Benutzerdefiniertes Sicherheitsereignisauslöseverhalten für die erweiterte Flow Collector Engine konfigurieren

Inhalt

Einleitung

In diesem Dokument werden zwei erweiterte Flow Collector-Einstellungen beschrieben, die die Art und Weise ändern können, wie der SNA Flow Collector benutzerdefinierte Sicherheitsereignisse (CSEs) auslöst.

Hintergrund

Die erweiterte Einstellung early_check_age flow collector zusammen mit der neuen erweiterten Einstellung case_exec_interval_secs flow collector bestimmen, wie benutzerdefinierte Sicherheitsereignisse von der Flow Collector-Engine ausgelöst werden. Der Flow Collector ist die erste Appliance in der SNA-Systemarchitektur, die den Datenfluss im Netzwerk erkennt. Daher ist die Flow Collector Engine für die Überwachung der Eigenschaften des Datenflusses bzw. der Datenflüsse im Flow Cache und für die Bestimmung, ob der Datenfluss die konfigurierten Kriterien eines bestimmten benutzerdefinierten Sicherheitsereignisses erfüllt, zuständig. Diese erweiterten Einstellungen für Flow Collector ändern jedoch NICHT die Feuereigenschaften der integrierten Core-Sicherheitsereignisse.

Standardverhalten von FlowCollector

Standardmäßig ist die erweiterte Einstellung early_check_age des Flow Collectors auf 160 Sekunden konfiguriert. Das bedeutet, dass die Flow Collector-Engine mindestens 160 Sekunden in einen Flow wartet, bevor überprüft wird, ob dieser Flow mit einem konfigurierten

benutzerdefinierten Sicherheitsereignis übereinstimmt. Diese Prüfung wird standardmäßig erst nach Ende des Datenflusses wiederholt.

Dieser Wert für die frühzeitige Überprüfung von 160 Sekunden wurde speziell gewählt, da Telemetrie-Exporteure bei Verwendung von Best Practices so konfiguriert werden müssen, dass sie alle 60 Sekunden Telemetrie senden. Mit diesem Standardwert kann der Flow Collector in einer typischen Umgebung genügend Zeit haben, um die Informationen zu beiden Seiten einer bestimmten Konversation bzw. eines bestimmten Flusses anzuzeigen. Aus diesem Grund ist die early_check_age in der Liste der erweiterten Einstellungen nicht vordefiniert. Dies geschieht durch das Design, und Sie dürfen diesen Wert nicht ändern, ohne vorher mit dem Support/Engineering beraten zu haben. Dieses anfängliche Design bietet jedoch keine gute Leistung, wenn es um lange und leise Datenflusseigenschaften in Verbindung mit benutzerdefinierten Sicherheitsereigniskonfigurationen geht, bei denen Byte- oder Paketzahlen angesammelt werden. Dies war der Grund für die Erstellung des erweiterten Einstellungsparameters cse_exec_interval_secs .

Die erweiterte Einstellung von cse_exec_interval_secs

Die erweiterte Einstellung cse_exec_interval_secs Flow Collector wurde in 7.4.2 zur Verfügung gestellt und ermöglicht es nun, die Engine anzuweisen, die Datenflüsse im Flow Cache regelmäßig mit konfigurierten benutzerdefinierten Sicherheitsereignissen zu vergleichen. Diese erweiterte Einstellung ist besonders nützlich bei langen Datenflüssen, bei denen ein bestimmter Datenfluss nicht den CSE-Kriterien in der Standardeinstellung von 160 Sekunden early_check_age entspricht, aber diesen Schwellenwert später im Datenfluss überschreitet. Ohne diese erweiterte Einstellung wird das benutzerdefinierte Sicherheitsereignis erst nach dem Ende des Datenflusses ausgelöst, was in manchen Fällen Tage später der Fall sein kann.

Auswirkungen auf die Leistung

Bei der Ausführung dieser Intervall-CSE-Kriterien werden Flüsse öfter im Lebenszyklus des Flusses überprüft, als durch die Standardwerte definiert wird. Die Anweisungen führen Sie durch die Untersuchung des Inhalts der Datei sw.log auf der Flow Collector Engine, um eine Leistungsbasislinie zu ermitteln, bevor Sie den Parameter cse_exec_interval_secs aktivieren. Wenn Sie erwägen, diese erweiterte Einstellung zu aktivieren, und TAC bei der Bestätigung Ihres Flow Collector-Status zur Vorbereitung auf diese Änderung unterstützen möchten, können Sie ein Support-Ticket erstellen und ein Flow Collector-Diagnosepaket an den Serviceticket anhängen.

Messen der Dauer des classify_flows-Threads

Eine schnelle Messung der Auswirkungen auf die Leistung, die Sie durchführen können, ist die Untersuchung von sw.log von heute und der Vergleich der nach den "cf-"log-Einträgen aufgelisteten Zahlen vor der Aktivierung der Einstellung mit den Zahlen nach der Anwendung der Einstellung.

