在安全網路分析中排除NetFlow/IPFIX遙測接收故障

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [疑難排解指南](#)
- [採用元件](#)

[背景資訊](#)

- [必填欄位](#)

[疑難排解程式](#)

- [驗證NetFlow/IPFIX遙測接收](#)
- [驗證NetFlow/IPFIX模板](#)
- [新增缺少的欄位後驗證NetFlow/IPFIX遙測輸入](#)
- [驗證NetFlow/IPFIX遙測接收埠](#)
- [驗證NetFlow/IPFIX遙測接收NetFlow選項是否已啟用](#)

[相關資訊](#)

簡介

本文說明如何對安全網路分析(SNA)中的Netflow遙測接收進行疑難排解。

必要條件

- Cisco SNA知識
- NetFlow/IPFIX知識

需求

- 7.5.0或更高版本中的安全網路分析
- 7.5.0或更高版本中的流量收集器
- 以系統管理員身份對流量收集器的CLI訪問
- 管理員UI訪問許可權，以管理員身份訪問流量收集器

疑難排解指南

- [為安全網路分析上的遙測接收配置NetFlow/IPFIX](#)

採用元件

- 7.5.0上的SNA管理員和流量收集器

- Wireshark軟體

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。

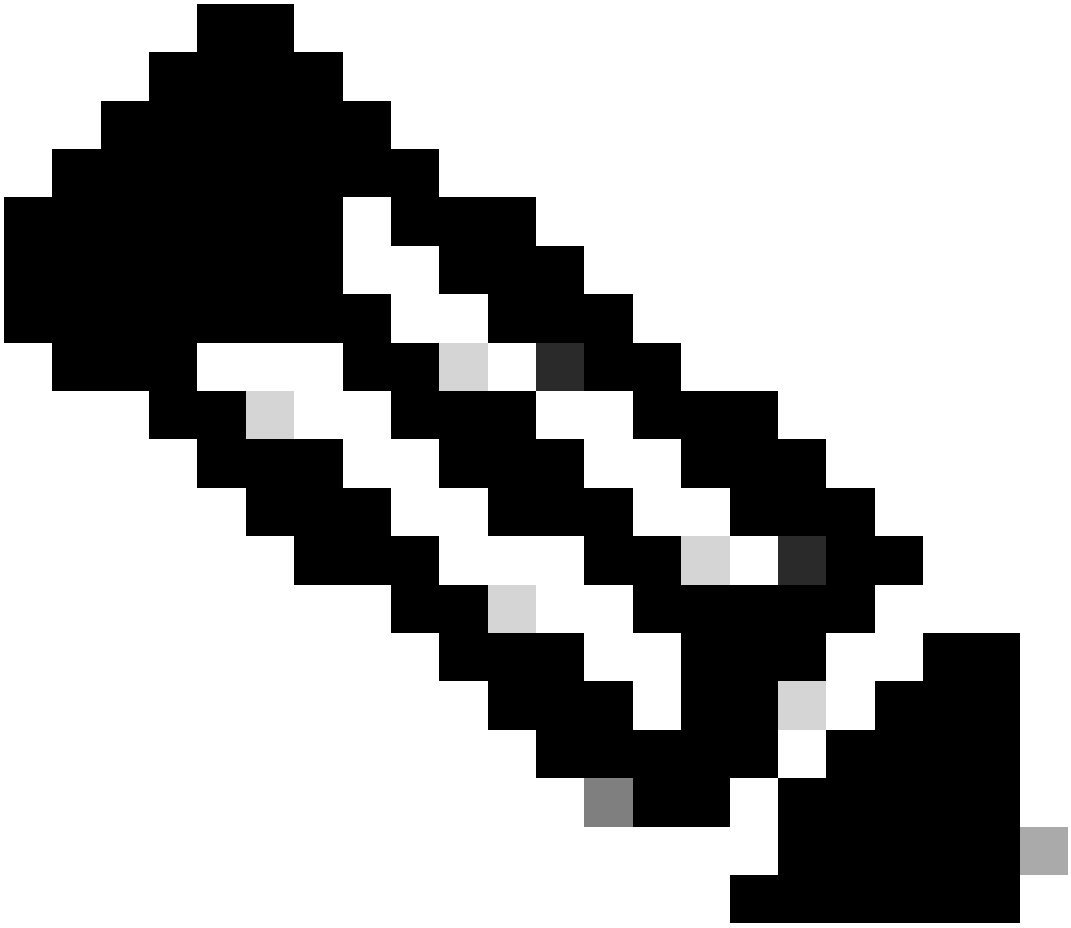
背景資訊

流量收集器是一種SNA裝置，負責收集、處理和儲存傳送到安全網路分析的流量。對於NetFlow版本9或IPFIX，可以在NetFlow/IPFIX模板上包含多個欄位，以新增與網路流量相關的詳細資訊，但是，對於流量收集器處理這些流量，必須在NetFlow/IPFIX模板中包含9個特定欄位。流量收集器不會處理包含無效模板的傳入流，因此SNA不會在Web UI或案頭客戶端下顯示這些匯出器的流資訊。

