在Secure Analytics中配置SLF和SQLF安全事件

目錄

[簡介](#)

[背景資訊](#)

[調整/配置](#)

[解決方案](#)

簡介

本文檔描述了可用於調整可疑長流(SLF)和可疑安靜長流(SQLF)安全事件的兩個引數。

背景資訊

可疑長流事件是由Secure Analytics生成的特定型別的安全事件，旨在檢測主機之間比正常會話更長的會話。疑似長流事件分為兩種不同型別：可疑長流量和可疑的安靜長流量。

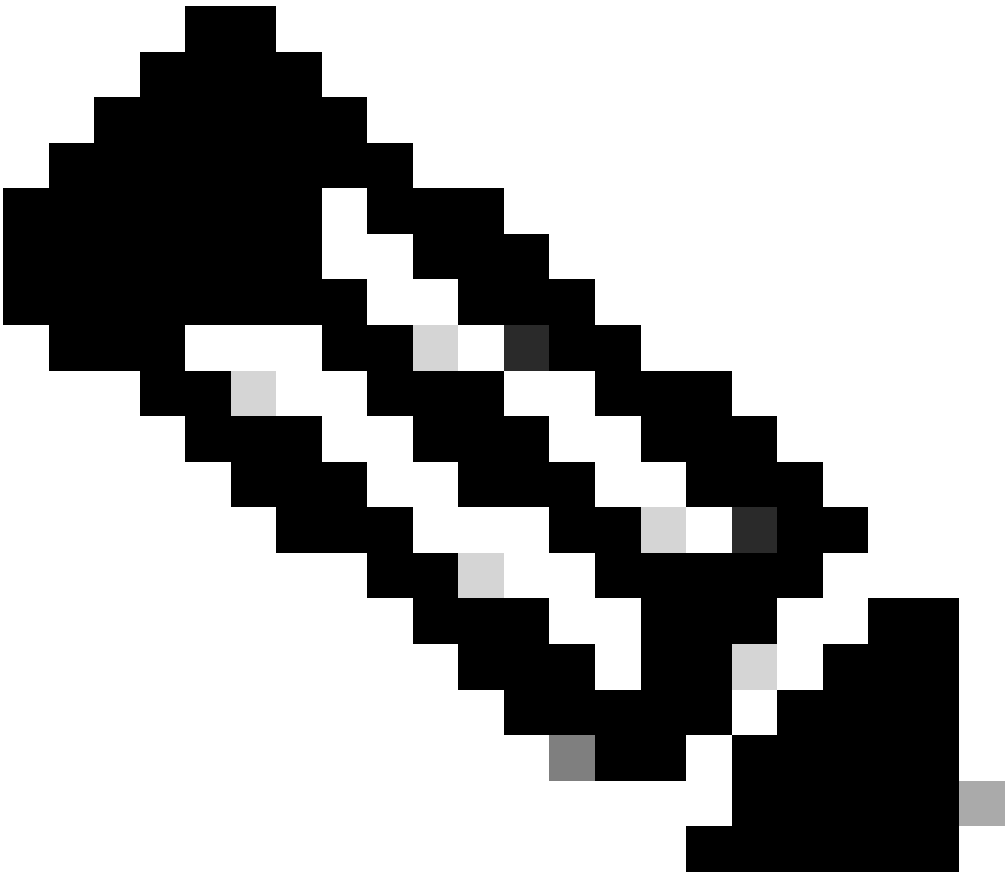
假設您通過隱式VPN將筆記型電腦連線到家用PC三天，但家用PC和筆記型電腦通常都不會進行長流量連線。流量收集器檢測到此異常，並根據通過的流量和流量的持續時間觸發安全事件。這些事件旨在識別長時間運行的流和傳遞最小流量的長時間運行的流。

