配置高級流量收集器引擎自定義安全事件觸發行為

目錄

簡介

本檔案介紹兩個流量收集器進階設定，可變更SNA流量收集器激發自訂安全事件(CSE)的方式。

背景

舊版early_check_age流量收集器高級設定以及新的cse_exec_interval_secs流量收集器高級設定決定了流量收集器引擎觸發自定義安全事件的方式。 流量收集器是SNA系統架構中第一個檢視網路上的流量的裝置，因此流量收集器引擎負責在流量快取中監控流量特徵，並確定流量是否符合指定的自訂安全事件的設定標準。 但是，這些流量收集器高級設定不會更改任何內建核心安全事件的觸發特性。

預設流量收集器行為

預設情況下，流量收集器early_check_age 高級設定配置為160秒。 這表示流量收集器引擎在檢查流量是否與已配置的自定義安全事件匹配之前，至少要等待160秒進入該流量。 預設情況下，此檢查不會在流結束之後再次進行。

之所以選擇此160秒早期檢查值，是因為如果使用最佳實踐，必須將遙測匯出器配置為每60秒傳送一次遙測。 此預設值允許流量收集器在典型環境中有足夠的時間檢視與給定會話/流量兩端相關的流量資訊。 因此，early_check_age未在高級設定清單中預先定義。 這是出於設計的考慮，未經諮詢支援/工程，您不得更改此值。 但是，當考慮長且比較安靜的流特性以及涉及位元組或資料包計數累積的自定義安全事件配置時，此初始設計不能很好地執行。 這就是建立cse_exec_interval_secs高級設定引數的原因。

cse_exec_interval_secs高級設定

在7.4.2中提供，新增了cse_exec_interval_secs流量收集器高級設定，現在可指示引擎根據配置的自定義安全事件定期檢查其流量快取中的流。 此高級設定對於長流特別有用，在長流中，給定流在預設的160秒early_check_age的CSE標準上不匹配，但在流中較晚超過該閾值。 如果沒有此高級設定，自定義安全事件在流結束之前不會觸發，有時可能會在幾天後觸發。

效能影響

執行這些間隔CSE標準檢查流在流生命週期中的次數，比預設定義的檢查次數需要更多CPU。該說明將指導您完成調查流收集器引擎上sw.log檔案的內容，以便在啟用cse_exec_interval_secs引數之前確定效能基線。 如果您正考慮啟用此高級設定，並希望TAC協助確認您的流量收集器運行狀況以準備此更改，可以開啟支援案例並將流量收集器診斷包附加到SR來完成此操作。

測量classify_flows執行緒的持續時間

您可以執行的一個快速效能影響度量是調查從今天開始的sw.log，並將啟用設定之前「cf-」日誌條目後列出的數字與應用設定後列出的數字進行比較。

/lancope/var/sw/today/logs/grep "cf-" sw.log

20:43:21 I-flo-f0:classify_flows:flows n-1744317 ns-178613 ne-188095 nq-0 nd-0 nx-0到–300 cf-21 ft-126473/792802/940383/14216

20:44:20 I-flo-f4:classify_flows:flow n-1754296 ns-191100 ne-167913 nq-0 nd-0 nx-0到–300 cf-20 ft-122830/783378/949392/14928

20:44:21 I-flo-f2:classify_flows:flows n-1773175 ns-191930 ne-169039 nq-0 nd-0 nx-0到–300 cf-20 ft-123055/788507/962264/15431

20:44:21 I-flo-f3:classify_flows:flow n-1750066 ns-189197 ne-165940 nq-0 nd-0 nx-0到–300 cf-20 ft-122563/779792/944192/15154

20:44:21 I-flo-f5:classify_flows:flows n-1753899 ns-190477 ne-168004 nq-0 nd-0 nx-0到–300 cf-20 ft-122261/783375/946651/15423

20:44:21 I-flo-f1:classify_flows:flow n-1763952 ns-191342 ne-169518 nq-0 nd-0 nx-0到–300 cf-20 ft-122782/786822/955997/15175

20:44:21 I-flo-f7:classify_flows:flow n-1757535 ns-188154 ne-166221 nq-0 nd-0 nx-0到–300 cf-20 ft-122808/781388/951528/14363

20:44:21 I-flo-f6:classify_flows:flows n-1764211 ns-190964 ne-169013 nq-0 nd-0 nx-0到–300 cf-21 ft-122713/784446/954149/16320

20:44:21 I-flo-f0:classify_flows:flows n-1764197 ns-189780 ne-168784 nq-0 nd-0 nx-0到–300 cf-21 ft-123290/787327/952186/14352

20:45:22 l-flo-f4:classify_flows:flow n-1780277 ns-177512 ne-149843 nq-0 nd-0 nx-0到–300 cf-21 ft-129553/766777/964933/14864

20:45:22 l-flo-f2:classify_flows:flows n-1789285 ns-175763 ne-155809 nq-0 nd-0 nx-0到–300 cf-21 ft-129685/772482/976850/15289

20:45:22 l-flo-f3:classify_flows:flow n-1774883 ns-177085 ne-149715 nq-0 nd-0 nx-0到–300 cf-22 ft-129067/764272/962000/15090

20:45:22 l-flo-f5:classify_flows:flows n-1775998 ns-176898 ne-150682 nq-0 nd-0 nx-0到–300 cf-22 ft-128835/768374/963353/15347