必填欄位

下一個欄位必須包含在NetFlow/IPFIX模板上，用於遙測接收。確保這9個欄位包含在NetFlow/IPFIX模板中，以便Secure Network Analytics處理傳入流量。

- 來源IP位址
- 目標IP地址
- 來源連線埠
- 目的地連線埠
- 第3層通訊協定
- 位元組數
- 資料包計數
- 流開始時間
- 流結束時間



附註：NetFlow/IPFIX配置中可能包含更多欄位，但之前的欄位是遙測接收的安全網路分析的最低要求。

疑難排解程式

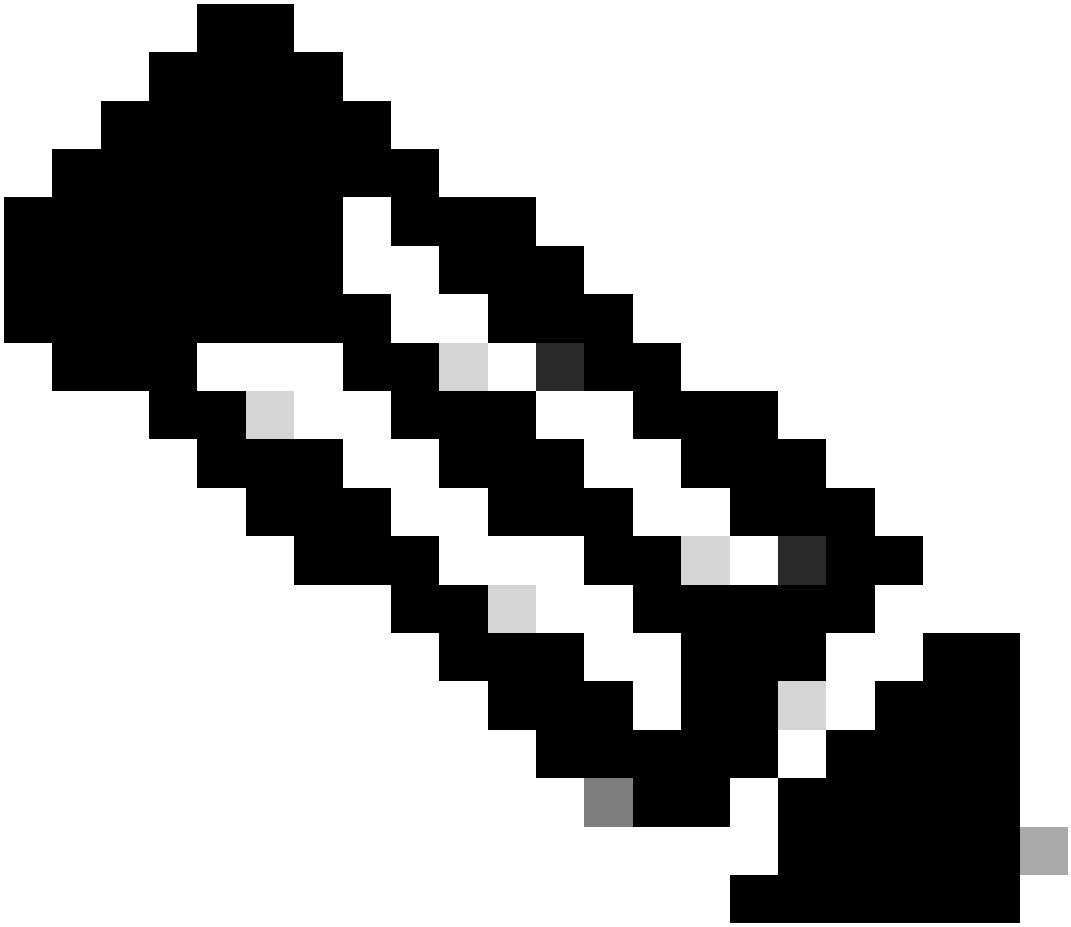
驗證NetFlow/IPFIX遙測接收

要確認SNA流量收集器是否從匯出器接收和插入NetFlow/IPFIX遙測，請執行以下操作：

1. 使用管理員憑據登入到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左側面板上，導航到支援 > 瀏覽檔案
3. 導航到下一個資料夾：sw > today > logs
4. 按一下sw.log檔案將其下載到本地電腦，然後在文本編輯器中將其開啟。
5. 在日誌底部搜尋這些行，每五分鐘建立一次此摘要：

```
18:45:00 I-sch-t: process_5_min_period: begin
```

```
18:45:00 I-sch-t: process_5_min_period: periods(177)
18:45:00 S-per-t: Performance Period 177
18:45:00 S-per-t:     Engine status Status normal
18:45:00 S-per-t:     Processed 6948 flows at 24 fps this period
18:45:00 S-per-t:     Processed 4226 biflows at 15 fps this period
18:45:00 S-per-t:     Dropped 0 flows this period
18:45:00 S-per-t:     Discarded 4358 flows this period due to insufficient template data
18:45:00 S-per-t:     Processed 1838743 flows at 35 fps today
18:45:00 S-per-t:     Dropped 0 flows today
18:45:00 S-per-t:     Discarded 11069 flows today due to insufficient template data
18:45:00 S-per-t:     Process instance 0 processed 3372 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 0 processed 2066 biflows at 7 fps this period
18:45:00 S-per-t:     Process instance 1 processed 3576 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 1 processed 2160 biflows at 8 fps this period
18:45:00 S-per-t:     Inserted 2048 flow stats at 7 fps this period
18:45:00 S-per-t:     Inserted 2013 interface stats at 7 fps this period
18:45:00 S-per-t:     Inserted 470932 flow stats at 9 fps today
18:45:00 S-per-t:     Inserted 678994 interface stats at 13 fps today
```



