Geavanceerd afvuren van Flow Collector Engine voor aangepaste security gebeurtenissen configureren

Inhoud

Inleiding

Dit document beschrijft twee geavanceerde instellingen voor stroomverzamelingen die de manier waarop de SNA Flow Collector aangepaste security gebeurtenissen (CSE's) afvuurt, kunnen wijzigen.

Achtergrond

De legacy early_check_age flow Collector geavanceerde instelling, samen met de nieuwe case_exec_interval_secs flow collector geavanceerde instelling bepalen de manier waarop aangepaste security gebeurtenissen worden afgevuurd door de flow collector engine. De stroomverzamelaar is het eerste apparaat in de SNA systeemarchitectuur om de stroom op het netwerk te zien, en dus is de stroomverzamelaar motor verantwoordelijk voor het bewaken van de kenmerken van de stroom(s) tijdens het flow cache, en het bepalen of de stroom voldoet aan de ingestelde criteria van een bepaalde Custom Security Event. Deze flow Collector geavanceerde instellingen veranderen echter NIET de vuureigenschappen van een van de ingebouwde Core Security Events.

Standaard Flow Collector-gedrag

Standaard is de flow Collector early_check_age advanced instelling ingesteld op 160 seconden. Dit betekent dat de Flow Collector-motor minimaal 160 seconden wacht op een stroom voordat hij controleert of die stroom overeenkomt met een geconfigureerde Custom Security Event.

Standaard wordt deze controle pas opnieuw uitgevoerd nadat de stroom is afgelopen.

Deze 160 seconden vroege controlewaarde werd specifiek gekozen omdat als het gebruiken van beste praktijken, de telemetrieexporteurs moeten worden gevormd om telemetrie om de 60 seconden te verzenden. Deze standaardwaarde staat voor genoeg tijd in een typisch milieu voor de stroomcollector toe om stroominformatie te zien met betrekking tot beide kanten van een bepaalde gesprek/stroom. Om deze reden is early_check_age niet vooraf gedefinieerd in de lijst met geavanceerde instellingen. Dit is door ontwerp, en u mag deze waarde niet wijzigen zonder eerst te raadplegen met ondersteuning / engineering. Dit eerste ontwerp presteert echter niet gunstig wanneer het nadenken over lange en enigszins stille stroomkenmerken gekoppeld aan de configuratie van de Aangepaste Security Event die de accumulatie van byte of pakkettellingen impliceren. Dit was de reden voor het aanmaken van de cse_exec_interval_secs geavanceerde setting parameter.

De case_exec_interval_secs geavanceerde instelling

Verkrijgbaar in 7.4.2, de toevoeging van de cse_exec_interval_secs flow collector geavanceerde instelling maakt het nu mogelijk om de motor te instrueren om periodiek de stromen in zijn flow cache te controleren tegen de geconfigureerde Custom Security Events. Deze geavanceerde instelling is met name handig in het geval van lange stromen, waarbij een bepaalde stroom niet voldoet aan de CSE-criteria bij de standaard 160 seconden early_check_age, maar die drempel later in de stroom kruist. Zonder deze geavanceerde instelling zou de Aangepaste Security Gebeurtenis niet vuren tot na de flow eindigt, soms kan dit dagen later zijn.

Effecten op prestaties

Het uitvoeren van deze interval CSE criteria controleert stromen meer tijden in het leven van de stroom dan wat de gebreken bepalen vereist meer cpu. De instructies begeleiden u door het onderzoeken van de inhoud van het sw.log- dossier op de motor van de stroomcollector om een prestatiesbasislijn te bepalen alvorens de cse_exec_interval_secs parameter toe te laten. Als u overweegt om deze geavanceerde instelling in te schakelen en TAC zou willen helpen bij het bevestigen van uw flowcollector gezondheid ter voorbereiding op deze verandering, kan dit worden gedaan door een ondersteuningscase te openen en een flowcollector diagnostisch pakket aan de SR te koppelen.

Het meten van de duur van de classify_flows thread

Eén snelle performance impact meting die je kunt doen is om sw.log vanaf vandaag te onderzoeken en de getallen die vermeld staan na de "cf-"log-ingangen te vergelijken voorafgaand aan de activering van de instelling naar de getallen nadat de instelling is toegepast.