20:45:22 l-flo-f1:classify_flows:flow n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0到–300 cf-22 ft-129255/770212/970360/15129

cf條目代表「Classify Flows」。 這表示執行緒通過它負責的Flow Cache部分所花費的秒數。 在「分類流」執行緒中，針對流應用CSE。 如果您看到這些數字在啟用該功能後上升，這是衡量對效能整體影響的良好指標。

新增此高級間隔設定後應出現上升，但如果此數字接近60,請刪除該設定，因為影響太大。預計會增加幾秒鐘，而且被認為是合理的。

績效期間的引擎狀態

您可以執行的另一項「之前與之後」效能測量是檢視sw.log檔案中的「效能時段」部分，該檔案每5分鐘記錄一次，以衡量該設定對流量處理的影響。 您也可以使用grep查詢這些塊。 如果引擎不堪重負，則必須禁用此高級設定間隔檢查。

/lancope/var/sw/today/logs/ grep -A3 "效能週期" sw.log

注意除「引擎狀態正常」以外的任何狀態。

「引擎狀態輸入速率過高」等狀態表示classify_flows執行緒佔用的CPU過多。

SFI — 靜態流索引

表示分類執行緒無法通過流快取完成它們的傳遞：它代表「靜態流索引」，它表示分類流執行緒中存在掙扎。這本身並不是災難，但它表明引擎開始達到極限，在當前cf級別效能開始下降。

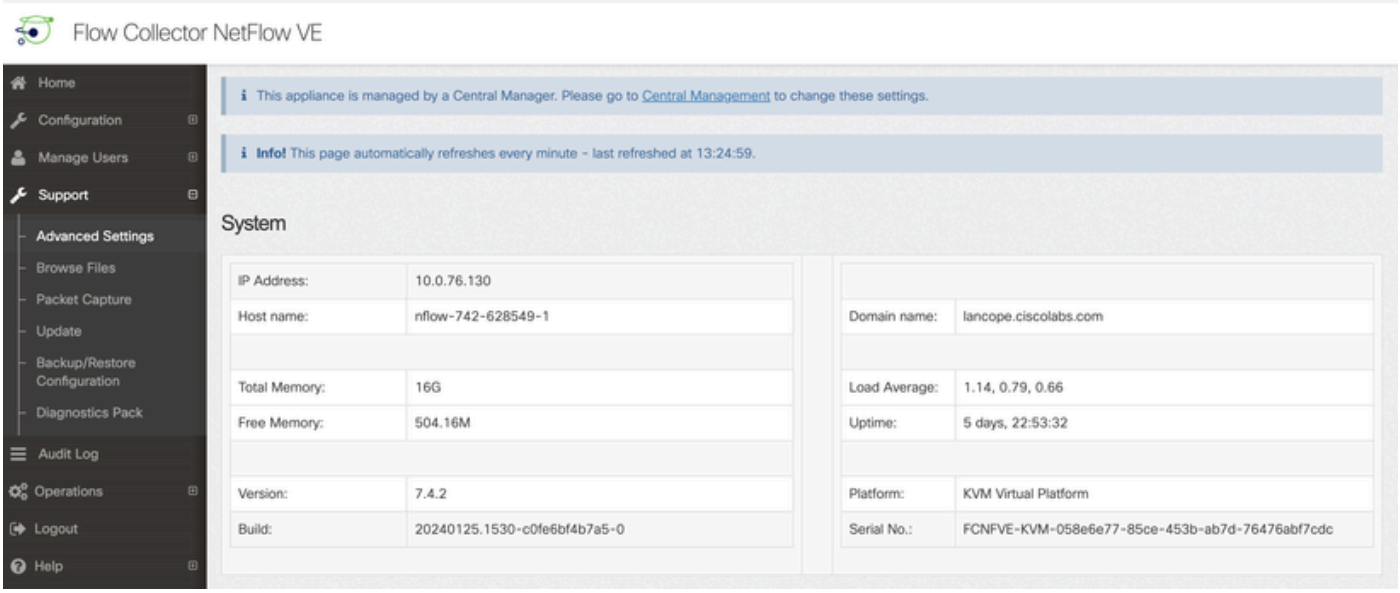
sw.log:16:09:49 l-flo-f1: classify_flows:sfi:base(8388608)(10522745 -> 11014427)max(16777215)cod(1)(491681/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f3:classify_flows:sfi:base(25165824)(27269277 -> 27754304)max(33554431)cod(1)(485026/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f4: classify_flows:sfi:base(33554432)(35652656 -> 36138422)max(41943039)cod(1)(485765/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f2: classify_flows:sfi:base(16777216)(18985626 -> 19499308)max(25165823)cod(1)(513681/8388608)---------->(6%)
sw.log:16:09:54 l-flo-f0:classify_flows:sfi:base(0)(1786480 -> 421161)max(8388607)cod(1)(7023288/8388608)---------->(83%)

