即將到期時自動續訂。但是，某些版本的Cisco安全防火牆FMC軟體存在已知問題，導致自動續訂流程無法在2025年3月30日之後成功完成。發生這種情況時，FMC無法使用Talos進行身份驗證，從而導致連線失敗和無法檢索更新的威脅情報。

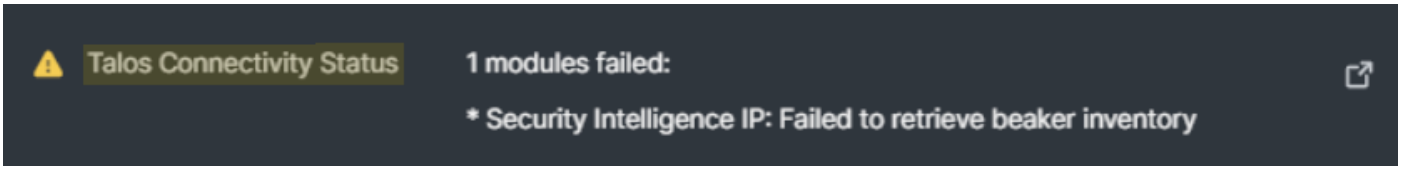
驗證證書狀態

FMC GUI

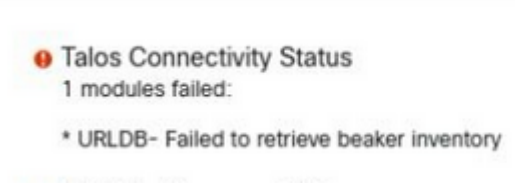
當客戶端證書無法續訂時，Cisco FMC會觸發健康警報，通知管理員與Cisco Talos的通訊中斷。您可以通過導航到System > Health並檢視Talos Connectivity Status部分來監控這些警報。

如果您的系統受到證書過期問題的影響，您通常會看到以下錯誤消息之一：

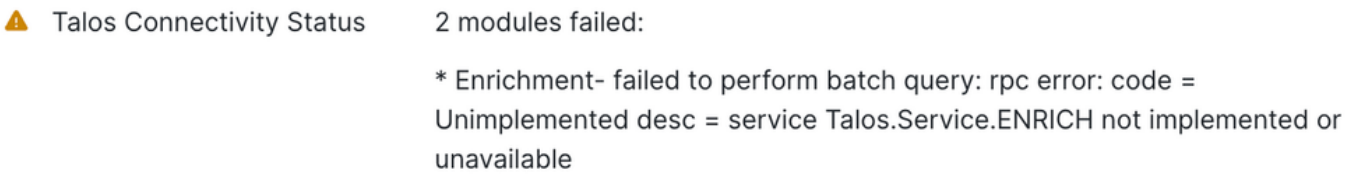
- "LSP — 無法檢索燒杯庫存":



- "URLDB — 無法檢索燒杯庫存":



- "富集 — 無法執行批處理查詢":



FMC CLI

要確定您的FMC裝置是否受到此問題的影響，請訪問expert mode並運行命令以驗證客戶端證書的當前到期日期：

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'

sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
```

在命令輸出中，找到有效性部分。Not　After欄位表示證書的當前到期日期。如果此日期已過或即將到，續訂流程失敗，需要手動重新啟動服務以啟動證書續訂。

範例：

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

```
Validity

Not Before: Jan 30 22:32:39 2024 GMT

Not After :

 Mar 30 22:32:39 2025 GMT
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

疑難排解

1.確定您的方案

軟體版本	關聯的錯誤ID	主要原因
7.6.0或7.7.0	思科錯誤ID CSCwo63951	證書過期/連線故障
7.6.1+或7.7.10+	思科錯誤ID CSCwr23982	註冊/許可配置（例如，氣隙）。

2. 7.6.0和7.7.0版故障排除

症狀

除了前面提到的運行狀況警報，您還會觀察到以下行為：

- FDM工作管理員錯誤："Snort 3雲更新失敗：沒有來自更新伺服器的響應或連線超時。"
- 日誌條目：/ngfw/var/log/messages中的錯誤指示：無法連線到隧道(UUID)，錯誤：未連線。
- 狀態:UI中的停滯更新：URL過濾首選項螢幕顯示「尚未更新」。

臨時解決方法

要立即恢復服務，請通過專家模式重新啟動所需的進程：

步驟1.訪問CLI並進入專家模式。

步驟2.運行以下命令：

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

附註：此解決方法將觸發一個有效期只有五天的證書。您必須每五天重複一次此過程，直到應用永久修補程式。

永久決議

要永久解決此問題，請確保滿足以下條件：

步驟1.檢驗連通性：確保裝置具有對https://api-sse.cisco.com的出站訪問許可權。為此，請訪問FMC CLI，進入專家模式，然後運行以下命令：