附註：第8行表示由於上一時段的模板資料不足而丟棄了資料流。

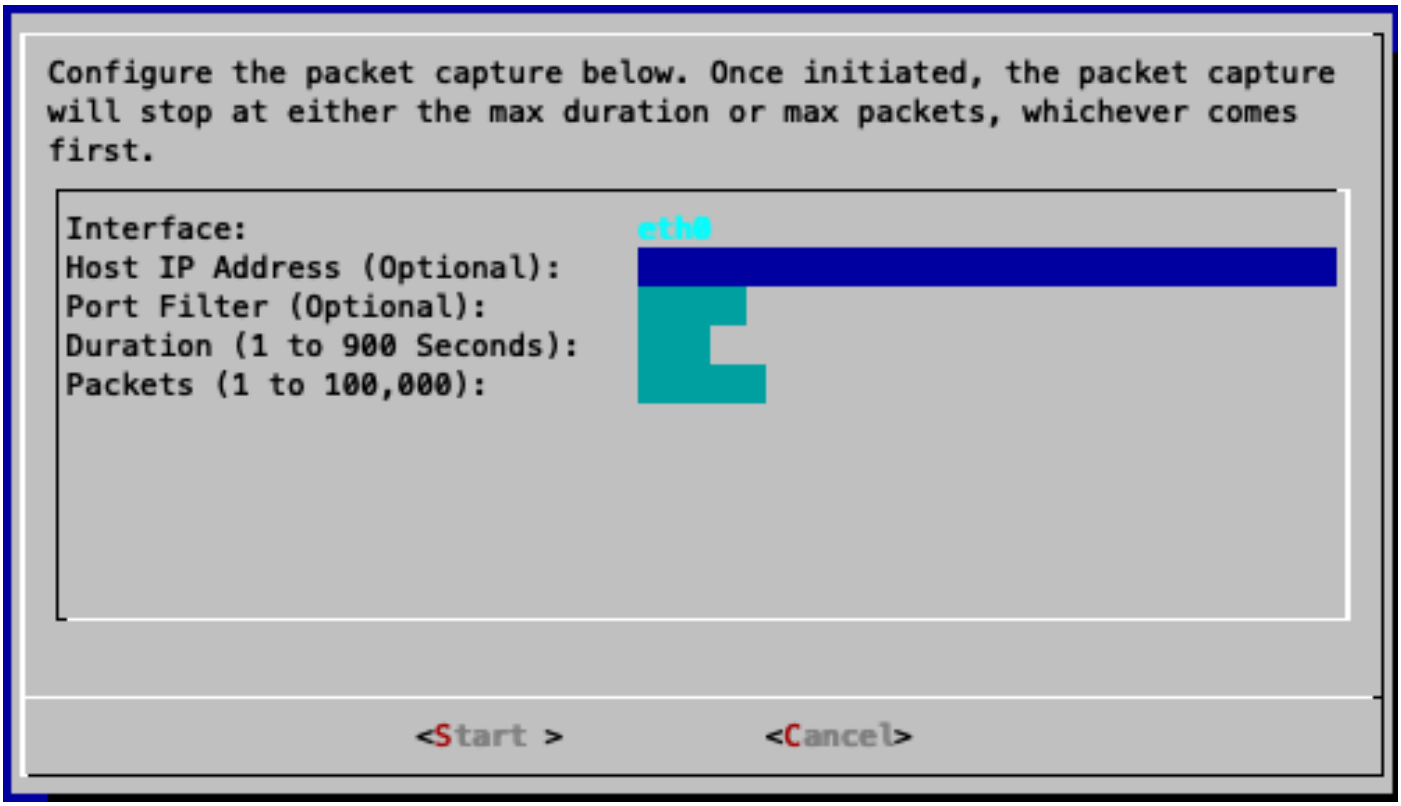
驗證NetFlow/IPFIX模板

要確認NetfFlow/IPFIX模板中包含的欄位：

1.使用sysadmin憑據登入到SNA流量收集器CLI。

2.在SystemConfig功能表上，導覽至：Advanced > Packet Capture

3.輸入在SNA上未顯示流的匯出器的資訊：



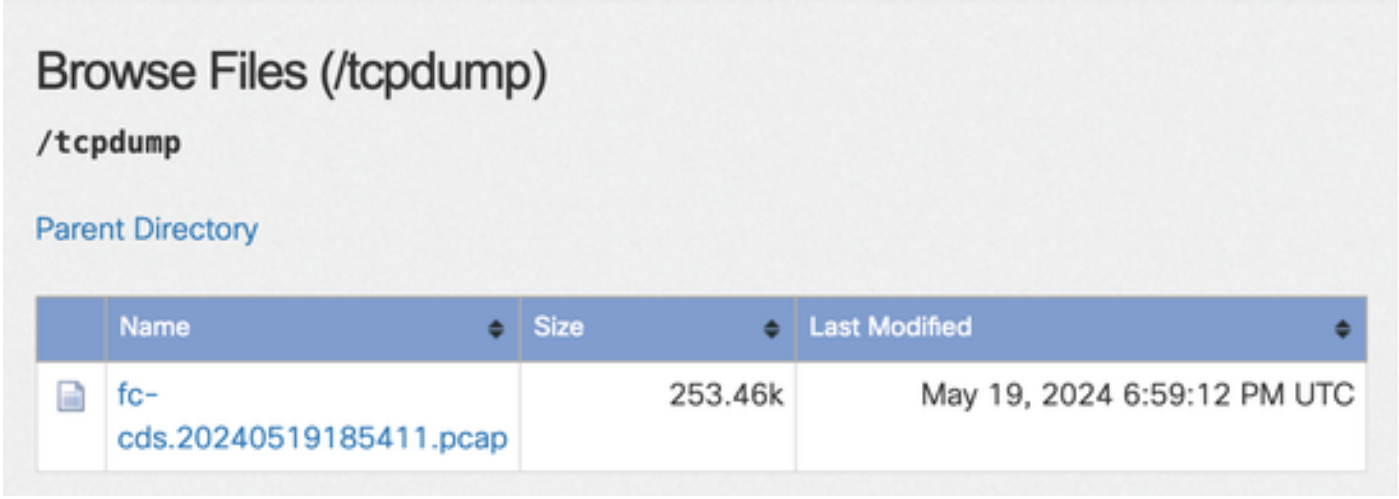