sw.log:16:10:49 l-flo-f0:classify_flows:sfi:base(0)(421161 ->
1402189)max(8388607)cod(0)(981027/8388608)---------->(11%)
sw.log:16:10:49 l-flo-f2: classify_flows:sfi:base(16777216)(19499308 ->
17522620)max(25165823)cod(0)(6411919/8388608)---------->(76%)
sw.log:16:10:49 l-flo-f1: classify_flows:sfi:base(8388608)(11014427 ->
8976309)max(16777215)cod(0)(6350489/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f3:classify_flows:sfi:base(25165824)(27754304 ->
25702968)max(33554431)cod(0)(6337271/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f7:classify_flows:sfi:base(58720256)(58848913 ->
59630528)max(67108863)cod(0)(781614/8388608)---------->(9%)
sw.log:16:10:49 l-flo-f4: classify_flows:sfi:base(33554432)(36138422 ->
34064015)max(41943039)cod(1)(6314200/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f5:classify_flows:sfi:base(41943040)(43310891 ->
44059251)max(50331647)cod(1)(748359/8388608)---------->(8%)
sw.log:16:10:49 l-flo-f6: classify_flows:sfi:base(50331648)(51714170 ->
52444661)max(58720255)cod(1)(730490/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f5:classify_flows:sfi:base(41943040)(44059251 ->
42121104)max(50331647)cod(0)(6450460/8388608)---------->(76%)
sw.log:16:11:49 l-flo-f0:classify_flows:sfi:base(0)(1402189 ->
2373792)max(8388607)cod(1)(971602/8388608)---------->(11%)
sw.log:16:11:49 l-flo-f6: classify_flows:sfi:base(50331648)(52444661 ->
50483491)max(58720255)cod(1)(6427437/8388608)---------->(76%)
sw.log:16:11:49 l-flo-f3:classify_flows:sfi:base(25165824)(25702968 ->
26385879)max(33554431)cod(1)(682910/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f1: classify_flows:sfi:base(8388608)(8976309 ->
9662167)max(16777215)cod(1)(685857/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f4: classify_flows:sfi:base(33554432)(34064015 ->
34742593)max(41943039)cod(1)(678577/8388608)---------->(8%)
sw.log:16:11:50 l-flo-f7:classify_flows:sfi:base(58720256)(59630528 ->
60298366)max(67108863)cod(1)(667837/8388608)---------->(7%)
sw.log:16:11:50 l-flo-f2: classify_flows:sfi:base(16777216)(17522620 ->
18202249)max(25165823)cod(1)(679628/8388608)---------->(8%)

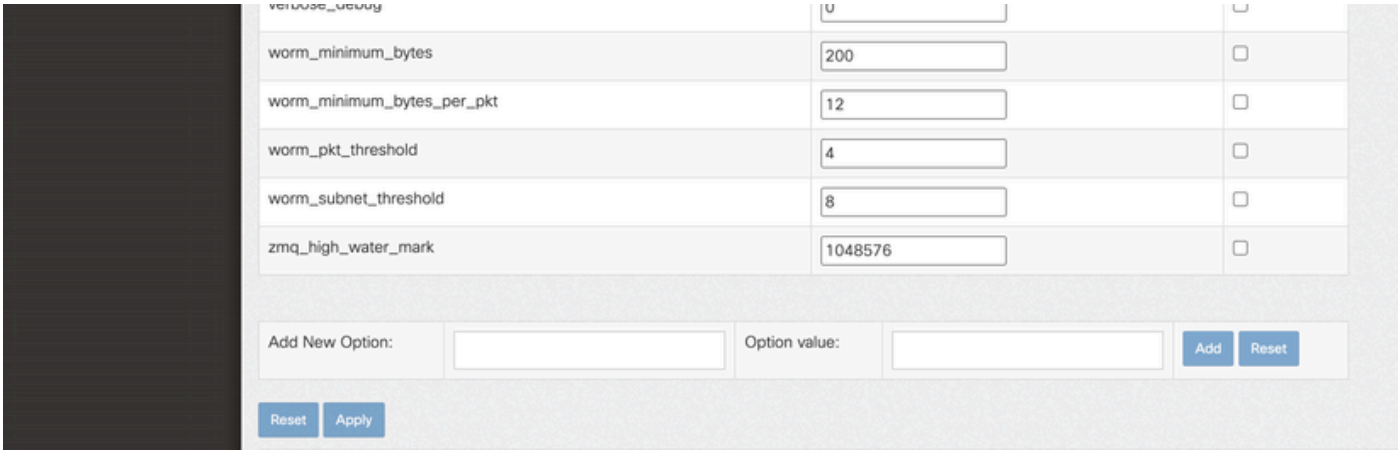
設定

開啟Web瀏覽器並直接導航到流量收集器裝置IP。 以本地管理員使用者身份登入。

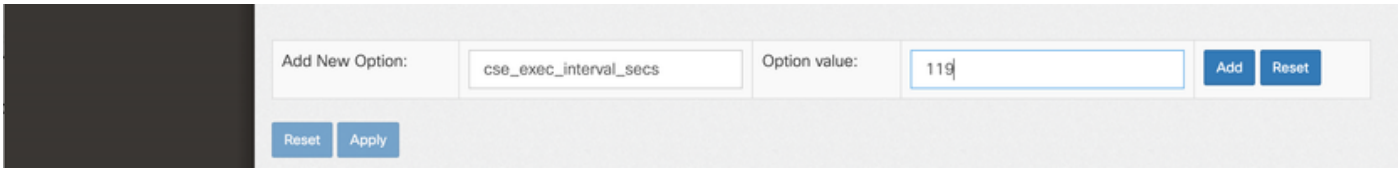
導航至Support（支援）— > Advanced Settings（高級設定）



