تكوين سلوك إطلاق حدث الأمان المخصص لمحرك مجمع التدفق المتقدم

المحتويات

المقدمة

يصف هذا المستند إعدادات متقدمة لمجمع التدفق يمكن أن تغير الطريقة التي يقوم بها مجمع تدفق SNA بتشغيل أحداث الأمان المخصصة (CSEs).

الخلفية

يحدد الإعداد المتقدم لمجمع التدفق early_check_age، بالإضافة إلى الإعداد المتقدم لمجمع التدفق CSE_EXEC_interval_secondsالجديد الطريقة التي يتم بها تشغيل أحداث الأمان المخصص بواسطة محرك مجمع التدفق. مجمع التدفق هو أول جهاز في بنية نظام SNA لرؤية التدفق على الشبكة، وبالتالي فإن محرك مجمع التدفق مسؤول عن مراقبة خصائص التدفق (التدفقات) أثناء وجوده في ذاكرة التخزين المؤقت للتدفق، وتحديد ما إذا كان التدفق يفي بالمعايير التي تم تكوينها لحدث أمان مخصص معين. لا تعمل هذه الإعدادات المتقدمة لمجمع التدفق على تغيير خصائص الإطلاق لأي من أحداث أمان المركز المضمنة.

سلوك مجمع التدفق الافتراضي

بشكل افتراضي، يتم تكوين الإعداد المتقدم لمجمع التدفق early_check_age على 160 ثانية. هذا يعني أن محرك مجمع التدفق ينتظر 160 ثانية كحد أدنى في تدفق قبل أن يتحقق مما إذا كان هذا التدفق يطابق حدث أمان مخصص تم تكوينه. بشكل افتراضي، لا يتم إجراء هذا التحقق مرة أخرى حتى بعد انتهاء التدفق.

تم إختيار قيمة الفحص المبكر هذه التي تبلغ 160 ثانية تحديدا لأنه في حالة إستخدام أفضل الممارسات، يجب تكوين مصدري بيانات تتبع الاستخدام لإرسال بيانات تتبع الاستخدام كل 60 ثانية. تتيح هذه القيمة الافتراضية الوقت الكافي في بيئة نموذجية

.نيعم قفدت/ةثداحم يبناج الكب ةقلعتملا قفدتلا تامولعم ىلع عالطالل قفدتلا عمجمل كلذو .ةمدقتملا تادادعإلا ةمئاق يف اقبسم early_check_age فيرعت متي مل ،ببسلا اذهلو الوأ ةسدنهلا/معدلا ةراشتسإ نودب ةميقلا هذه رييغتب موقت الأ بجيو ،ميمصتلا بسح .صئاصخ رابتعالا يف ذخألا دنع يباجيإ لكشب يلوألا ميمصتلا اذه لمعي ال ،كلذ عمو صصخملا نامألا ثدح نيوكتب ةنرتقم ءيشلا ضعب ةئداه نوكت يتلاو ةليوطلا قفدتلا ل ةمدقتملا دادعإلا ةملعم ءاشنإ مت ببسلا اذهلو .مزحلا وأ تيابلا ددع مكارت نمضتي يذلا cse_exec_interval_seconds .

مدقتملا دادعإلا cse_exec_interval_seconds

7.4.2 يف رفوتملا cse_exec_interval_seconds قفدتلا عمجمل مدقتملا دادعإلا ةفاضإ حيتت نيزختلا ةركاذ يف ةدوجوملا تاقفدتلا نم يرود لكشب ققحتلل كرحملا هيجوت ةيناكمإ اذه نوكيو .اهنيوكت مت يتلا صصخملا نامألا ثادحأ لباقم هب ةصاخلا قفدتلل تقؤملا قفدت قباطتي ال ثيح ،ةليوطلا تاقفدتلا ةلاح يف صاخ لكشب اديفم مدقتملا دادعإلا هنكلو ،Early_CHECK_AGE نم ةيناث 160 يضارتفالا دادعإلا يف CSE رييامع عم نيعم نامألا ثدح" ليغشت متي نل ،مدقتملا دادعإلا اذه نودب .قفدتلا يف اقحال دحال كلذ زواجتي صصخملا" الإ دعب انا ءاهتنا قفدتلا ،قوو ثدحي كلذ انايحأ دعب مايأ.

ءادألا تاريثأت

ةايح يف رثكأ تارم تاقفدتلا نم اقحت اذه يتمزلا لصافلل CSE رييامع ذيفنت بلطتي كدشرت .ةيزكرملا ةجلاعملا ةدحو نم ديزملا ةيضارتفالا ميقلا هفرعت ام نم قفدتلا ساسأ ديدحتل قفدتلا عمجم كرحم ىلع sw.log فلم تايوتحم نم ققحتلا لالخ نم تاداشرإلا دادعإلا اذه نيكمت يف رظنت تنك اذإ .cse_exec_interval_seconds ةملعملا نيكمت لبق ءادأ اذهل ريضحتلا يف كيدل قفدتلا عمجم ةيامح ديكأت يف TAC دعاسي نأ ديرتو مدقتملا ب قفدتلا عمجم صيخشت ةمزح قافراو معد ةلاح حتف لالخ نم كلذب مايقلا نكمي ،رييغتلا SR.

قايس ةدم رشؤم طبارت CLASSIFICATION_FLOW

مويلا نم sw.log يف قيقحتلا وهو هب مايقلا كنكمي ءادألا ريثأتل عيرس دحاو قايس كانه قيبطت دعب ماقرألاب دادعإلا طيشنت لبق "cf لجس تالاخدإ دعب ةجردملا ماقرألا ةنراقمو دادعإلا.