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

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

20:44:20 l-flow-f4: classify_flows: flows n-1754296 ns-191100 ne-167913 nq-0 nd-0 nx-0 bis -300 cf-20 ft-122830/783378/949392/14928

20:44:21 l-flow-f2: classify_flows: flows n-1773175 ns-191930 ne-169039 nq-0 nd-0 nx-0 bis -300 cf-20 ft-123055/788507/962264/15431

20:44:21 l-flow-f3: classify_flows: flows n-1750066 ns-189197 ne-165940 nq-0 nd-0 nx-0 bis -300 cf-20 ft-122563/779792/944192/15154

20:44:21 l-flow-f5: classify_flows: flows n-1753899 ns-190477 ne-168004 nq-0 nd-0 nx-0 bis -300 cf-20 ft-122261/783375/946651/15423

20:44:21 l-flow-f1: classify_flows: flows n-1763952 ns-191342 ne-169518 nq-0 nd-0 nx-0 bis -300 cf-20 ft-122782/786822/955997/15175

20:44:21 l-flo-f7: classify_flows: flows n-1757535 ns-188154 ne-166221 nq-0 nd-0 nx-0 bis -300 cf-20 ft-122808/781388/951528/14363

20:44:21 l-flow-f6: classify_flows: flows n-1764211 ns-190964 ne-169013 nq-0 nd-0 nx-0 bis -300 cf-21 ft-122713/784446/954149/16320

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

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

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

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

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

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

Die cf-Einträge stehen für "Classify Flows". Dieser Wert gibt die Anzahl der Sekunden an, die der Thread benötigt hat, um den Abschnitt des Flusscaches zu durchlaufen, für den er verantwortlich ist. In den "Classify Flows"-Threads werden die CSEs auf die Flows angewendet. Wenn diese Zahlen nach der Aktivierung der Funktion steigen, ist dies eine gute Messgröße für die Gesamtauswirkung auf die Leistung.

Es wird ein Anstieg nach dem Hinzufügen dieser erweiterten Intervalleinstellung erwartet. Wenn diese Zahl jedoch auf 60 heranrückt, entfernen Sie die Einstellung, da die Auswirkung zu groß ist.

Ein Anstieg von wenigen Sekunden wäre zu erwarten und wird als vernünftig angesehen.

Motorstatus über Leistungszeitraum

Eine weitere Leistungsmessung, die Sie vor und nach einem Angriff durchführen können, ist der Abschnitt "Performance Period" in der Datei sw.log, der alle 5 Minuten protokolliert wird, um die Auswirkungen der Einstellung auf die Datenflussverarbeitung zu messen. Sie können diese Blöcke auch mit grep suchen. Wenn die Engine überlastet ist, muss diese erweiterte Überprüfung des Einstellungsintervalls deaktiviert werden.

/lancope/var/sw/today/logs/ grep -A3 "Performance Period" sw.log

Achten Sie auf jeden anderen Status als "Motorstatus normal".

Ein Status wie "Engine status Input rate too high" (Modulstatus-Eingaberate zu hoch) würde darauf hinweisen, dass der classify_flows-Thread zu viel CPU verbraucht.

SFI = Static Flow Index

Bedeutet, dass die Classify-Threads ihre Durchläufe durch den Flow-Cache nicht abschließen konnten: Dies steht für "Static Flow Index" und zeigt einen Konflikt in den Classify-Flows-Threads an. Es ist keine Katastrophe für sich, aber es zeigt, dass der Motor beginnt, die Decke zu treffen und dass die Leistung beginnt, sich auf dem aktuellen CF-Niveau zu verschlechtern.