調整/配置

主要有2個流量收集器配置引數負責控制這兩個事件的行為。

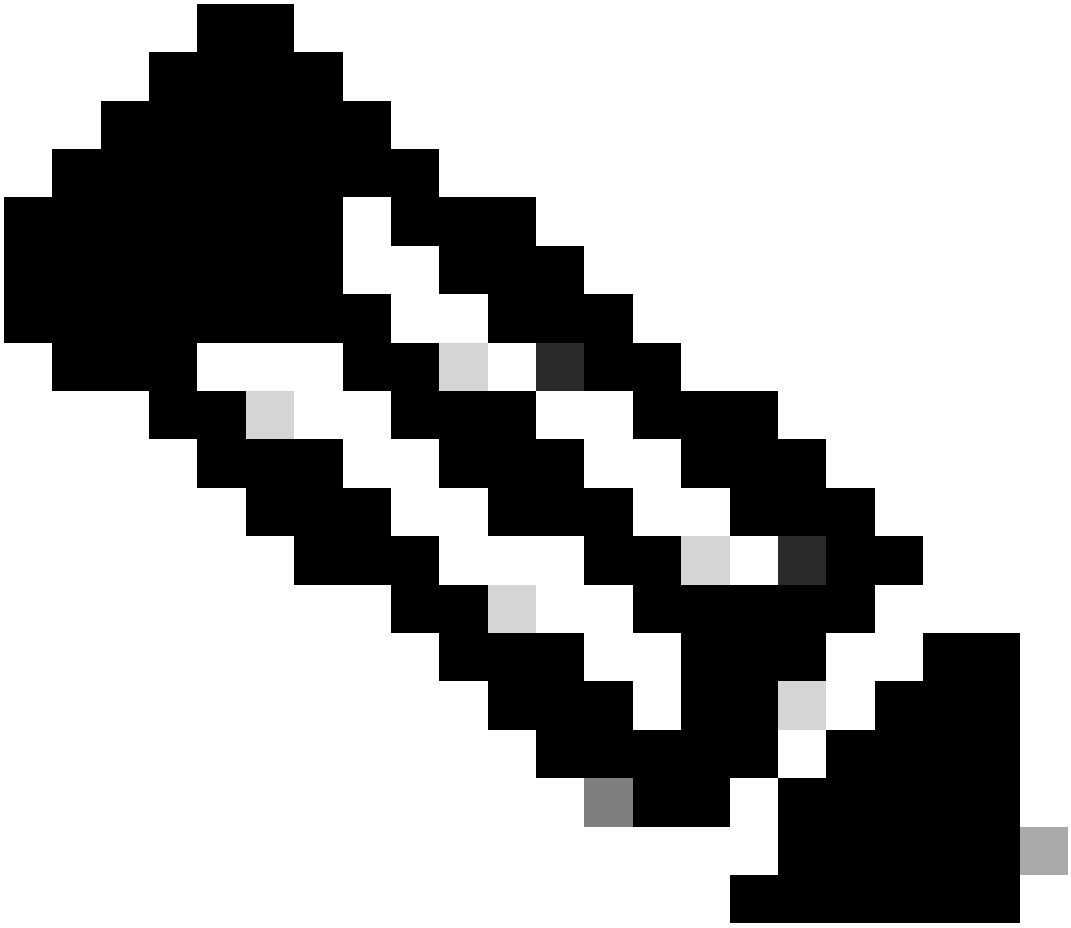
可通過訪問Manager裝置的WebUI中的配置>Flow Collectors > Advanced頁來調整這些設定。