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

20:43:21 I-Flo-F0: فينصت التدفقات: التدفقات n-1744317 NS-178613 NE-188095 NQ-0 nd-nx-0 to-300 cf-21ft-126473/792802/940383/14216

20:44:20 I-Flo-F4: فينصت التدفقات: التدفقات n-1754296 NS-191100 NE-167913 NQ-0 nd-nx-0 to-300 cf-20ft-122830/783378/94932/14928

20:44:21 I-Flo-F2: فينصت التدفقات: التدفقات n-1773175 ns-191930 ne-169039 nq-0 nd-nx-0 to-300 cf-20 ft-123055/788507/96264/15431

20:44:21 I-FLO-F3: فينصت_التدفقات: التدفقات n-1750066 ns-189197 ne-165940 nq-0 nd-nx-0 to-300 cf-20 ft-122563/779792/94192/15154

20:44:21 i-flo-f5: فينصت_flow: التدفقات n-1753899 ns-190477 ne-168004 nq-0 nd-nx-0 to-300 cf-20 ft-12261/783375/946651/15423

20:44:21 I-Flo-F1: فينصت التدفقات: التدفقات n-1763952 ns-191342 ne-169518 nq-0 nd-nx-0 to-300 cf-20 ft-122782/786822/95997/15175

20:44:21 I-Flo-F7: فينصت التدفقات: التدفقات n-1757535 ns-188154 ne-166221 nq-0 nd-nx-0 to-300 cf-20 ft-122808/781388/951528/14363

20:44:21 I-Flo-F6: فينصت التدفقات: التدفقات n-1764211 ns-190964 ne-169013 nq-0 nd-nx-0 to-300 cf-21 ft-122713/78446/954149/16320

20:44:21 I-Flo-F0: فينصت التدفقات: التدفقات n-1764197 ns-189780 ne-168784 nq-0 nd-nx-0 to-300 cf-21 ft-123290/787327/952186/14352

20:45:22 I-Flo-F4: فينصت التدفقات: التدفقات n-1780277 ns-177512 ne-149843 nq-0 nd-nx-0 to-300 cf-21 ft-129553/766777/964933/14864

20:45:22 i-flo-f2: فينصت_flow: التدفقات n-1789285 ns-175763 ne-155809 nq-0 nd-nx-0 to-300 cf-21 ft-129685/772482/976850/15289

20:45:22 i-flo-f3: فينصت_flow: التدفقات n-1774883 ns-17085 ne-149715 nq-0 nd-nx-0 to-300 cf-22 ft-129067/764272/962000/15090

20:45:22 i-flo-f5: فينصت_flow: التدفقات n-1775998 ns-176898 ne-150682 nq-0 nd-nx-0 to-300 cf-22 ft-128835/768374/963353/15347

20:45:22 I-Flo-F1: فينصت التدفقات: التدفقات n-1786441 ns-175776 ne-151846 nq-0 nd-nx-0 to-300 cf-22 ft-129255/770212/970360/15129

تمثل إدخالات CF "فينصت التدفقات". يمثل هذا عدد الثواني التي إستغرقها مؤشر الترابط لتمريره عبر قسم ذاكرة التخزين المؤقت للتدفق المسؤول عنه. إنه في مؤشرات الترابط التي تطبق على CSEs حيث يتم تطبيق "فينصت التدفقات" ترابط التدفقات. إذا رأيت أن هذه الأرقام تبدأ بعد تمكين الميزة، ذلك قياس جيد للتأثير الكلي على الأداء.

هذا تقارب إذا لكن، وهذا المتقدم الزمني الفاصل إعداد إضافة بعد إرتفاع حدوث المتوقع من المتوقع من قليل عدد زيادة المتوقع ومن .جدا كبير التأثير ألا نظرا إعداد الإزالة بقيمة 60، من الرقم الثواني، وتعتبر هذه الزيادة معقولة.

حالة المحرك عبر فترة الأداء

فلم في "الأداء فترة" أقسام إلى النظر هو به القيام يمكنك "بعد" قبل قياس آخر أداء يمكنك .التدفق معالجة على الإعداد تأثير قياس قيم 5 كل تسجيله يتم الذي sw.log أيضا GREP باستخدام لتلك هذه عن البحث للتحقق يجب تطبيق ،"المحرك" زواجات حالة في الفاصل الزمني للإعداد المتقدم هذا.

/lancope/var/sw/today/log/grep -A3 "فترة الأداء" sw.log

إخطار بأية حالة غير حالة المحرك العادية".

تشير حالة مثل "معدل إدخال حالة المرحك أعلى من المزالم" إلى أن مؤشر ارتباط CLASSIFICATION_FLOW يستهلك الكثير من وحدة المعالجة المركزية (CPU).

SFI - فهرس تدفق ثابت

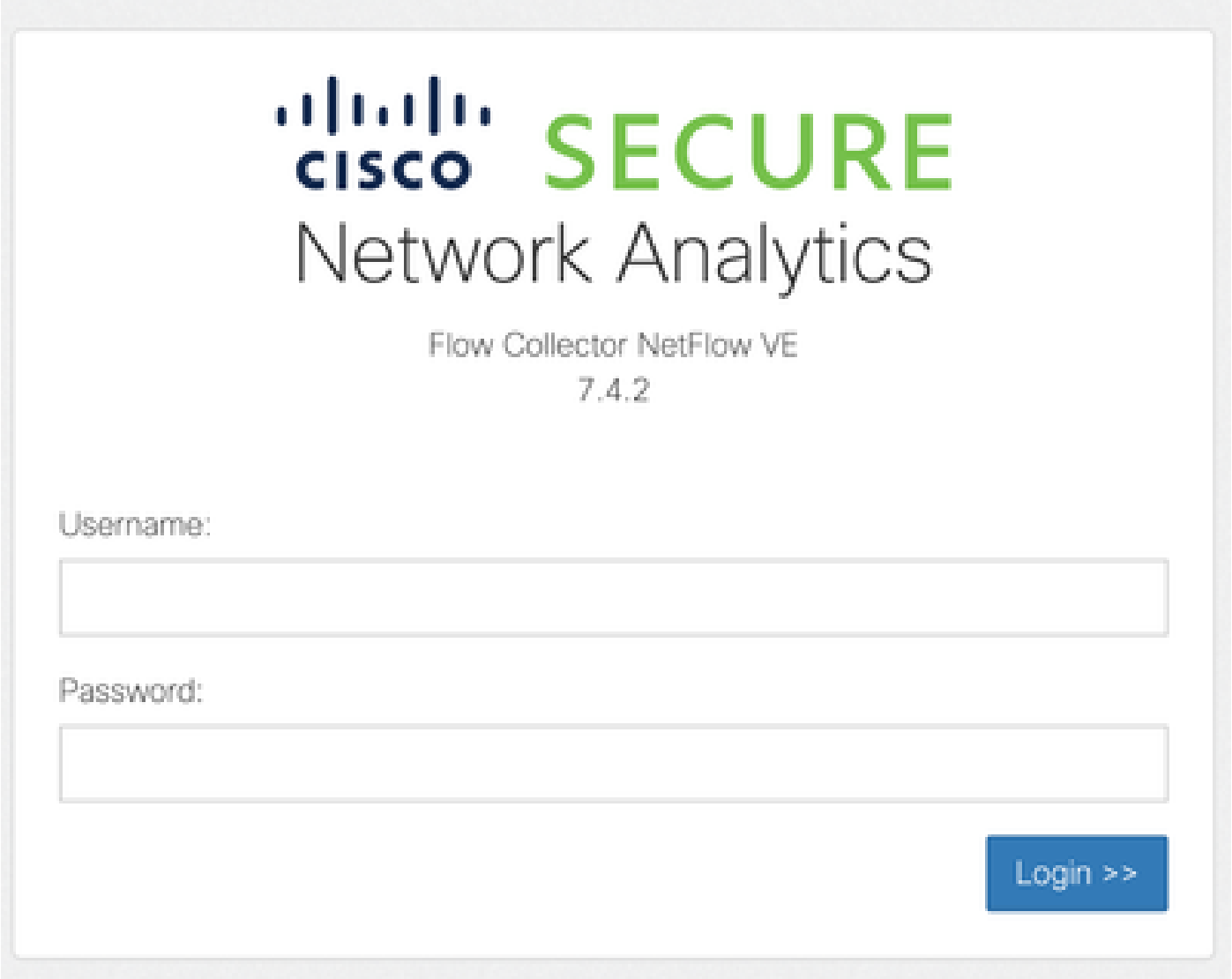
يعني أن مؤشرات الترابط المصنفة لم تتمكن من إكمال تمريرها عبر ذاكرة التخزين المؤقت للتدفق: وهي تمثل "مؤشر التدفق الثابت" وتشير إلى وجود تعارض في مؤشرات تصنيف التدفقات. وهي ليست كارثة بحد ذاتها، لكنها تدل على أن المرحك بدأ في الوصول إلى سقف أو أن الأداء بدأ في الانخفاض عند مستويات التكييف الكهرومغناطيسي الحالية.