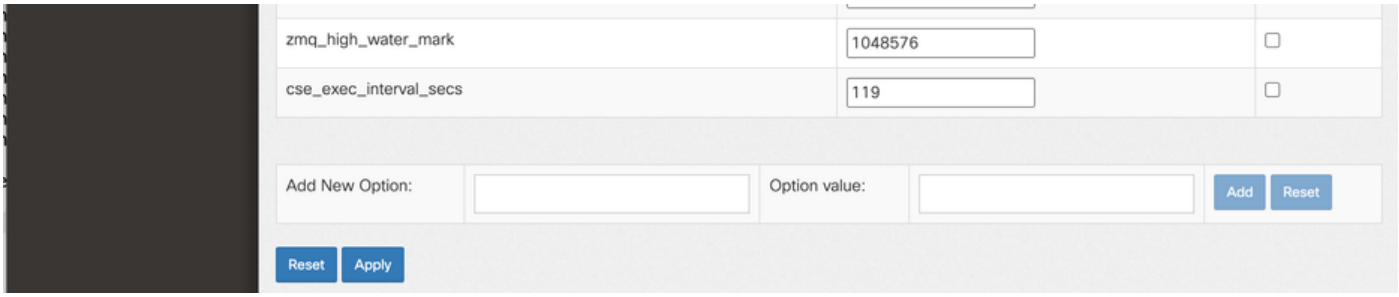
向下滾動「高級設定」螢幕，顯示清單底部的「新增新選項」配置框



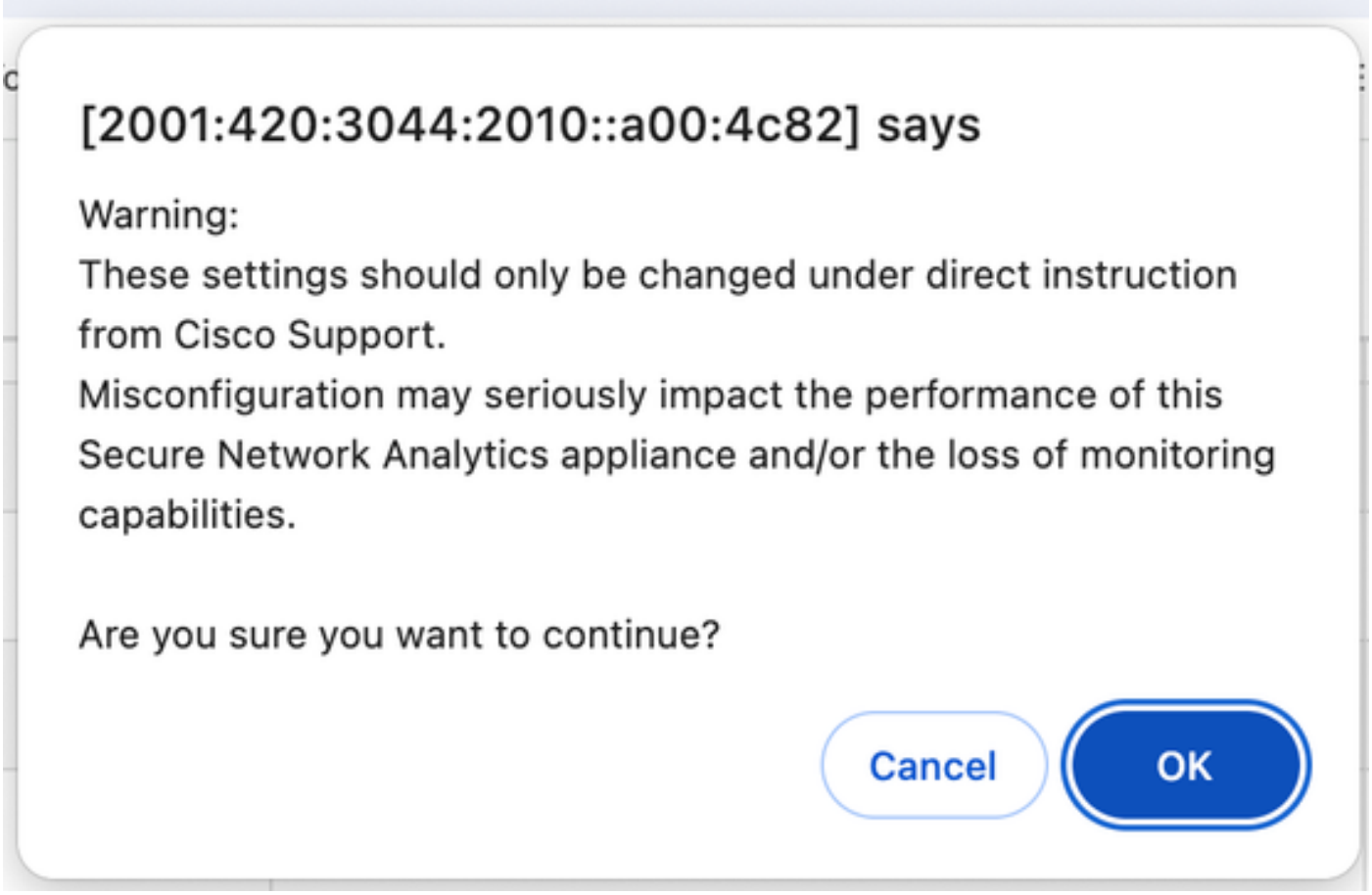
在「新增新選項：編輯」框中，輸入cse_exec_interval_secs，然後在「選項值：編輯」框中輸入119。編輯這些框將啟用Add按鈕。 在Add New Option:編輯框中輸入cse_exec_interval_secs後，按Add按鈕，在Option Value:/編輯框中輸入119。