- 將流限定為長持續時間的設定所需的秒數控制可疑長流事件的行為。



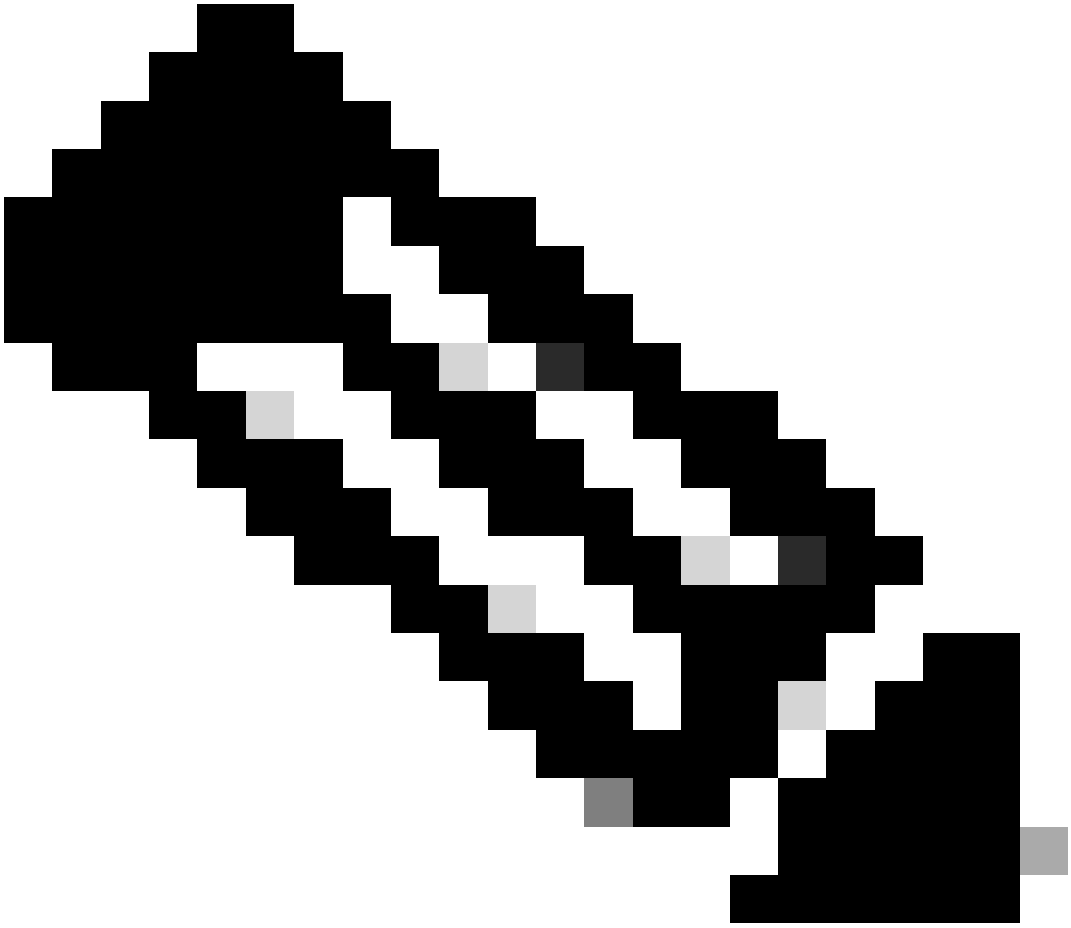
附註：WebUI中的此配置選項設定流收集器lc_thresholds.txt配置檔案中的long_flow_duration引數。