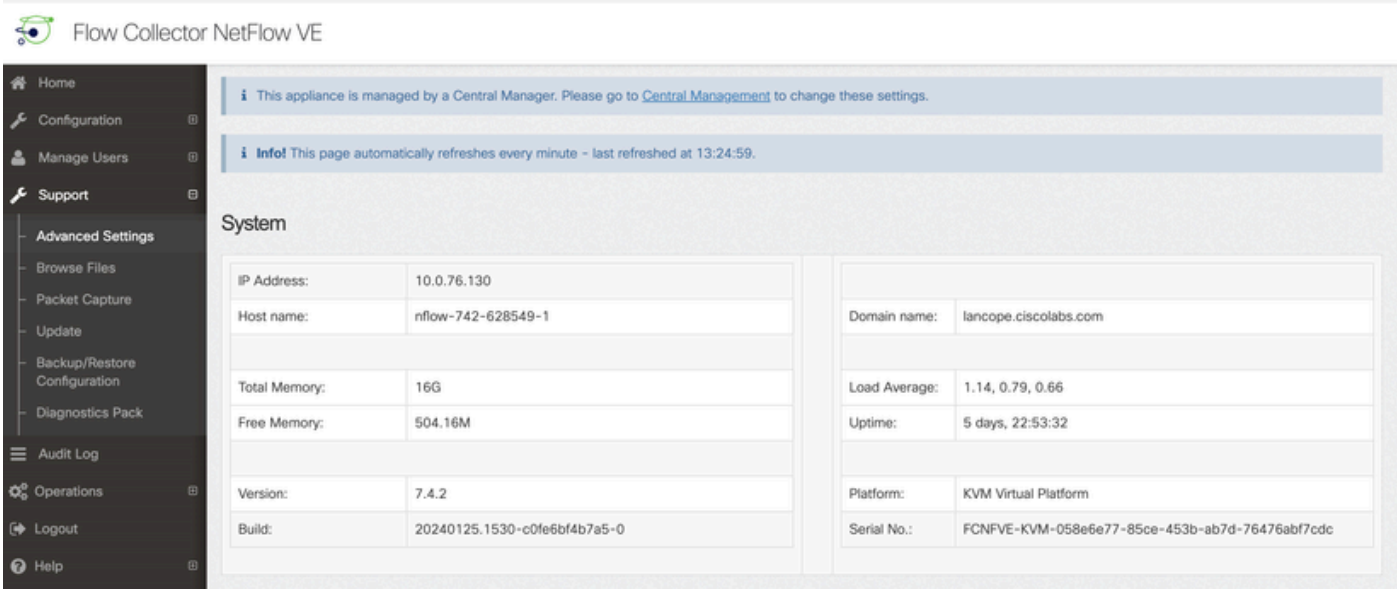
sw.log:16:09:49 I-flo-f1: classify_flows: sfi:base(8388608) (10522745 -> 11014427)
max(16777215) cod(1) (491681/8388608)---------->(5 %)
sw.log:16:09:49 I-flow-f3: classify_flows: sfi:base(25165824) (27269277 -> 27754304)
max(33554431) cod(1) (485026/8388608)---------->(5 %)
sw.log:16:09:49 I-flo-f4: classify_flows: sfi:base(33554432) (35652656 -> 36138422)
max(41943039) cod(1) (485765/8388608)---------->(5 %)
sw.log:16:09:49 I-flow-f2: classify_flows: sfi:base(16777216) (18985626 -> 19499308)
max(25165823) cod(1) (513681/8388608)---------->(6 %)
sw.log:16:09:54 I-flo-f0: classify_flows: sfi:base(0) (1786480 -> 421161) max(8388607) cod(1)
(7023288/8388608)---------->(83 %)
sw.log:16:10:49 I-flo-f0: classify_flows: sfi:base(0) (421161 -> 1402189) max(8388607) cod(0)
(981027/8388608)---------->(11 %)
sw.log:16:10:49 I-flow-f2: classify_flows: sfi:base(16777216) (19499308 -> 17522620)
max(25165823) cod(0) (6411919/8388608)---------->(76 %)
sw.log:16:10:49 I-flow-f1: classify_flows: sfi:base(8388608) (11014427 -> 8976309)
max(16777215) cod(0) (6350489/8388608)---------->(75 %)
sw.log:16:10:49 I-flow-f3: classify_flows: sfi:base(25165824) (27754304 -> 25702968)
max(33554431) cod(0) (6337271/8388608)---------->(75 %)
sw.log:16:10:49 I-flo-f7: classify_flows: sfi:base(58720256) (58848913 -> 59630528)
max(67108863) cod(0) (781614/8388608)---------->(9 %)
sw.log:16:10:49 I-flo-f4: classify_flows: sfi:base(33554432) (36138422 -> 34064015)
max(41943039) cod(1) (6314200/8388608)---------->(75 %)
sw.log:16:10:49 I-flo-f5: classify_flows: sfi:base(41943040) (43310891 -> 44059251)

max(50331647) cod(1) (748359/8388608)---------->(8 %)
sw.log:16:10:49 l-flow-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-flow-f6: classify_flows: sfi:base(50331648) (52444661 -> 50483491)
max(58720255) cod(1) (6427437/8388608)---------->(76 %)
sw.log:16:11:49 l-flow-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-flow-f2: classify_flows: sfi:base(16777216) (17522620 -> 18202249)
max(25165823) cod(1) (679628/8388608)---------->(8 %)

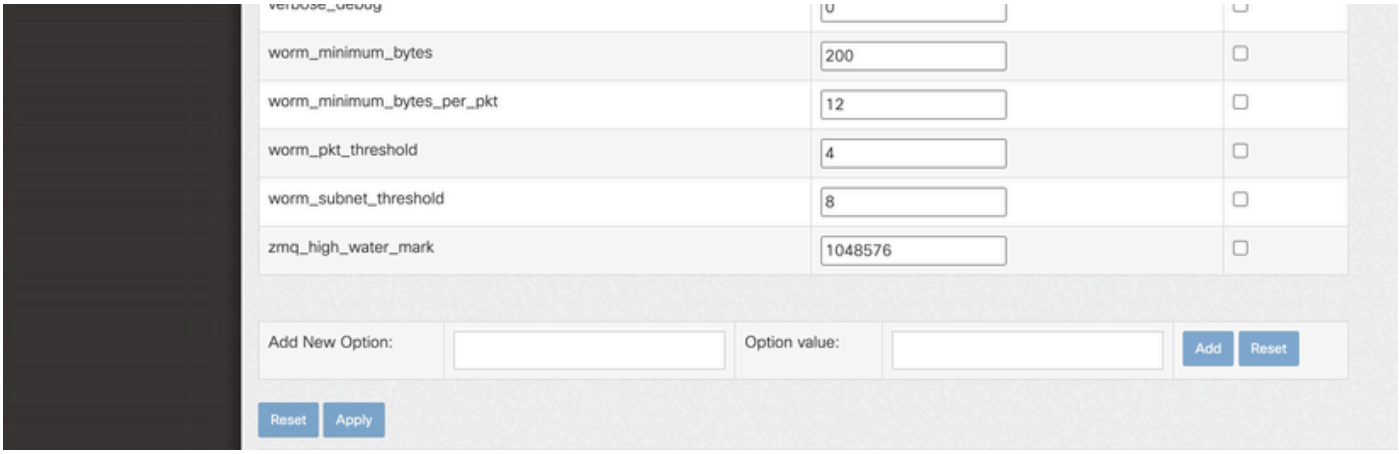
Konfiguration

Öffnen Sie einen Webbrowser, und navigieren Sie direkt zur IP-Adresse der Flow Collector Appliance. Melden Sie sich als lokaler Administrator an.