4.等待流程完成。

5.要下載檔案，請使用admin憑據登入到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html

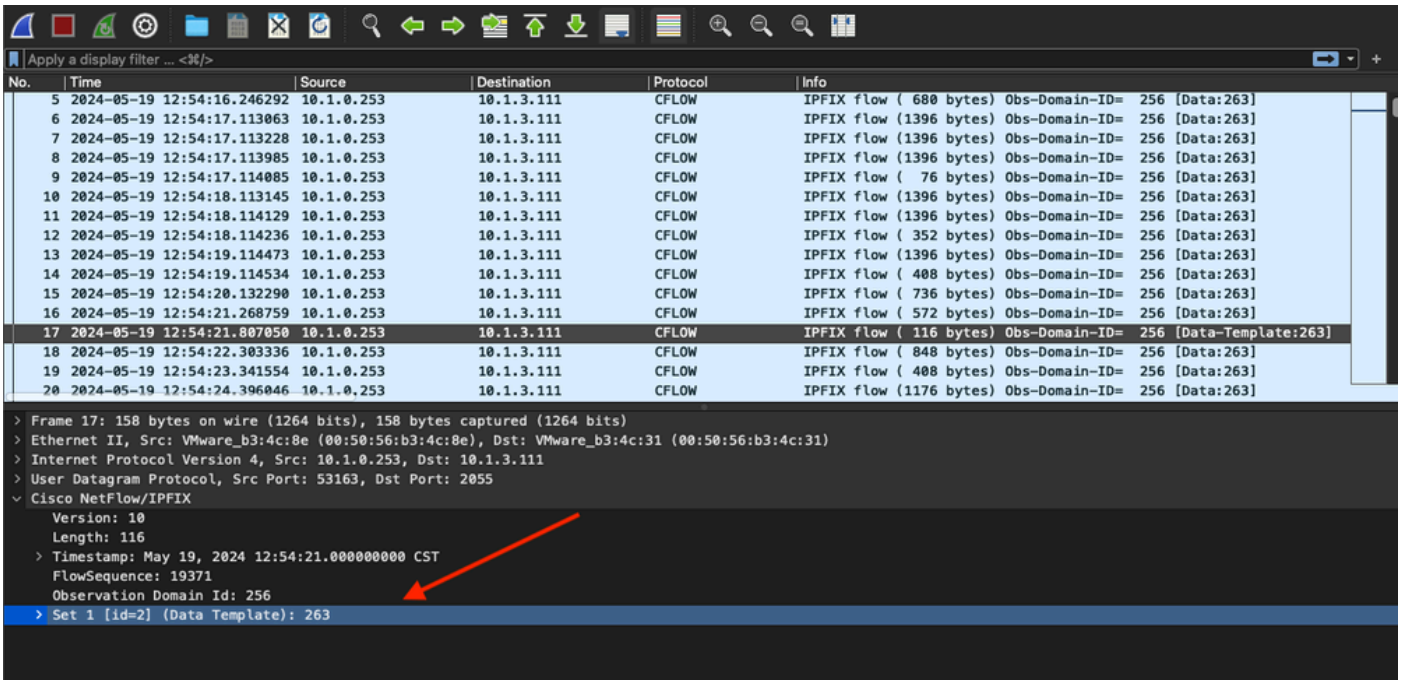
6.在左側面板上，導航到支援 > 瀏覽檔案

7.定位至下一個資料夾：tcpdump

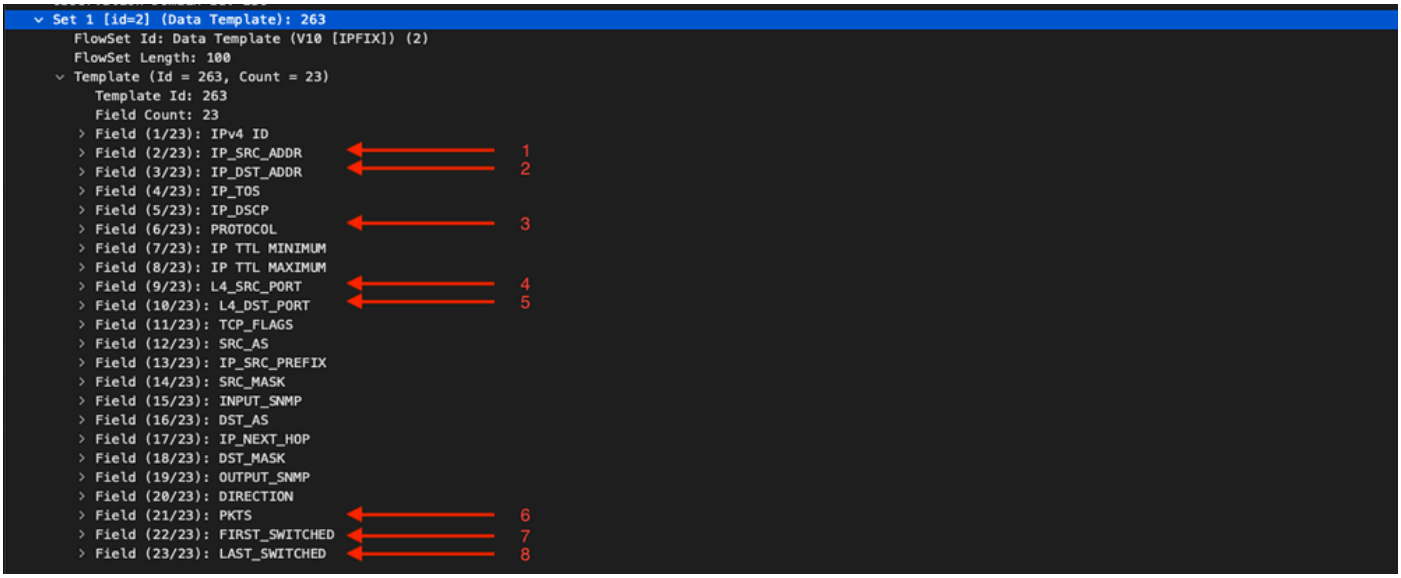
8.按一下資料包捕獲檔案將其下載到本地電腦，然後在Wireshark上開啟該檔案：