sw.log:16:09:49 i-flo-f1: تصنيف_flow: sfi:base(8388608) (10522745 -> 1101427) max(1677215) cod(1) (491681/8388608)—>(5٪)
sw.log:16:09:49 I-flo-f3: تصنيف_flow: sfi:base(25165824) (27269277 -> 27754304) max(3355431) cod(1) (485026/8388608)—>(5٪)
sw.log:16:09:49 i-flo-f4: تصنيف_flow: sfi:base(33554432) (35652656 -> 36138422) max(41943039) cod(1) (485765/8388608)—>(5٪)
sw.log:16:09:49 i-flo-f2: تصنيف_flow: sfi:base(16777216) (18985626 -> 1949308) max(25165823) cod(1) (513681/8388608)—>(6٪)
sw.log:16:09:54 i-flo-f0: تصنيف_flow: sfi:base(0) (1786480 -> 421161) max(8388607) cod(1) (7023288/8388608)—>(83٪)
sw.log:16:10:49 i-flo-f0: تصنيف_flow: sfi:base(0) (421161 -> 1402189) max(8388607) cod(0) (981027/8388608)—>(11٪)
sw.log:16:10:49 i-flo-f2: تصنيف_flow: sfi:base(16777216) (19499308 -> 17522620) max(25165823) cod(0) (6411919/8388608)—>(76٪)
sw.log:16:10:49 i-flo-f1: تصنيف_flow: sfi:base(8388608) (11014427 -> 8976309) max(1677215) cod(0) (6350489/8388608)—>(75٪)
sw.log:16:10:49 i-flo-f3: تصنيف_flow: sfi:base(25165824) (2754304 -> 25702968) max(33554431) cod(0) (6337271/8388608)—>(75٪)
sw.log:16:10:49 i-flo-f7: تصنيف_flow: sfi:base(58720256) (58848913 -> 59630528) max(67108863) cod(0) (781614/8388608)—>(9٪)
sw.log:16:10:49 i-flo-f4: تصنيف_flow: sfi:base(33554432) (36138422 -> 34064015) max(41943039) cod(1) (6314200/8388608)—>(75٪)
sw.log:16:10:49 i-flo-f5: تصنيف_flow: sfi:base(41943040) (4310891 -> 44059251) max(50331647) cod(1) (748359/8388608)—>(8٪)
sw.log:16:10:49 i-flo-f6: تصنيف_flow: sfi:base(50331648) (51714170 -> 5244661) max(58720255) cod(1) (730490/8388608)—>(8٪)
sw.log:16:11:49 i-flo-f5: تصنيف_flow: sfi:base(41943040) (44059251 -> 4212104) max(50331647) cod(0) (6450460/8388608)—>(76٪)
sw.log:16:11:49 i-flo-f0: تصنيف_flow: sfi:base(0) (1402189 -> 2373792) max(8388607) cod(1) (971602/8388608)—>(11٪)
sw.log:16:11:49 i-flo-f6: تصنيف_flow: sfi:base(50331648) (5244661 -> 50483491) max(58720255) cod(1) (6427437/8388608)—>(76٪)
sw.log:16:11:49 i-flo-f3: تصنيف_flow: sfi:base(25165824) (25702968 -> 26385879) max(3355431) cod(1) (682910/8388608)—>(8٪)
sw.log:16:11:49 i-flo-f1: تصنيف_flow: sfi:base(8388608) (8976309 -> 9662167) max(1677215)