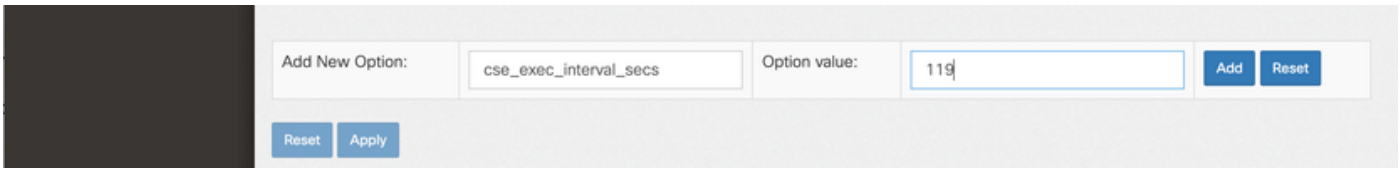
Navigieren Sie zu Support -> Erweiterte Einstellungen



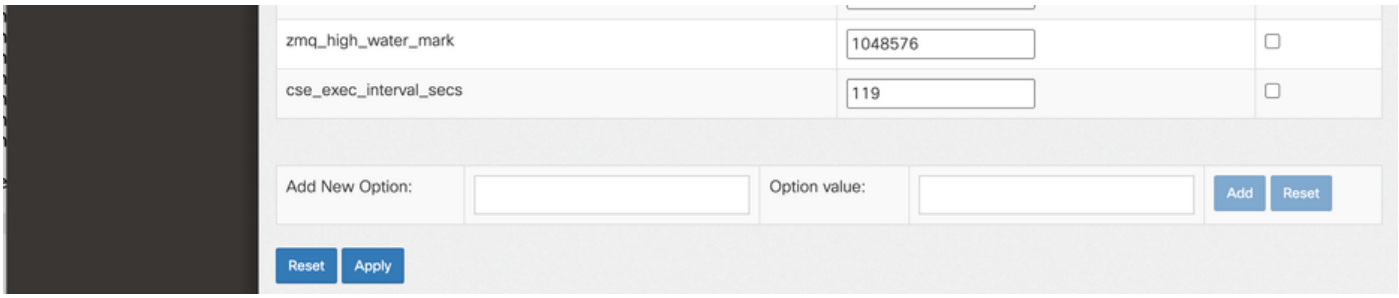
Scrollen Sie im Bildschirm "Erweiterte Einstellungen" nach unten, um das Konfigurationsfeld "Neue Option hinzufügen" am unteren Rand der Liste anzuzeigen.



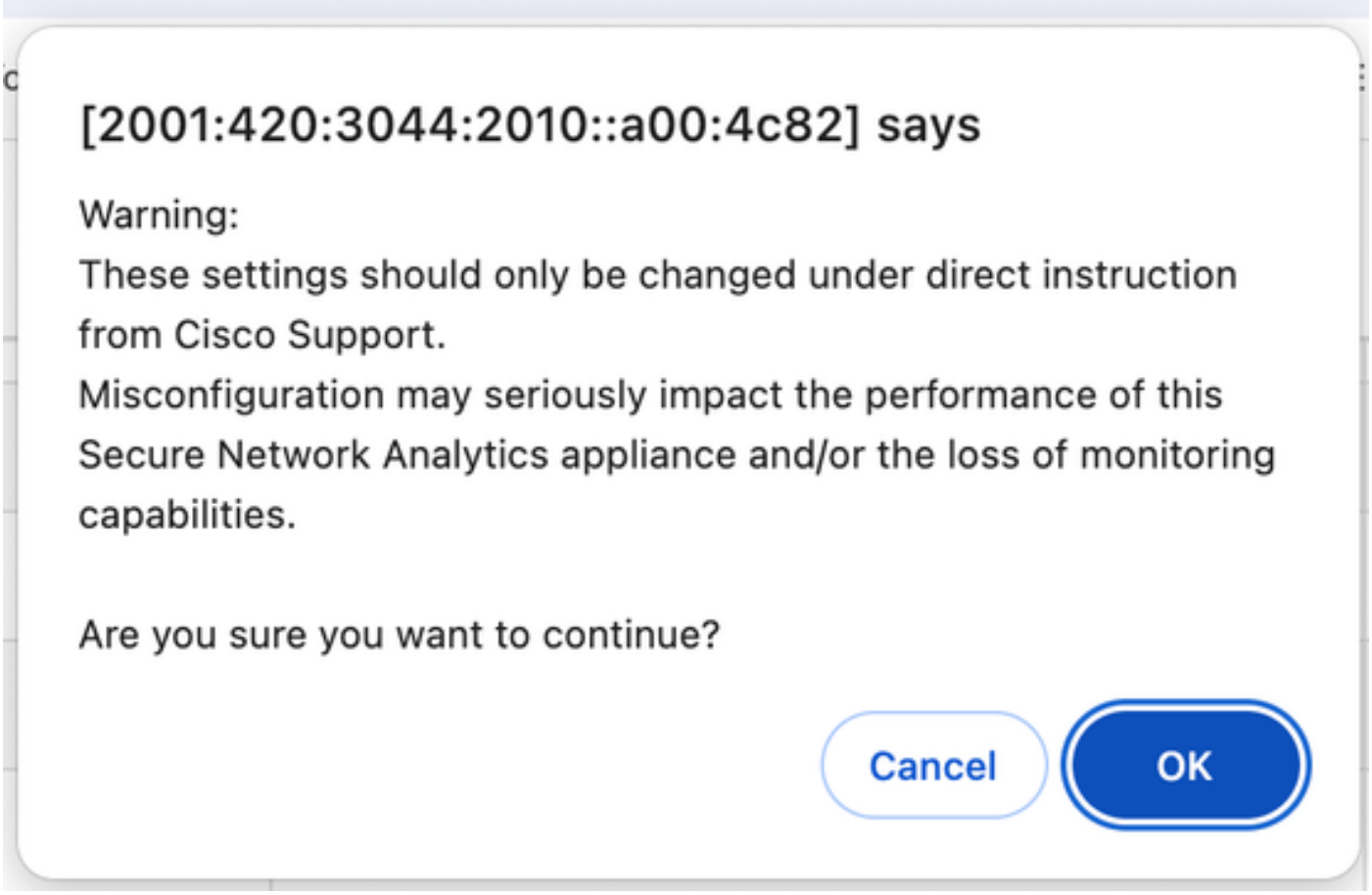
Geben Sie im Bearbeitungsfeld Neue Option hinzufügen: cse_exec_interval_secs und im Optionswert: Bearbeitungsfeld 119 ein. Durch Bearbeiten dieser Felder wird die Schaltfläche Hinzufügen aktiviert. Drücken Sie die Schaltfläche Hinzufügen, nachdem Sie case_exec_interval_secs in das Feld Neue Option hinzufügen: edit und 119 in das Feld Optionswert: edit eingegeben haben.