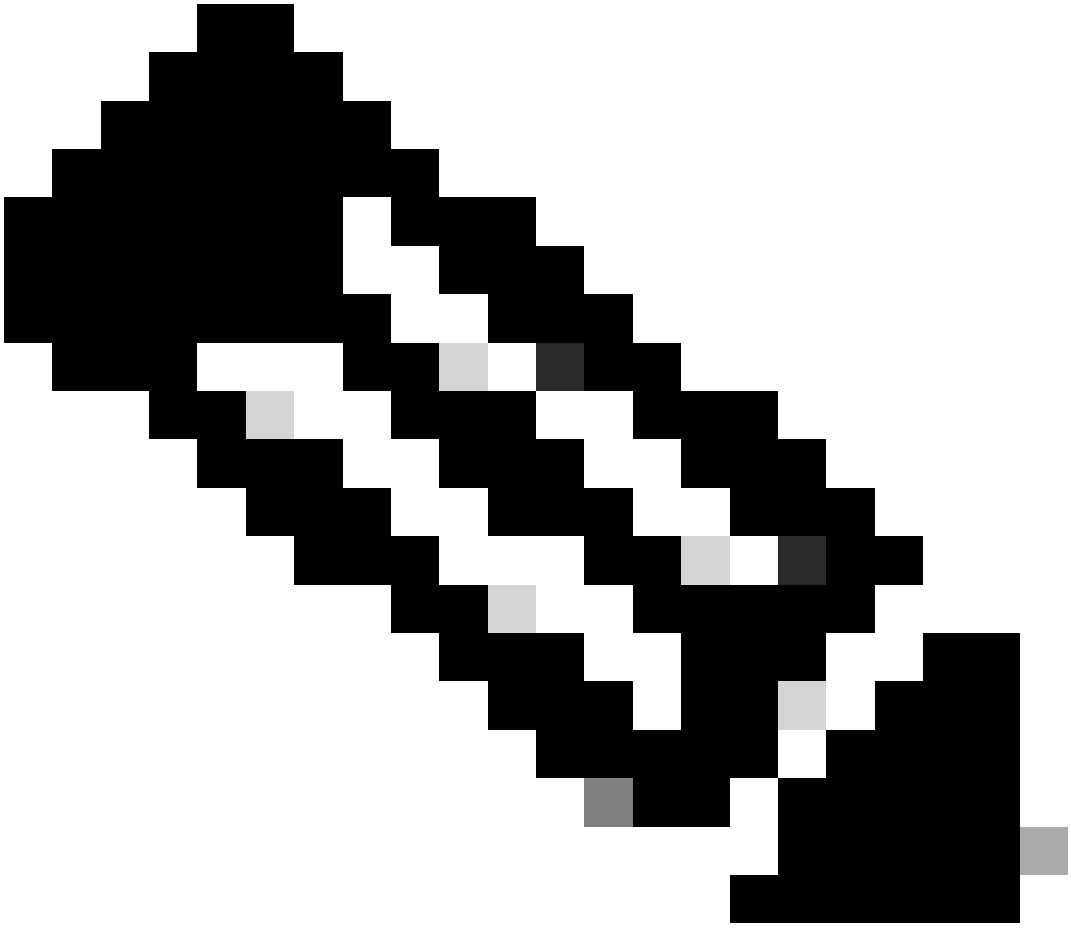


9. 確定接收NetFlow/IPFIX模板的幀。



10.驗證9個必填欄位是否顯示在模板上





附註：請注意，在該模板上，SNA接收遙測所需的9個必填欄位中只有8個，對於此方案，缺少BYTES欄位。

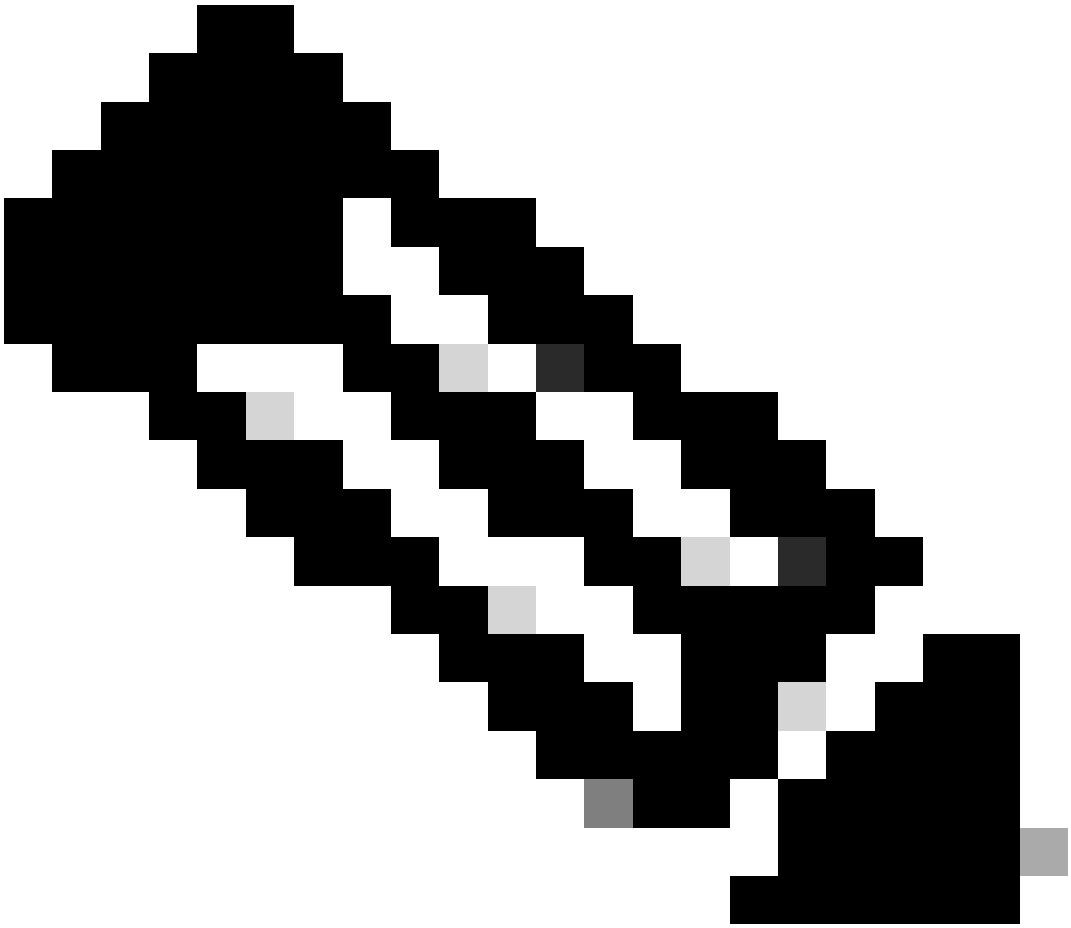
新增缺少的欄位後驗證NetFlow/IPFIX遙測輸入

要確認SNA流量收集器在更改後是否從匯出器接收和插入NetFlow/IPFIX遙測，請執行以下操作：

1. 使用管理員憑據登入到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左側面板上，導航到支援 > 瀏覽檔案
3. 導航到下一個資料夾：sw > today > logs
4. 按一下sw.log檔案將其下載到本地電腦，然後在文本編輯器中開啟。
5. 在日誌底部搜尋這些行

```
19:20:00 I-sch-t: process_5_min_period: begin
19:20:00 I-sch-t: process_5_min_period: periods(184)
19:20:00 S-per-t: Performance Period 184
19:20:00 S-per-t:     Engine status Status normal
```

```
19:20:00 S-per-t:     Processed 10992 flows at 37 fps this period
19:20:00 S-per-t:     Processed 4176 biflows at 14 fps this period
19:20:00 S-per-t:     Dropped 0 flows this period
19:20:00 S-per-t:     Discarded 0 flows this period due to insufficient template data
19:20:00 S-per-t:     Processed 1896017 flows at 35 fps today
19:20:00 S-per-t:     Dropped 0 flows today
19:20:00 S-per-t:     Discarded 36041 flows today due to insufficient template data
19:20:00 S-per-t:     Process instance 0 processed 5575 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 0 processed 2195 biflows at 8 fps this period
19:20:00 S-per-t:     Process instance 1 processed 5417 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 1 processed 1981 biflows at 7 fps this period
19:20:00 S-per-t:     Inserted 2878 flow stats at 10 fps this period
19:20:00 S-per-t:     Inserted 4510 interface stats at 16 fps this period
19:20:00 S-per-t:     Inserted 486734 flow stats at 9 fps today
19:20:00 S-per-t:     Inserted 696260 interface stats at 13 fps today
```