- 將流限定為可疑安靜長流設定所需的秒數控制可疑安靜長流事件的行為。



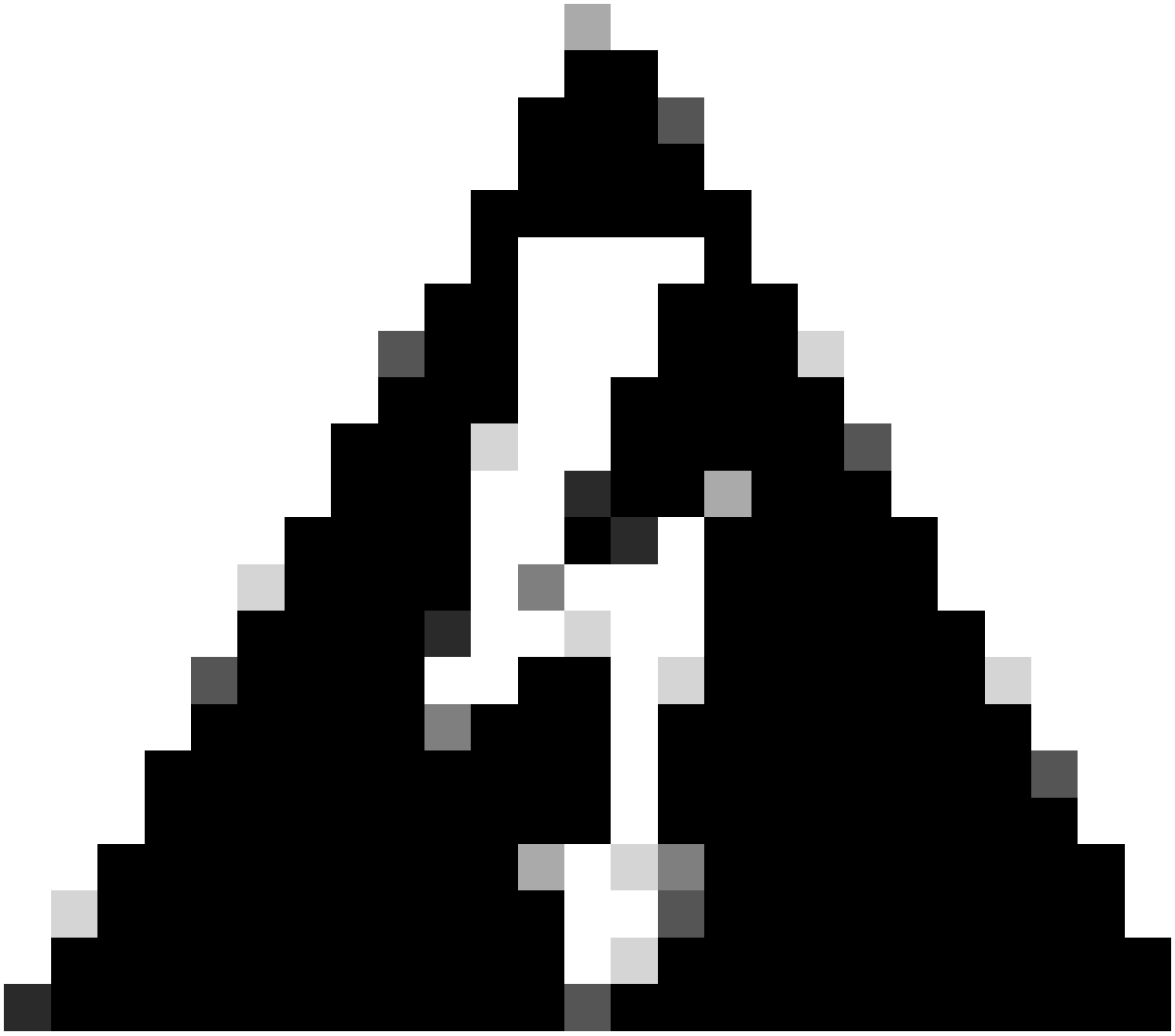
附註：WebUI中的此配置選項設定流收集器lc_thresholds.txt配置檔案中的quiet_long_flow_duration引數。

兩個計數器的預設值為32400 秒（9小時）。



附註：關於更改這些計數器，相關的CDET:

思科錯誤ID CSCwm05128



警告：這僅影響v7.5.1或早期版本。

該缺陷規定可疑靜默長流必須首先也是可疑長流。這意味著，如果將將驗證流為可疑的靜默長流所需的秒更改為短於驗證流為長持續時間設定所需的秒的持續時間，則可能會出現意外結果。