Die Bearbeitungsfelder Neue Option hinzufügen: und Option: löschen sich, um einen weiteren Eintrag vorzubereiten, falls mehrere neue Erweiterte Einstellungen eingegeben werden sollen. Die neu hinzugefügten erweiterten Einstellungen werden beim Hinzufügen am Ende der Liste übernommen. Dadurch hat der Benutzer die Möglichkeit, den Eintrag zu überprüfen. Die genaue Schreibweise der erweiterten Einstellung ist ebenso wichtig wie der Fall. Alle erweiterten Einstellungen werden in Kleinbuchstaben angezeigt.



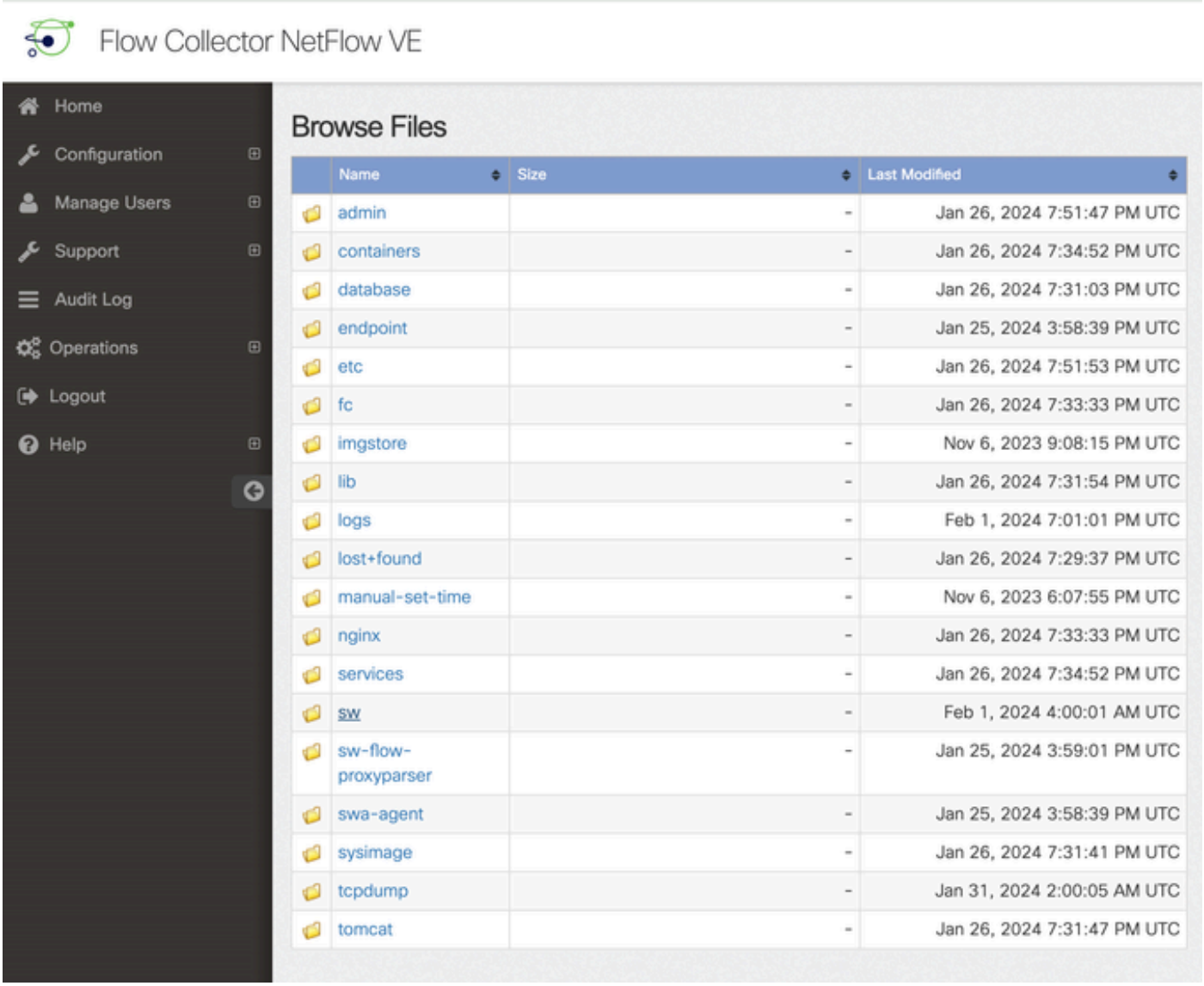
Nachdem Sie die erweiterten Einstellungen korrekt eingegeben haben, drücken Sie die Schaltfläche Anwenden. Beachten Sie, dass manchmal die Schaltfläche Apply nicht aktiviert ist. Um sie zu aktivieren, klicken Sie in das Feld Neue Option hinzufügen: bearbeiten, und dann wird die Schaltfläche Anwenden aktiviert. Wenn dieses Popup angezeigt wird, drücken Sie OK, um die neue erweiterte Einstellung und den neuen Wert zu senden.