步驟1.1.測試DNS解析：

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

nslookup api-sse.cisco.com

步驟1.2.測試TCP埠訪問：

<#root>

```
 expert
sudo su
//type the 'FMC CLI admin password'
```

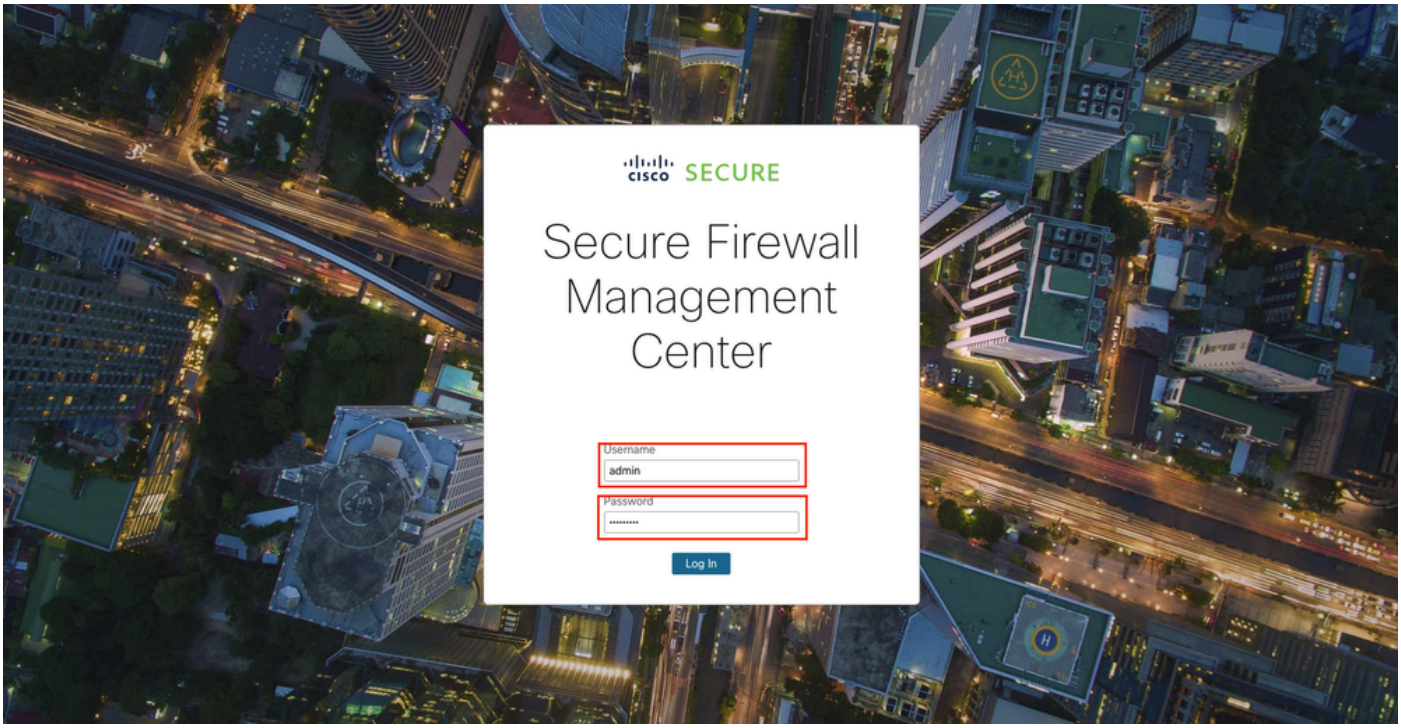
telnet api-sse.cisco.com 443

附註：驗證是否允許通過所有上游防火牆、代理或安全裝置對https://api-sse.cisco.com的出站HTTPS(TCP 443)訪問。

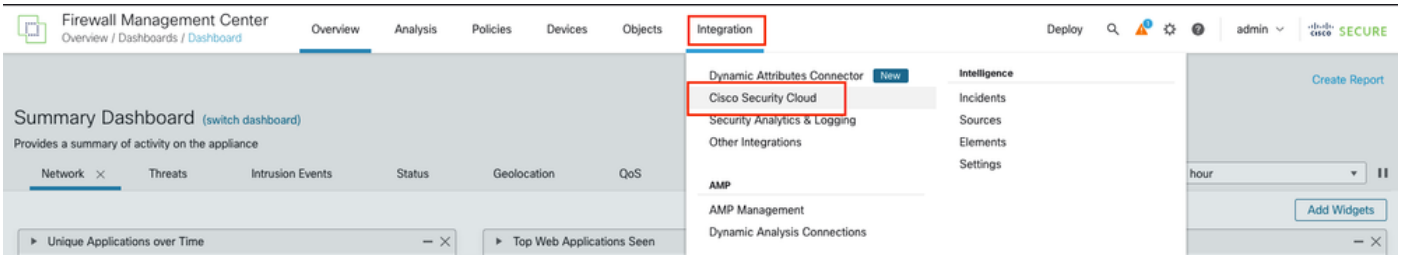
步驟2.啟用遙測：確保啟用客戶成功網路(CSN)遙測功能，以便SSEConnector可以獲取新證書。要在FMC上啟用CSN，請執行以下步驟：