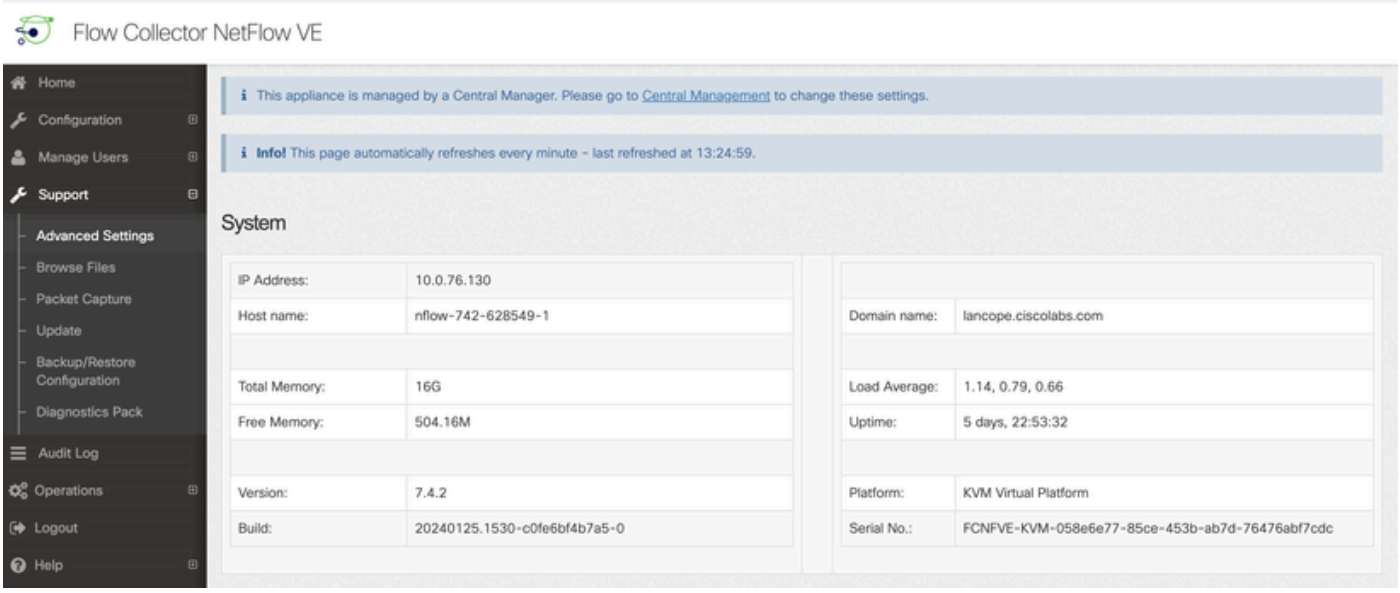
cod(1) (685857/8388608)—(8٪)
sw.log:16:11:49 i-flo-f4: تصنيف_flow: sfi:base(33554432) (34064015 -> 34742593)
max(41943039) cod(1) (678577/8388608)—>(8٪)
sw.log:16:11:50 i-flo-f7: تصنيف_flow: sfi:base(58720256) (59630528 -> 60298366)
max(67108863) cod(1) (667837/8388608)—>(7٪)
sw.log:16:11:50 i-flo-f2: تصنيف_flow: sfi:base(16777216) (17522620 -> 18202249)
max(25165823) cod(1) (679628/8388608)—>(8٪)

تهيئة

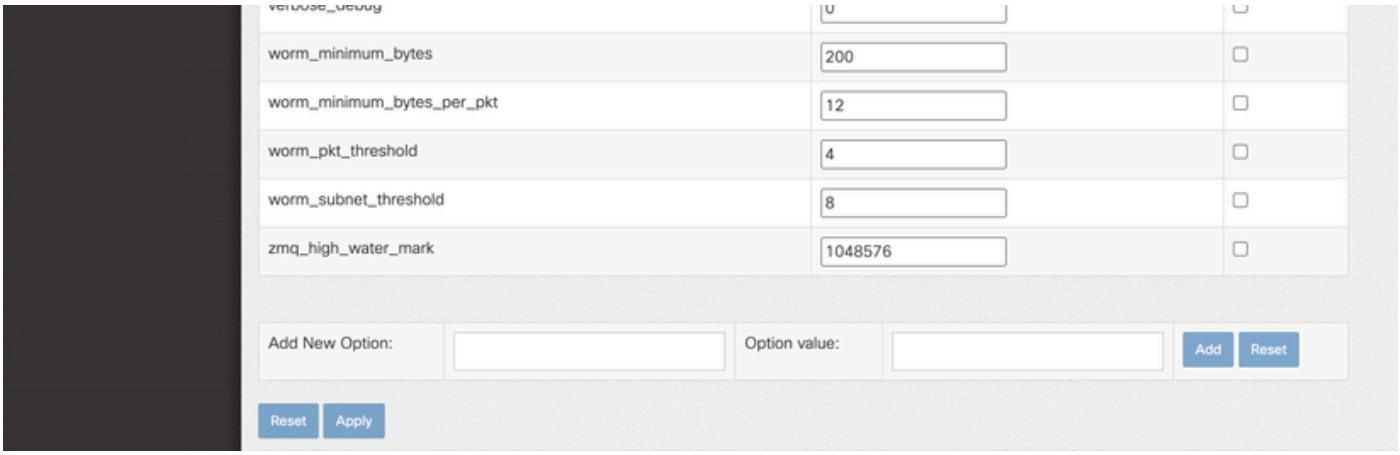
افتح مستعرض ويب وانتقل إلى IP الخاص بجهاز مجمع التدفق مباشرة. قم بتسجيل الدخول كمستخدم مسؤول محلي.