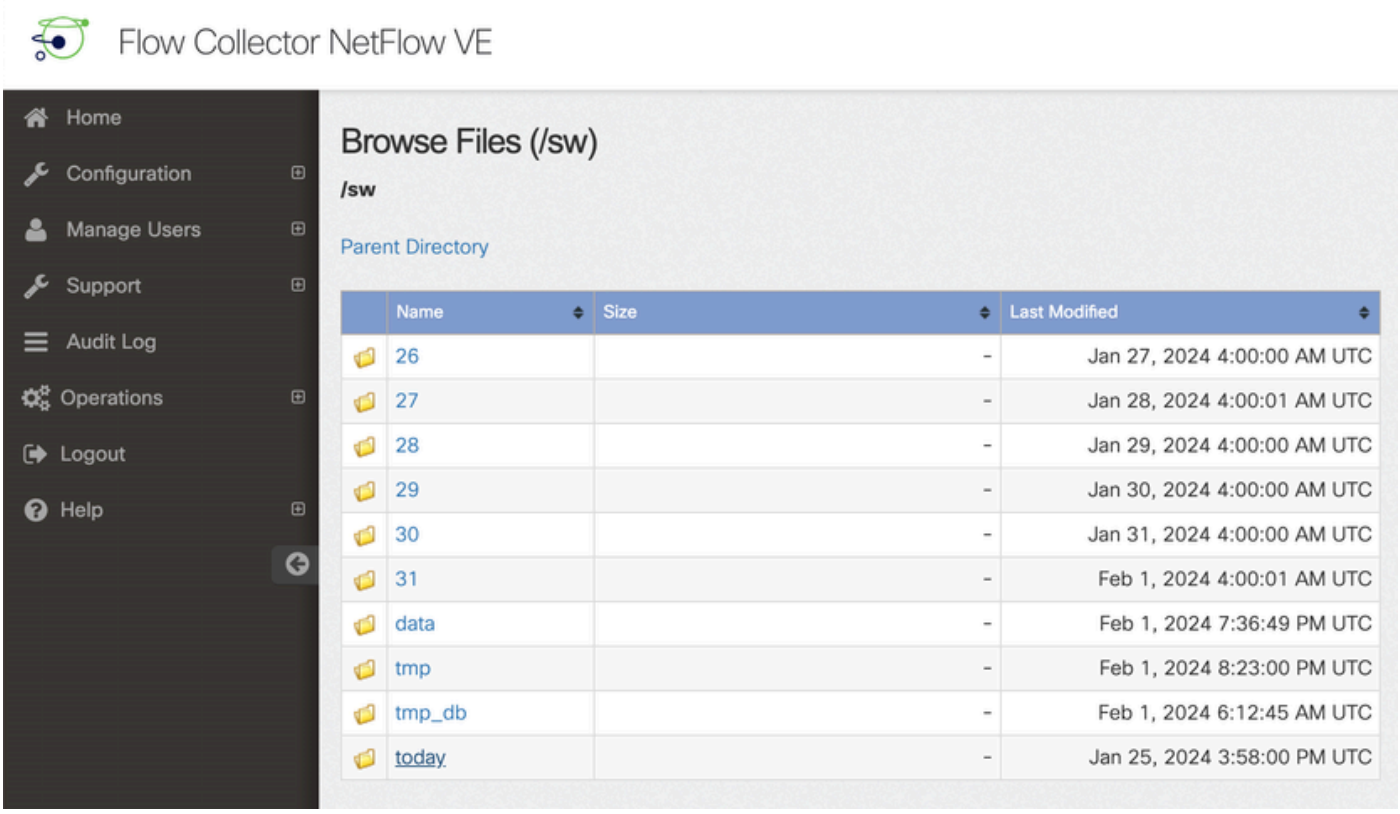
Bestätigen der Änderung

Diese abschließende Validierung ist die wichtigste. Klicken Sie erneut auf das Menü Support und wählen Sie Dateien durchsuchen.