步驟2.1.開啟Web瀏覽器並導覽至FMC URL，即可登入FMC GUI(例如：https://<FMC_IP_or_Hostname>)。 輸入您的使用者名稱和密碼以訪問

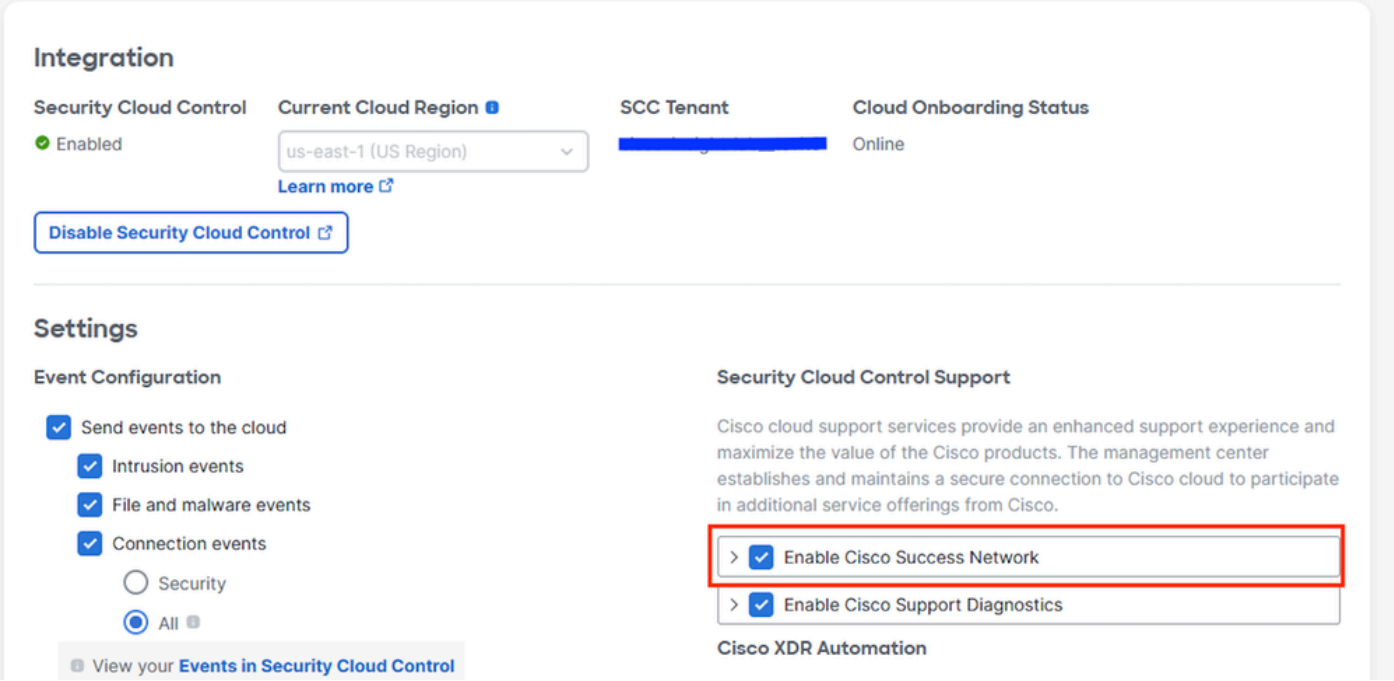
FMC GUI介面。



步驟2.2.導覽至Cisco Success Network Settings:從主選單中選擇Integration> Cisco Security Cloud。



步驟2.3.查詢並啟用標籤為Cisco Success Network的選項：為此，請選中Enable Cisco Success Network覈取方塊，以啟用遙測。



步驟3.安裝更新：安裝GeoDB 2025-04-03-094或VDB 406（或更高版本）。 這將觸發安裝新的365天證書。

附註：高可用性(HA)。 在HA對中，SSEConnector進程不在備用裝置上運行。要更新備用FMC，請執行角色切換以使備用變為活動狀態，然後安裝所需的VDB或GeoDB更新。

---

3. 7.6.1+和7.7.10+版故障排除

此問題通常發生於沒有標準思科安全雲(CSC)註冊的環境中，例如使用評估許可證、SSM內部部署、PLR或SLR的環境。

受影響的功能

- 自動/手動輕型安全包(LSP)更新。
- URL過濾資料庫內容更新和雲查詢。
- Talos豐富連線事件。

建議的操作

1.標準環境：通過整合>思科安全雲註冊FMC。註冊會在30分鐘內自動觸發新證書下載。

2.手動更新：如果自動更新失敗，請從software.cisco.com手動下載最新的LSP並將其直接安裝在FMC上。

3.氣隙環境：如果您的網路無法訪問Internet，則Talos連線狀態運行狀況模組將變得不相關。在這種情況下，請在應用的運行狀況策略中禁用此特定模組。

相關資訊

- 如需其他協助，請聯絡思科技術協助中心(TAC)。需要有效的支援合約：Cisco全球支援聯絡人。
- 思科支援與下載: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）。