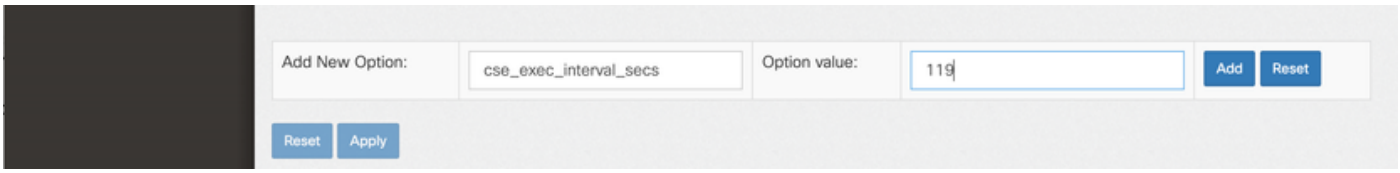
انتقل إلى الدعم -> إعدادات متقدمة



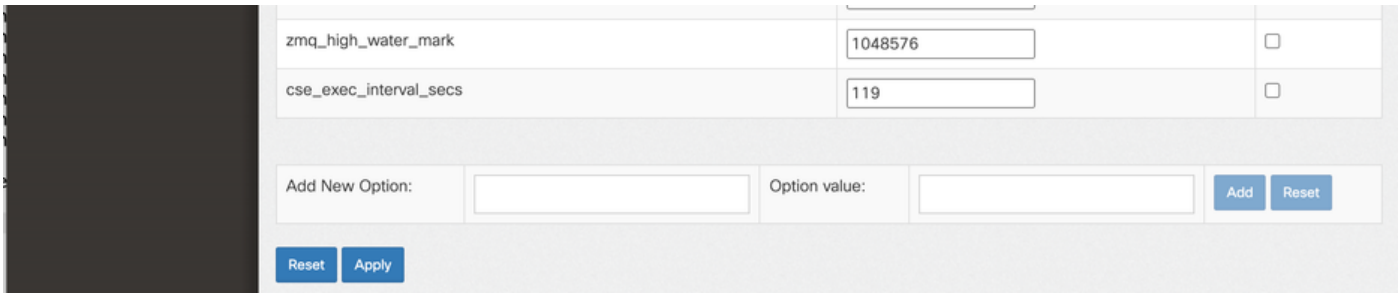
قم بالتمرير لأسفل إلى شاشة "الإعداد المتقدم" لكشف مربع تكوين "إضافة خيار جديد" الموجود أسفل القائمة



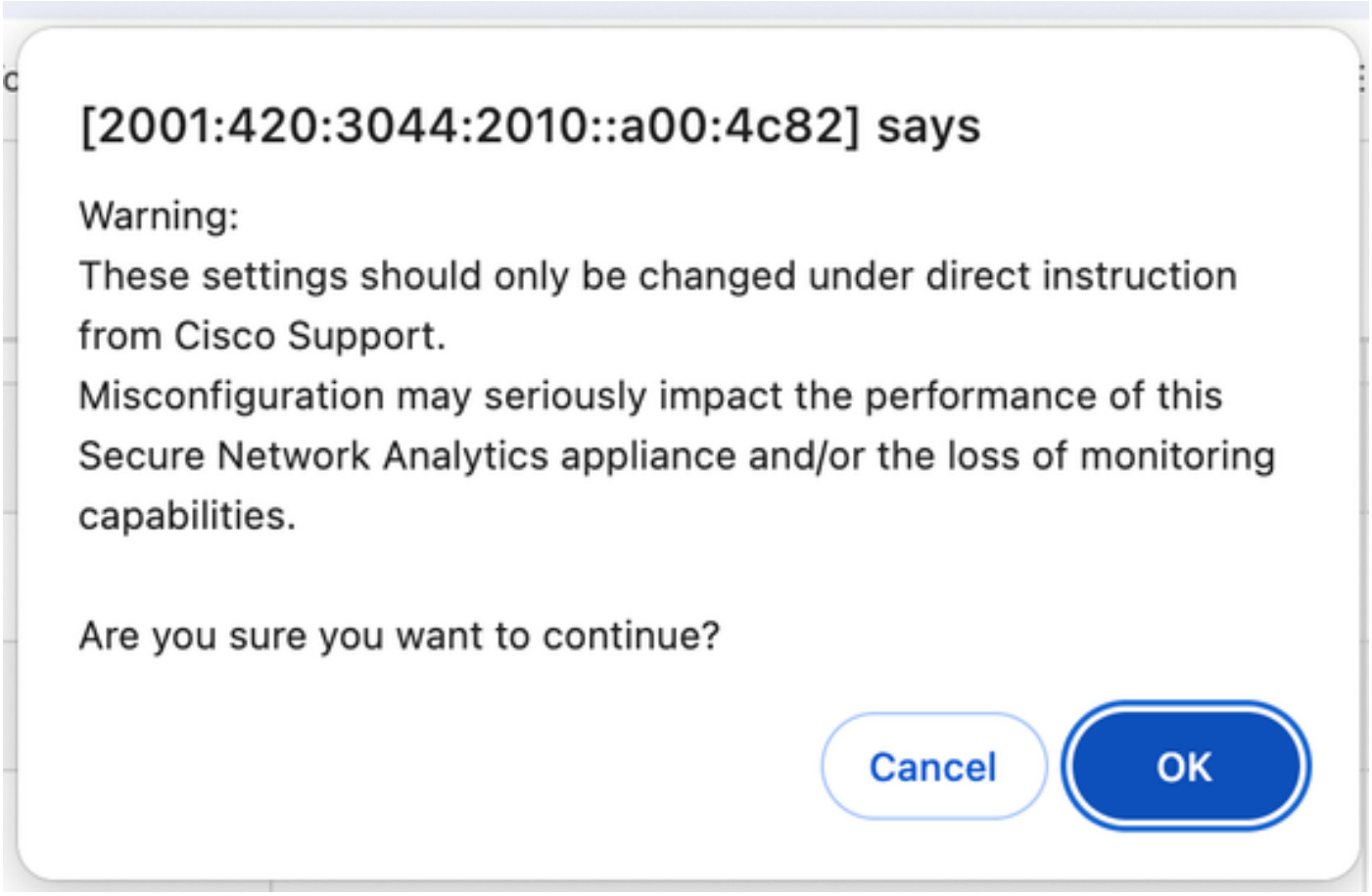
في الخيار إضافة جديد: قم بتحرير المربع إدخال cse_exec_interval_seconds وفي قيمة الخيار: قم بتحرير المربع أدخل 119. يتيح تحرير هذه المربعات الزر إضافة. اضغط زر إضافة بعد إدخال cse_exec_interval_seconds في إضافة خيار جديد: مربع التحرير و 119 في قيمة الخيار: مربع التحرير.



الخيار إضافة جديد: وقيمة الخيار: تحرير المربعات مسح في التحضير لإدخال آخر في حالة إدخال العديد من الإعدادات المتقدمة الجديدة. يتم ربط الإعدادات المتقدمة التي تمت إضافتها حديثا في أسفل القائمة كما تتم إضافتها. هذا يمنح المستخدم فرصة لتفتيش الإدخال. يعد التدقيق الإملائي للإعداد المتقدم مهما بالإضافة إلى الحالة. كل الإعدادات المتقدمة في حروف صغيرة.