在要輸入多個新的高級設定時，新增新選項和選項值：編輯框將清除以準備另一個條目。 新新增的Advanced Settings會在新增時加到清單的底部。 這樣使用者就可以檢查該條目。 Advanced Setting的確切拼寫與大小寫一樣重要。 所有Advanced Settings都以小寫形式顯示。



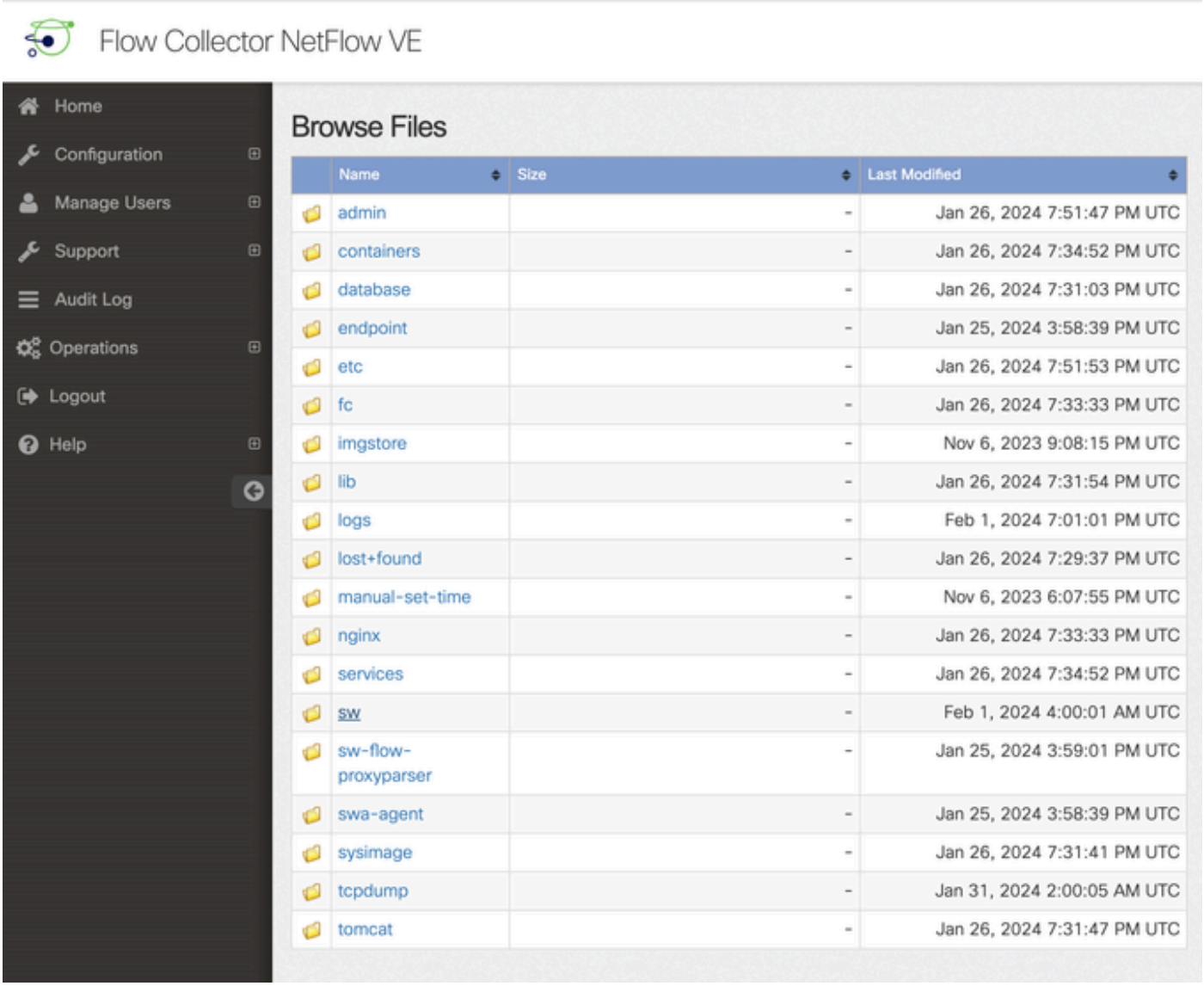
正確輸入Advanced Setting後，按Apply按鈕。 請注意，有時Apply按鈕未啟用。 要啟用此功能，請點選新增新選項：編輯框，然後啟用應用按鈕以供點選。 出現此彈出視窗時，按「確定」按鈕以提交新的「高級設置和值」。