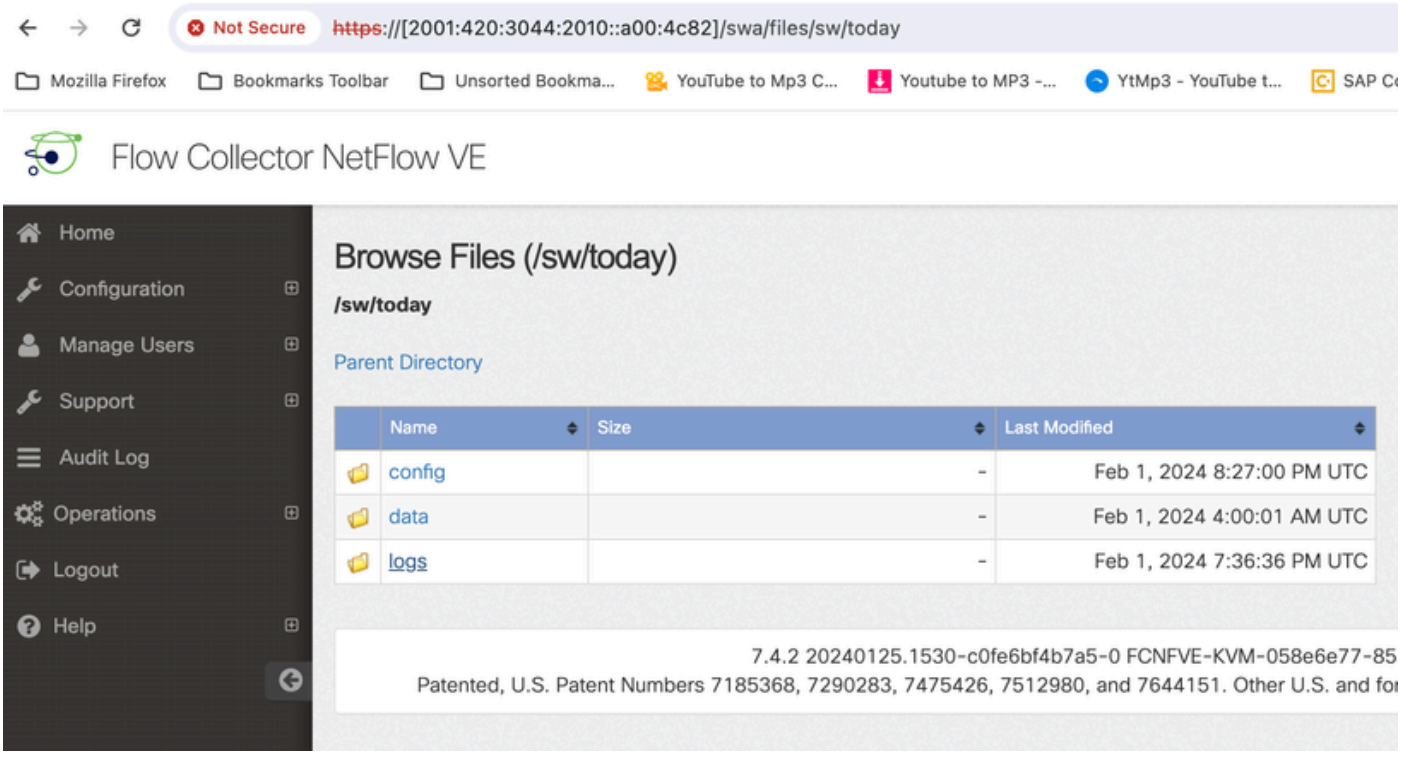
Dadurch gelangen Sie zum Dateisystem auf der FC. Klicken Sie auf sw.