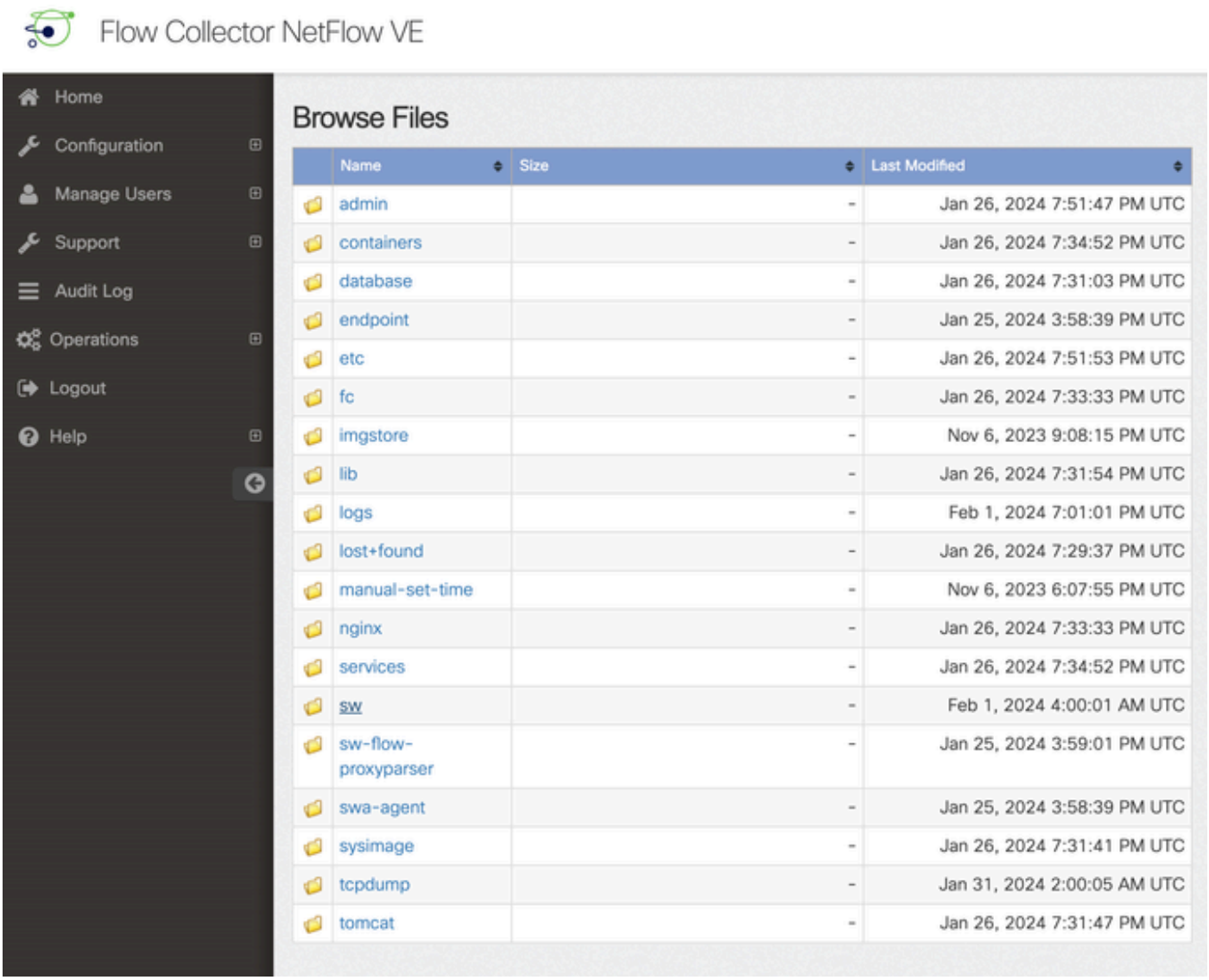
الآن بعد أن تم إدخال الإعداد المتقدم بشكل صحيح، اضغط على الزر تطبيق. لاحظ أنه في بعض الأحيان لا يتم تمكين الزر تطبيق. لتمكينها، انقر في مربع إضافة خيار جديد: تحرير ثم يصبح زر تطبيق متاحا للنقر. عند تقديم هذا الإطار المنبثق، اضغط زر موافق للإرسال الإعداد المتقدم الجديد والقيمة.