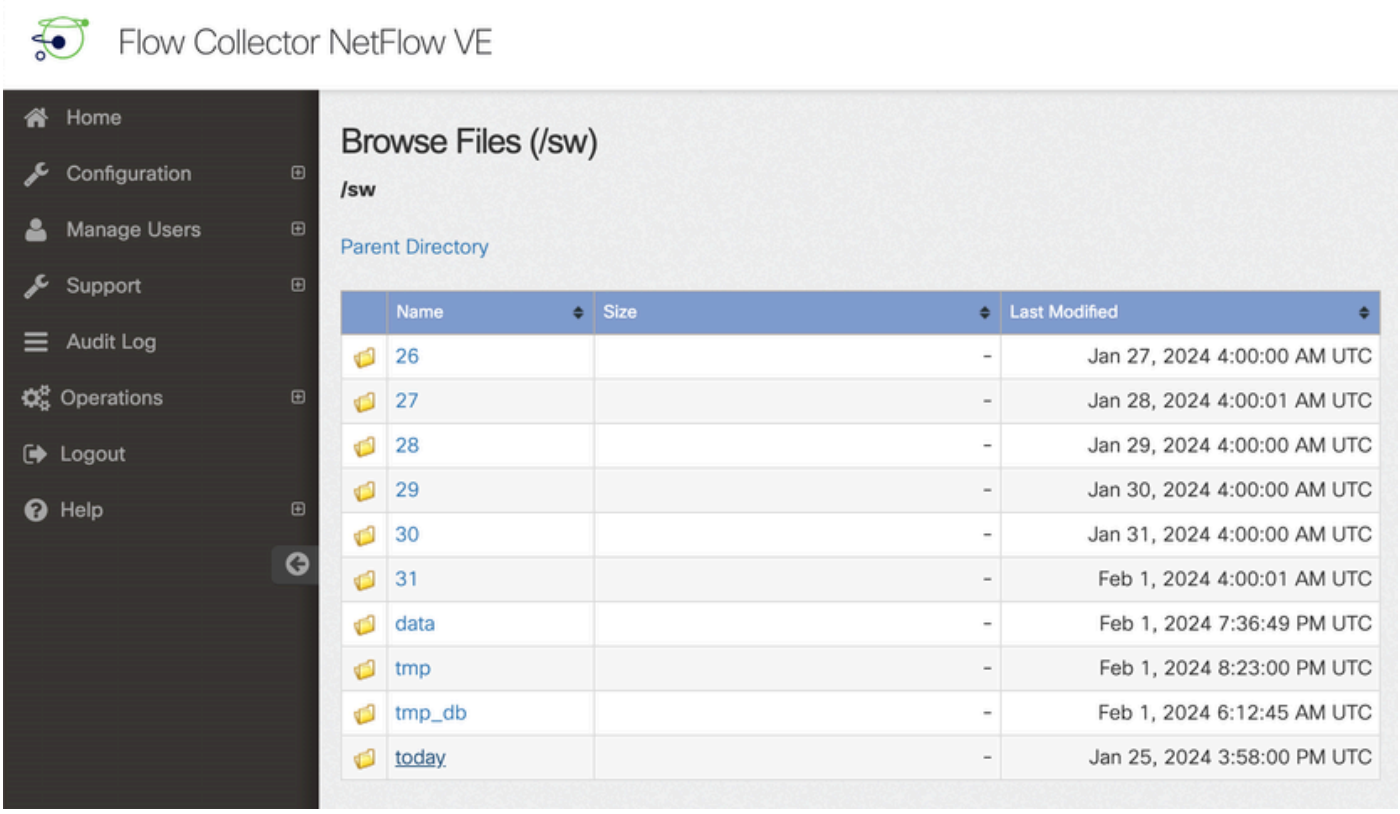
確認更改

此最終驗證是最重要的。再次按一下Support選單，然後選擇Browse Files。

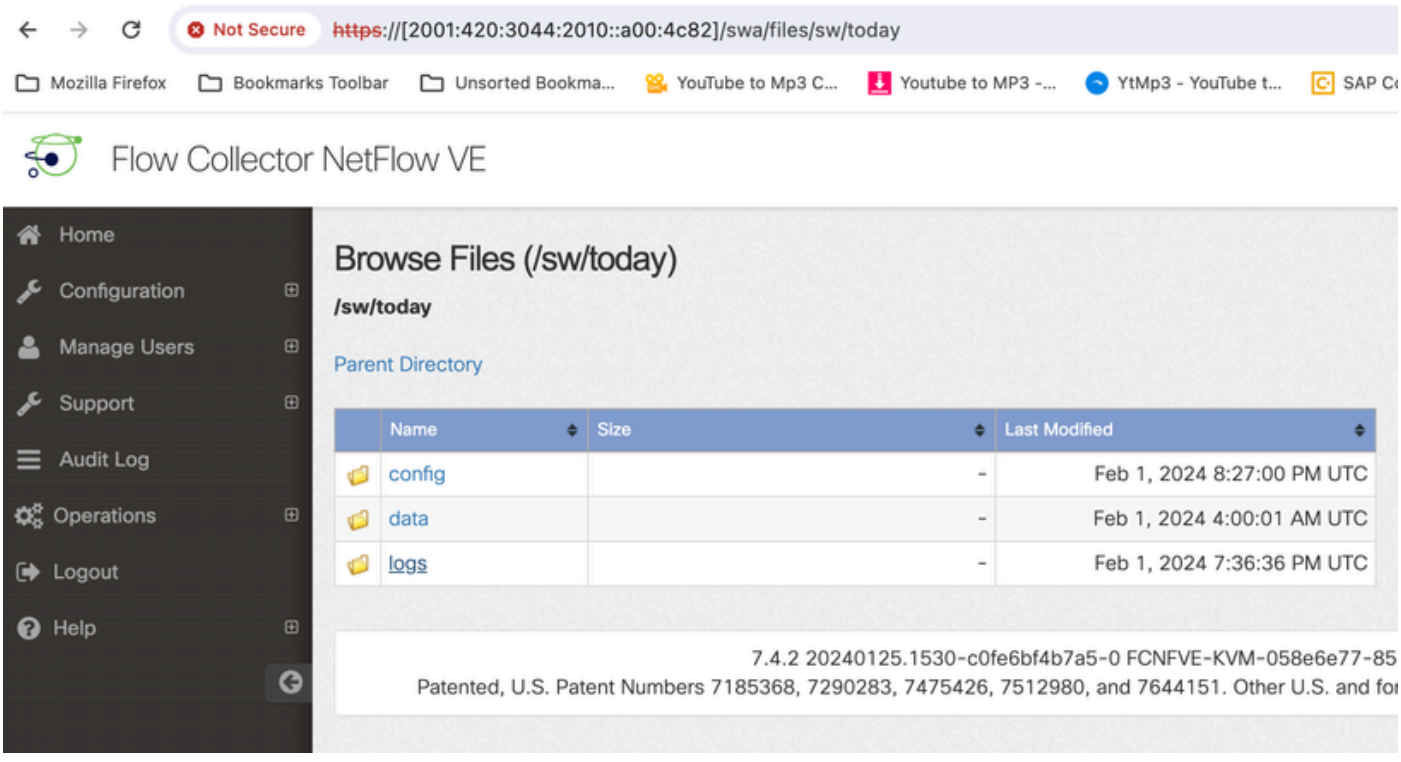
這會將您引導到FC上的檔案系統。按一下sw。


Flow Collector NetFlow VE
Home
Configuration
Manage Users
Support
Audit Log
Operations
Logout
Help
Browse Files
Name
Size
Last Modified
admin - Jan 26, 2024 7:51:47 PM UTC
containers - Jan 26, 2024 7:34:52 PM UTC
database - Jan 26, 2024 7:31:03 PM UTC
endpoint - Jan 25, 2024 3:58:39 PM UTC
etc - Jan 26, 2024 7:51:53 PM UTC
fc - Jan 26, 2024 7:33:33 PM UTC
imgstore - Nov 6, 2023 9:08:15 PM UTC
lib - Jan 26, 2024 7:31:54 PM UTC
logs - Feb 1, 2024 7:01:01 PM UTC
lost+found - Jan 26, 2024 7:29:37 PM UTC
manual-set-time - Nov 6, 2023 6:07:55 PM UTC
nginx - Jan 26, 2024 7:33:33 PM UTC
services - Jan 26, 2024 7:34:52 PM UTC
sw - Feb 1, 2024 4:00:01 AM UTC
sw-flow-proxyparser - Jan 25, 2024 3:59:01 PM UTC
swa-agent - Jan 25, 2024 3:58:39 PM UTC
sysimage - Jan 26, 2024 7:31:41 PM UTC
tcpdump - Jan 31, 2024 2:00:05 AM UTC
tomcat - Jan 26, 2024 7:31:47 PM UTC