如果更改其中一項或兩項高級設定，則可能導致檢測長流失敗。

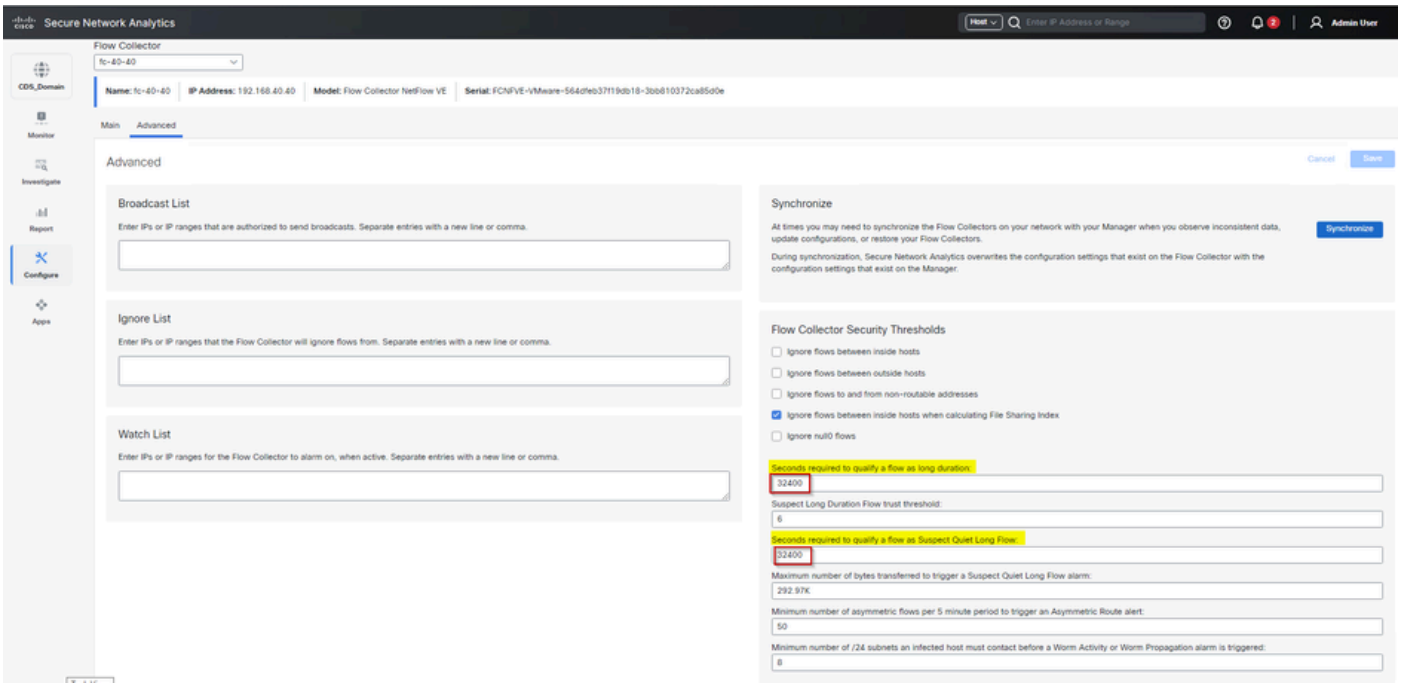
由於靜默長流在定義中也必須是一個長流，正確處理這兩個設定的邏輯是首先使流超過長流要求，然後再測試它是靜默長流。

例如，如果long_flow_duration的預設值保留為9小時，而quiet_long_flow_duration設定為較小的值（如8小時），則在流至少為9小時之前，引擎不會引發平靜的長持續時間流事件。

或者，如果long_flow_duration保留為預設值9小時，而quiet_long_flow_duration設定為10小時，則此配置將有效地禁用靜默持續時間長流事件（除非該流是持續時間大於10小時的quiet_long_flow_duration的單個匯出）。

解決方案

這兩個高級設定需要設定為相同的所需值，或者quiet_long_flow_duration必須始終為>= long_flow_duration。



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）。