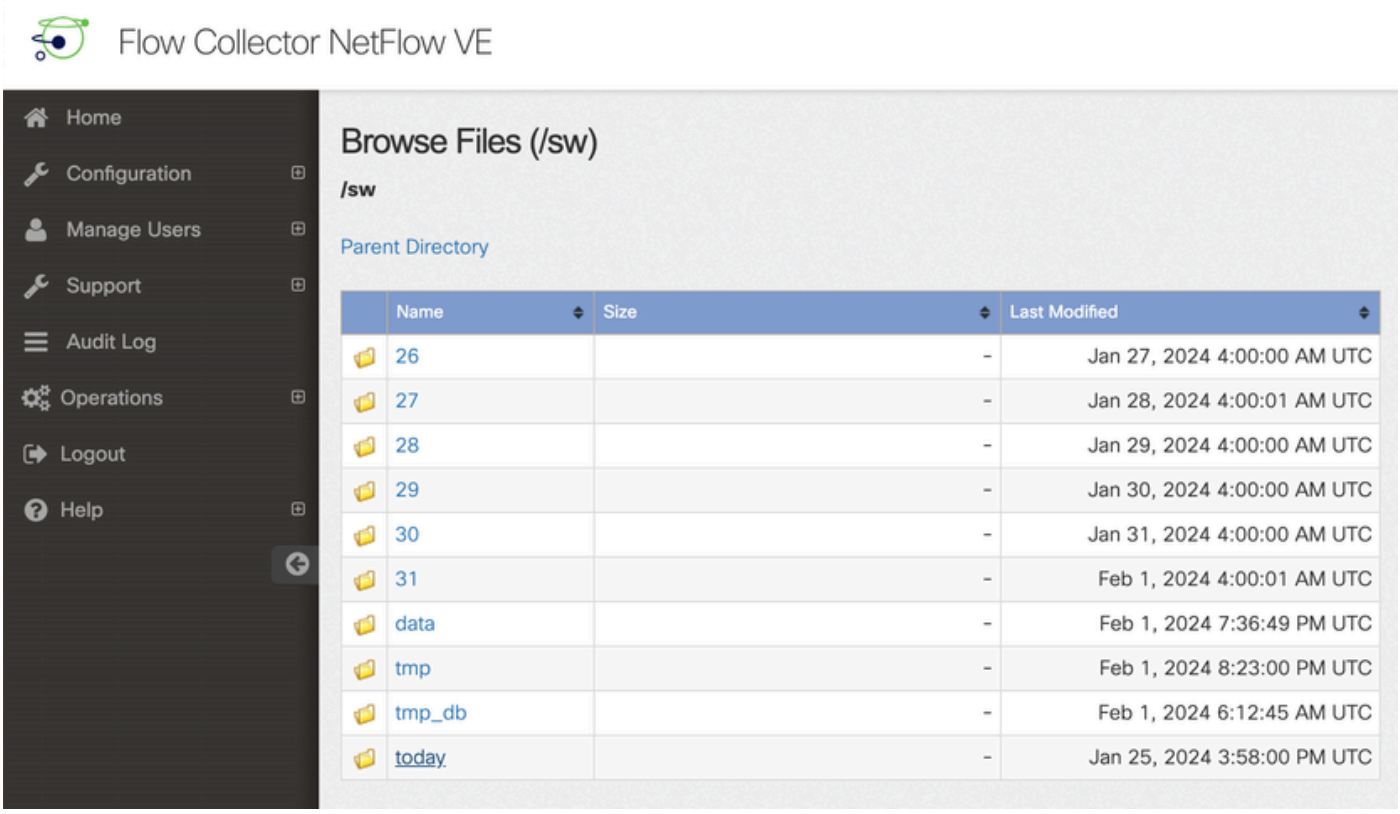
تأكيد التغيير

وهذا التحقق النهائي هو الأهم. انقر فوق قائمة الدعم مرة أخرى واختر إستعراض الملفات.

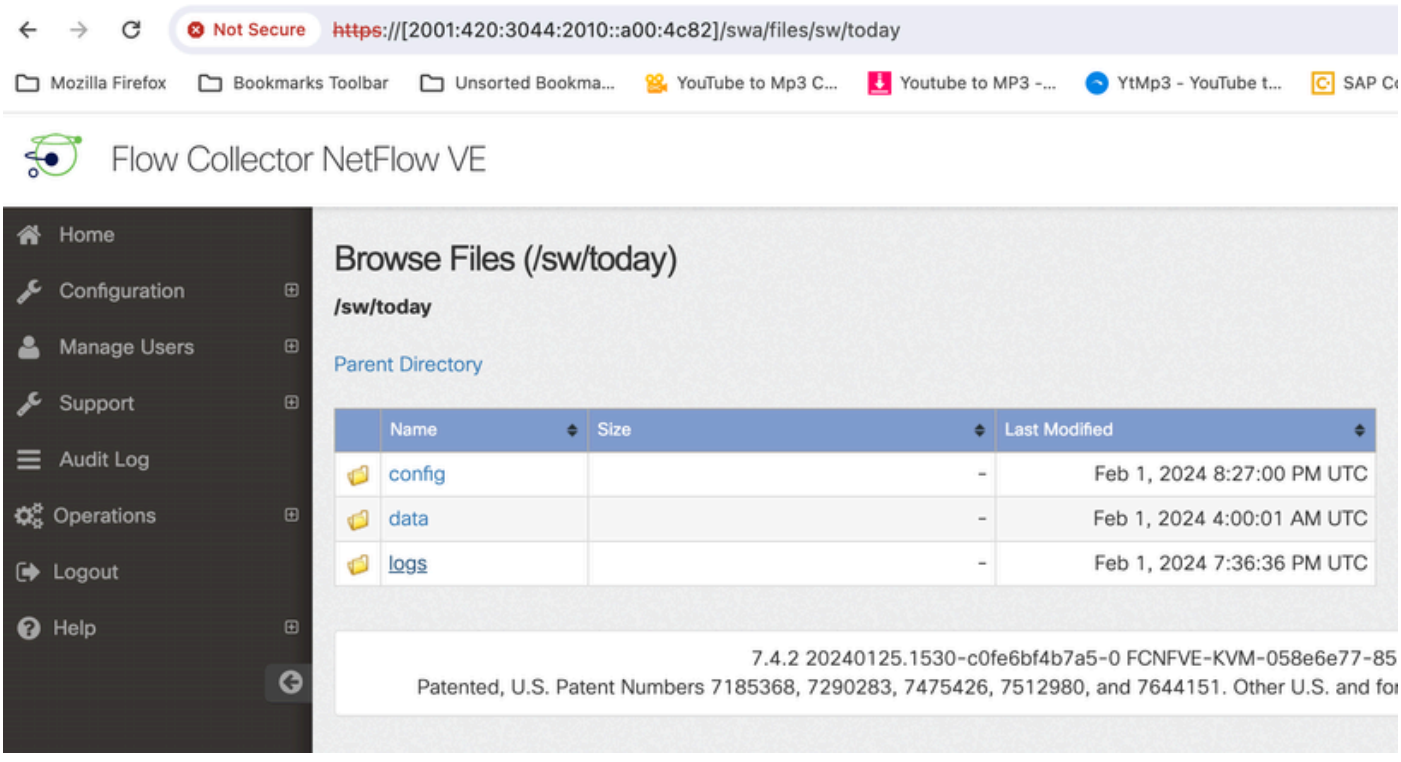
هذا يأخذك إلى نظام الملفات على القناة الليفية. طقطقت على sw.