附註：第8行表示最後一個時段沒有丟棄的流。

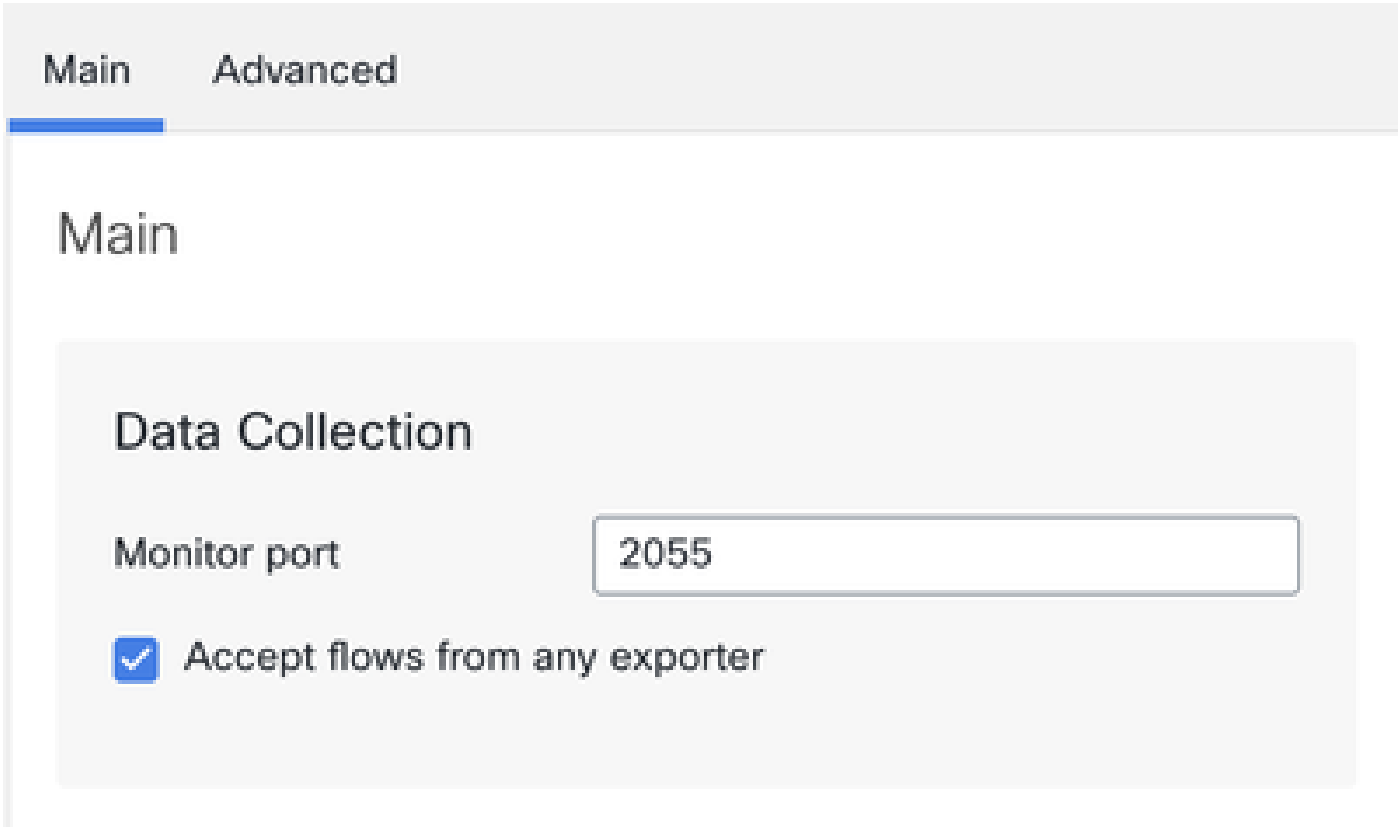
驗證NetFlow/IPFIX遙測接收埠

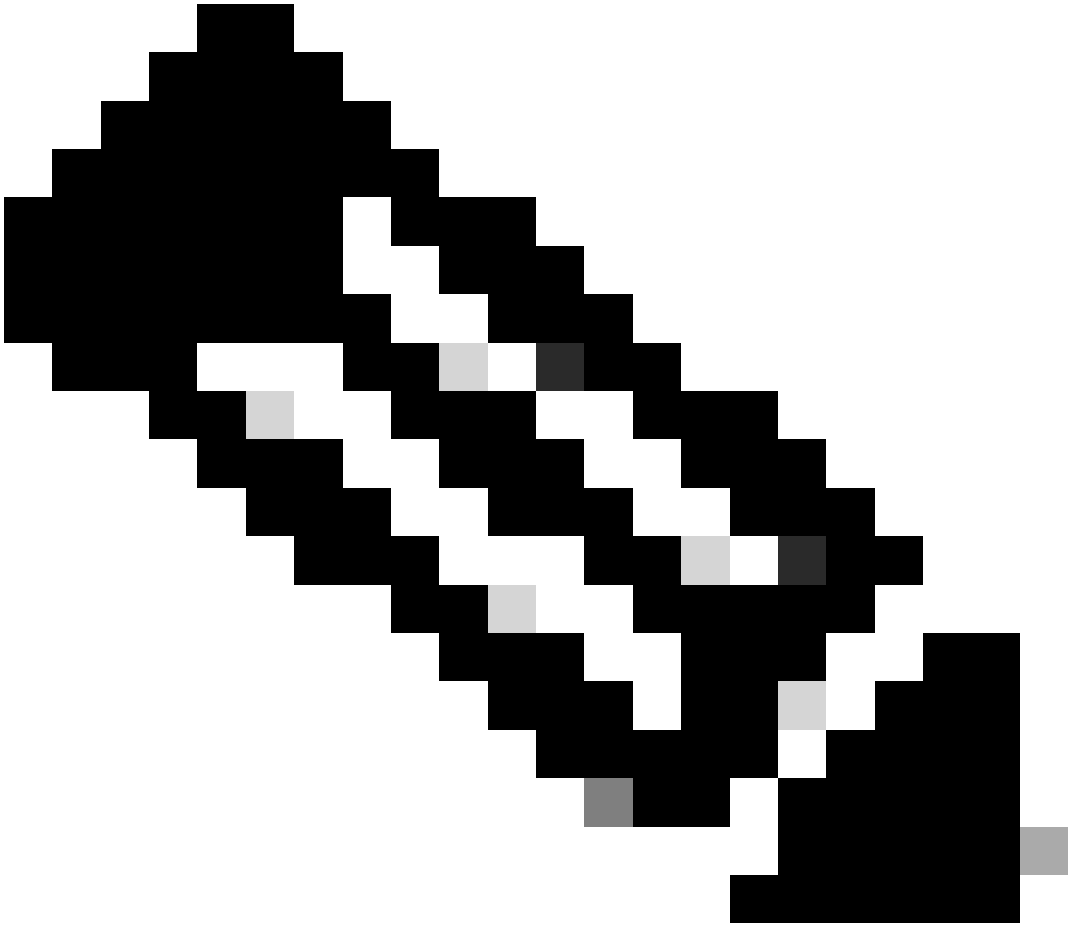
要確認SNA流量收集器是否從正確埠上的匯出器接收NetFlow/IPFIX遙測，請執行以下操作：

1.使用具有管理員許可權的使用者登入到SNA Web UI。

2.在「頂部選單」上，定位至「配置」並選擇「流量收集器」

3.確認SNA流量收集器使用匯出器配置為傳送NetFlow/IPFIX的相同埠





附註：NetFlow的預設埠是2055，但是您可以選擇其他埠，請確保在流量收集器上的首次設定過程中使用同一埠。

驗證NetFlow/IPFIX遙測接收NetFlow選項是否已啟用

要確認是否已啟用NetFlow/IPFIX遙測接收的SNA流量收集器選項：

1. 使用管理員憑據登入到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左側面板上，導航到支援 > 高級設定
3. 確認選項enable_netflow已設定為1:

相關資訊

- 如需其他協助，請聯系技術協助中心(TAC)。需要有效的支援合約：Cisco全球支援聯絡人。
- 您還可以在此處訪問思科安全分析社群。
- 技術支援與文件 - Cisco Systems

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）。