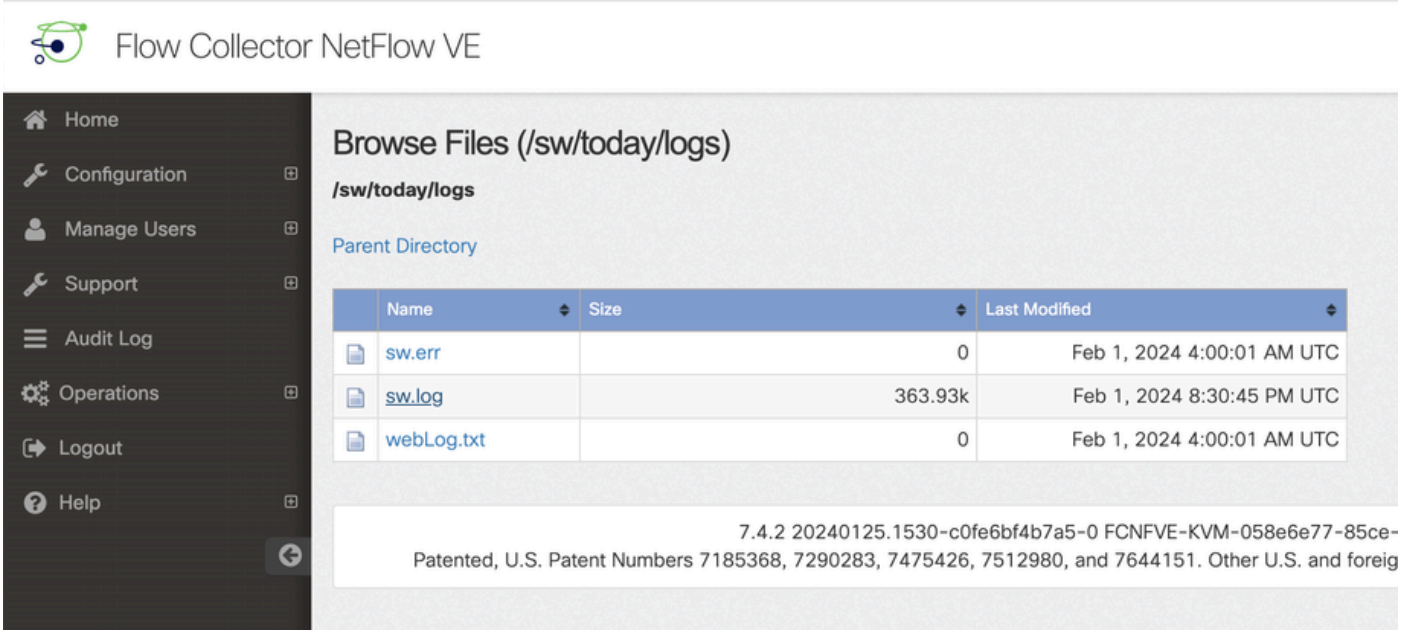
按一下「今天」



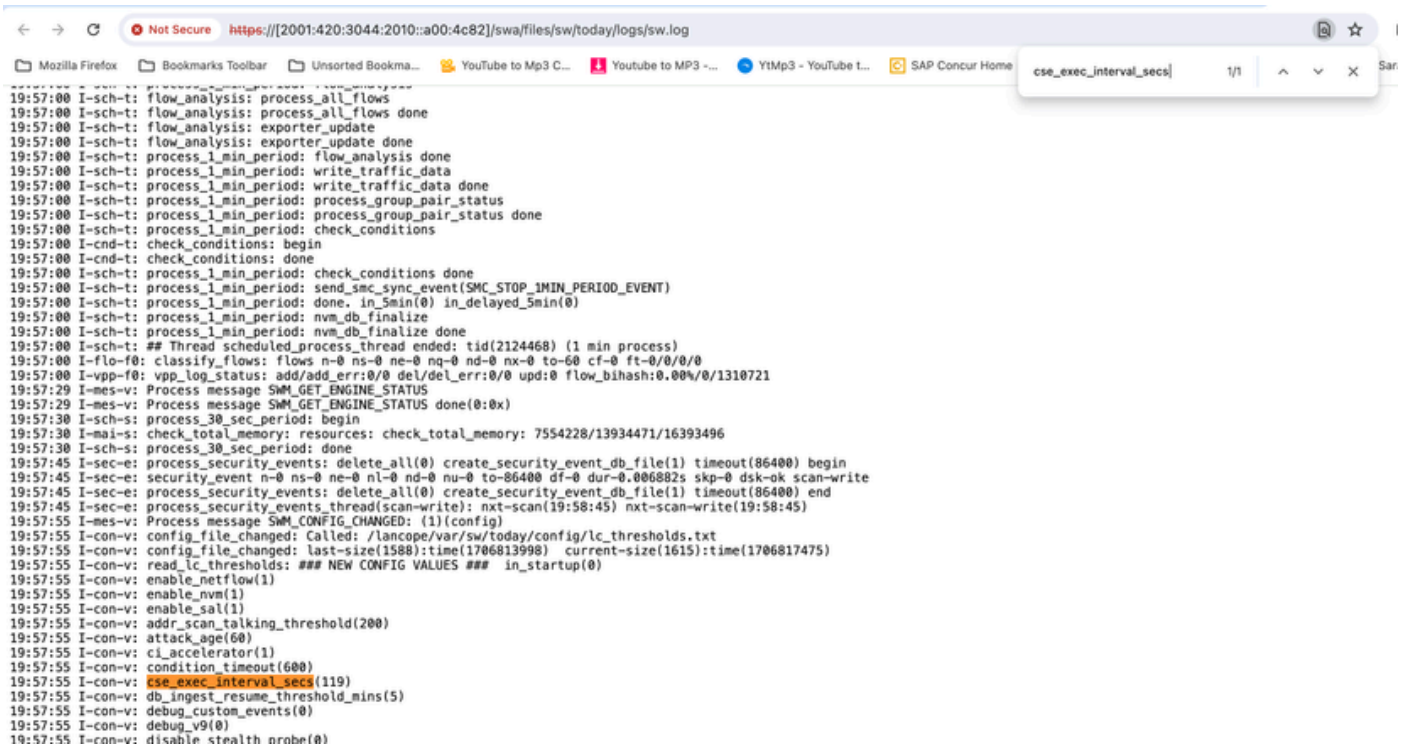
按一下logs。



按一下sw.log



在瀏覽器頁面中執行搜尋，在搜尋框中輸入cse_exec_interval_secs以查詢「Advanced Setting（高級設定）」



已接受的高級設定如螢幕截圖所示列出。

未接受的選項以「不是輸入配置的一部分」的形式列出，在本例中是由於使用者錯誤拼寫了設定。這就是進行此類配置更改後檢查日誌的重要性所在。

```
20:41:52 I-con-v: read_lc_thresholds: ### NEW CONFIG VALUES ###  in_startup(0)
20:41:52 I-con-v: enable_netflow(1)
20:41:52 I-con-v: enable_nvm(1)
20:41:52 I-con-v: enable_sal(1)
20:41:52 I-con-v: addr_scan_talking_threshold(200)
20:41:52 I-con-v: attack_age(60)
20:41:52 I-con-v: ci_accelerator(1)
20:41:52 I-con-v: condition_timeout(600)
20:41:52 I-con-v: (cse_exec_interval_sec) not part of input configuration
20:41:52 I-con-v: cse_exec_interval_secs(119)
```

祝賀你！

您剛剛輸入了一個新的高級設定，並已驗證引擎是否接受該設定。

現在，該功能已啟用，以便在流量達到early_check_age (預設為160 秒)後約每2分鐘對流量執行CSE邏輯。

如果CSE規則涉及累積位元組計數，則此功能將改進CSE觸發符合您定義的條件的流的時機。

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）。