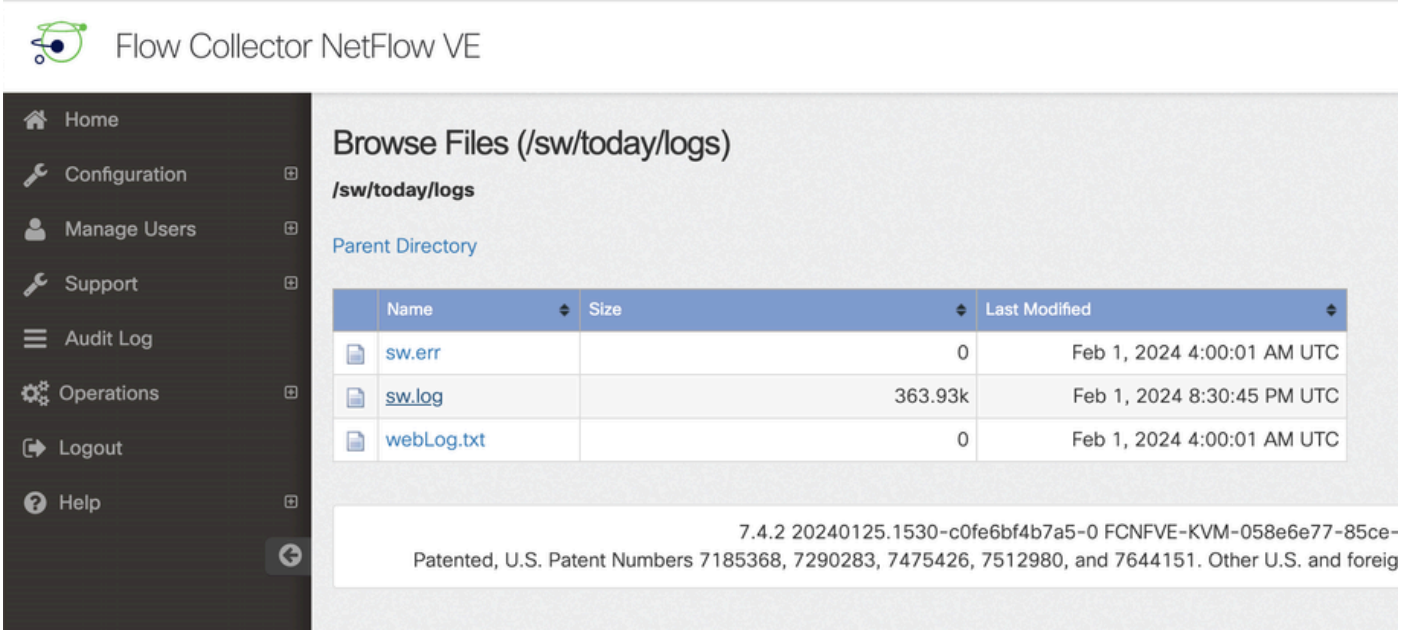
انقر فوق اليوم



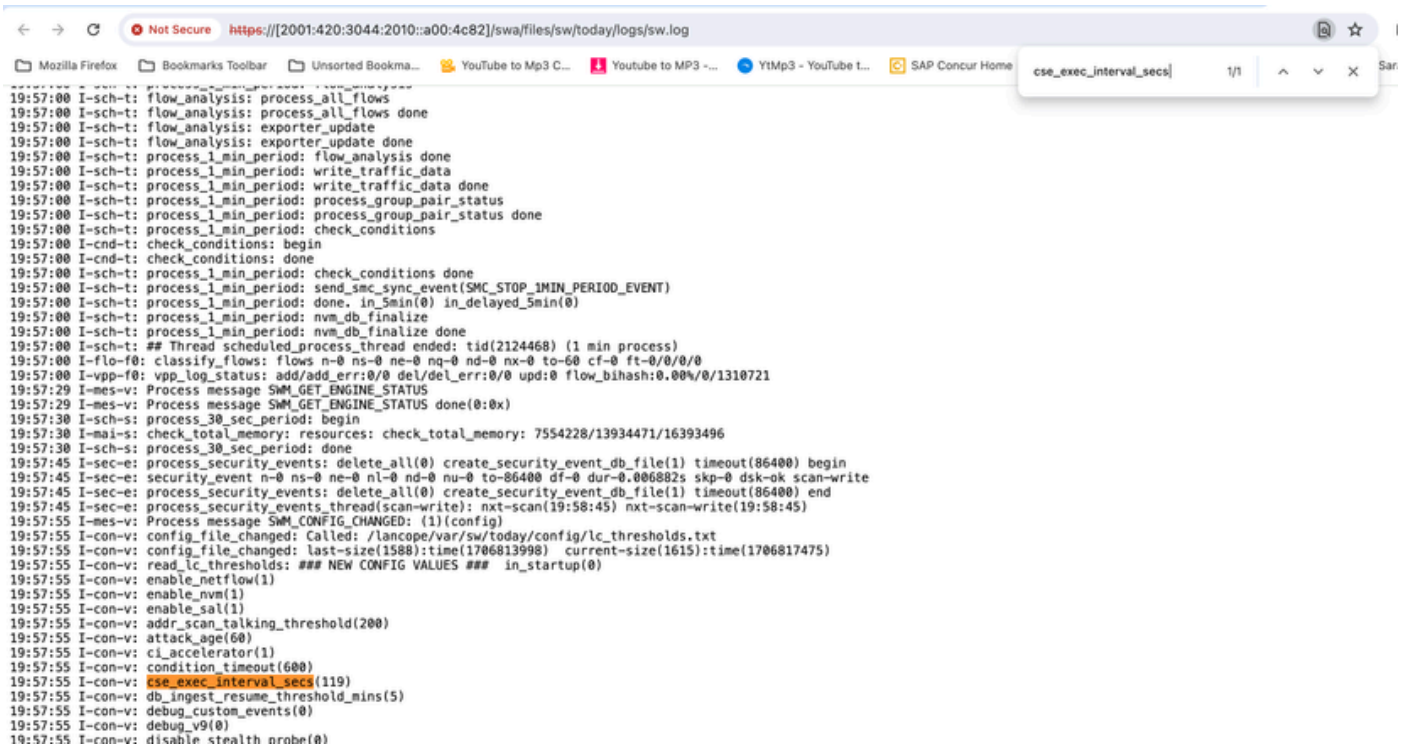
انقر فوق السجلات.



طقطقت على sw.log



قم بإجراء بحث في صفحة المستعرض، أدخل cse_exec_interval_seconds في مربع البحث للعثور على الإعداد المتقدم



يتم سرد "الإعدادات المتقدمة المقبولة" كما هو موضح في لقطة الشاشة.

أما العناصر التي لم يتم قبولها فيتم سردها كما هو موضح ليست جزءا من تكوين الإدخال"، وفي هذه الحالة كان السبب هو خطأ المستخدم في كتابة الإعداد. وهذا هو السبب في أهمية التحقق من السجل بعد إجراء تغييرات التكوين هذه.

```
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)
```

تهانينا!

لقد قمت للتو بإدخال "إعداد متقدم" جديد وتم التحقق من قبوله من قبل المحرك.

الآن، مكنت السمة أن يركض ال CSE منطق على التدفق تقريبا كل 2 دقيقة بعد أن يصل التدفق إلى early_check_age أي تقصير إلى 160 ثاني.

إذا كانت قواعد CSE تتضمن تراكم أعداد البايت على مر الوقت، فإن هذه الميزة تحسن التوقيت الذي يتم عنده تشغيل CSE للتدفقات التي تطابق المعايير التي قمت بتعريفها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).