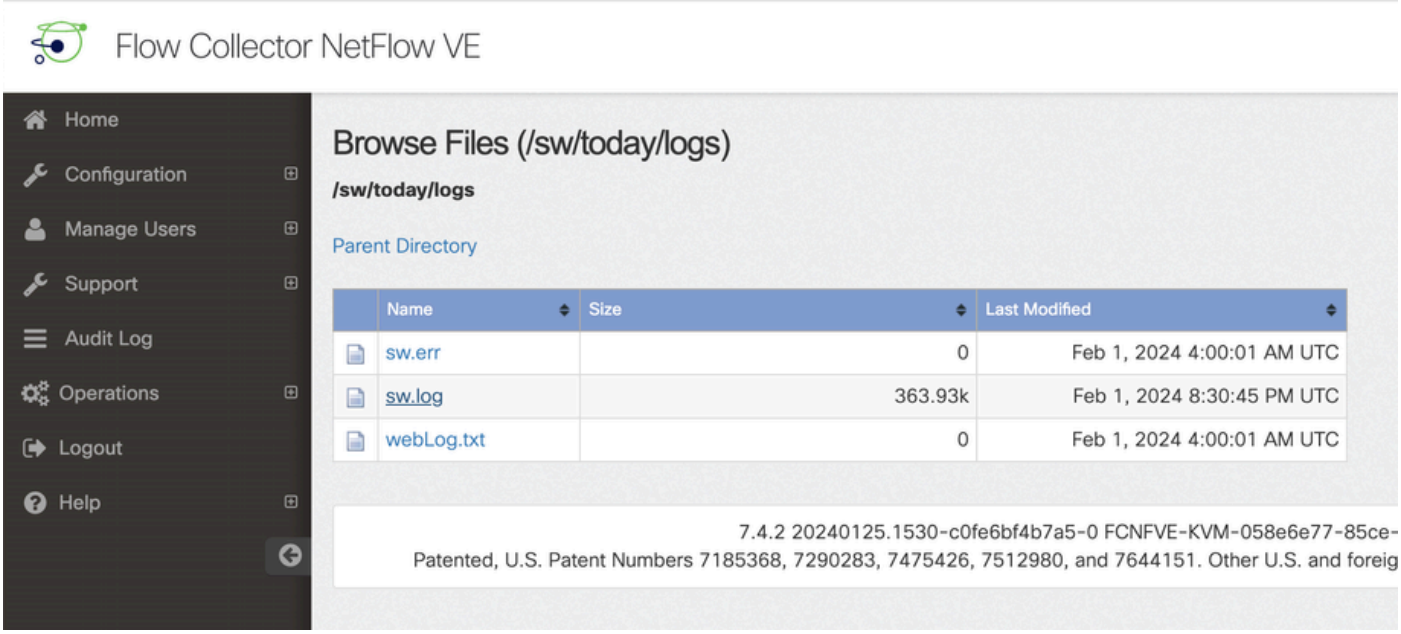
Klicken Sie heute auf



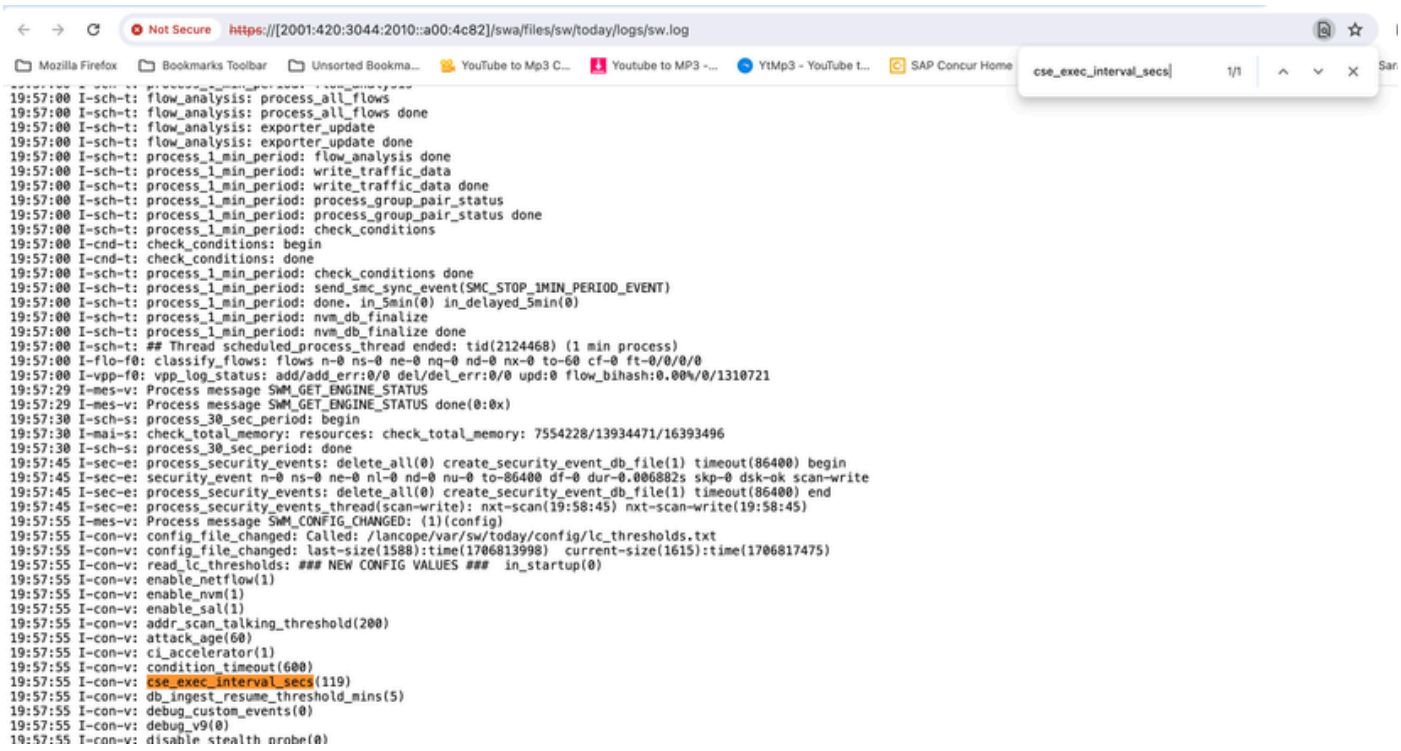
Klicken Sie auf Protokolle.



Klicken Sie auf sw.log



Führen Sie eine Suche auf der Browserseite durch. Geben Sie cse_exec_interval_secs in das Suchfeld ein, um nach der erweiterten Einstellung zu suchen.



Akzeptierte erweiterte Einstellungen werden wie im Screenshot gezeigt aufgelistet.

Die nicht akzeptierten werden als "nicht Teil der Eingabekonfiguration" angezeigt, in diesem Fall aufgrund einer falschen Schreibweise des Benutzers. Aus diesem Grund ist es wichtig, das Protokoll zu überprüfen, nachdem Sie diese Konfigurationsänderungen vorgenommen haben.

```
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)
```

Herzlichen Glückwunsch!

Sie haben soeben eine neue erweiterte Einstellung eingegeben und ihre Annahme durch die Engine validiert.

Jetzt ist die Funktion so aktiviert, dass die CSE-Logik für die Flows ungefähr alle 2 Minuten ausgeführt wird, nachdem der Flow das early_check_age erreicht hat, das standardmäßig 160 Sekunden beträgt.

Wenn die CSE-Regeln die Akkumulation von Bytezahlen über einen längeren Zeitraum beinhalten, verbessert diese Funktion die zeitliche Steuerung, zu der die CSEs bei Flows auslösen, die den von Ihnen definierten Kriterien entsprechen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.