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

20:43:21 I-flo-f0: classificeer_flows: stromen n-1744317 ns-178613 ne-188095 nq-0 en-0 nx-0 tot en met 300 cf-21 ft-126473/792802/940383/14216

20:44:20 l-flo-f4: classificeer_flows: stromen n-1754296 ns-191100 ne-167913 nq-0 en-0 nx-0 tot-300 cf-20 ft-122830/783378/949392/14928

20:44:21 l-flo-f2: classificeer_flows: stromen n-1773175 ns-191930 ne-169039 nq-0 en-0 nx-0 tot-300 cf-20 ft-123055/788507/962264/15431

20:44:21 l-flo-f3: classify_flows: stromen n-1750066 ns-189197 ne-165940 nq-0 en-0 nx-0 tot en met 300 cf-20 ft-122563/779792/944192/15154

20:44:21 l-flo-f5: classify_flows: stromen n-1753899 ns-190477 ne-168004 nq-0 en-0 nx-0 tot en met 300 cf-20 ft-122261/783375/946651/15423

20:44:21 l-flo-f1: classify_flows: stromen n-1763952 ns-191342 ne-169518 nq-0 en-0 nx-0 tot en met 300 cf-20 ft-122782/786822/955997/15175

20:44:21 l-flo-f7: classify_flows: stromen n-1757535 ns-188154 ne-166221 nq-0 en-0 nx-0 tot en met 300 cf-20 ft-122808/781388/951528/14363

20:44:21 l-flo-f6: classify_flows: stromen n-1764211 ns-190964 ne-169013 nq-0 en-0 nx-0 tot en met 300 cf-21 ft-122713/784446/954149/16320

20:44:21 l-flo-f0: classificeer_flows: stromen n-1764197 ns-189780 ne-168784 nq-0 en-0 nx-0 tot en met 300 cf-21 ft-123290/787327/952186/14352

20:45:22 l-flo-f4: classificeer_flows: stromen n-1780277 ns-177512 ne-149843 nq-0 en-0 nx-0 tot-300 cf-21 ft-129553/766777/964933/14864

20:45:22 l-flo-f2: classificeer_flows: stromen n-1789285 ns-175763 ne-155809 nq-0 en-0 nx-0 tot-300 cf-21 ft-129685/772482/976850/15289

20:45:22 l-flo-f3: classify_flows: stromen n-1774883 ns-177085 ne-149715 nq-0 en-0 nx-0 tot en met 300 cf-22 ft-129067/764272/962000/15090

20:45:22 l-flo-f5: classificeren_flows: stromen n-1775998 ns-176898 ne-150682 nq-0 en-0 nx-0 tot en met 300 cf-22 ft-128835/768374/963353/15347

20:45:22 l-flo-f1: classify_flows: stromen n-1786441 ns-175776 ne-151846 nq-0 en-0 nx-0 tot en met 300 cf-22 ft-129255/770212/970360/15129

De cf-vermeldingen staan voor "Stromen classificeren". Dit geeft het aantal seconden weer dat de thread nodig had om zijn pass uit te voeren door het deel van Flow Cache dat verantwoordelijk is. In de "classificeer stromen"-draden worden de centrale entiteiten toegepast op de stromen. Als je ziet dat deze getallen stijgen na het inschakelen van de functie, dat is een goede meting van de totale impact op de prestaties.

Er wordt een stijging verwacht na het toevoegen van deze geavanceerde intervalinstelling, maar als dit getal 60 nadert, verwijdert u de instelling omdat de impact te groot is. Een verhoging met enkele seconden wordt verwacht en redelijk geacht.

Motorstatus tijdens de prestatieperiode

Een andere prestatie "voor vs na" meting die u kunt doen is kijken naar de "Prestatie Periode" secties in het sw.log bestand die elke 5 minuten worden vastgelegd om de impact van de instelling op flow processing te meten. Je kunt deze blokken ook zoeken met grep. Als de Engine overweldigd is, moet deze geavanceerde instellingsinterfacecontrole worden uitgeschakeld.

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

kennis te nemen van elke andere status dan "Normale motorstatus";

Een status zoals "Engine status Input rate too high" geeft aan dat de classify_flows thread te veel CPU verbruikt.

SFI - Statische Flow Index

De classificatiethreads waren niet in staat om hun passages door het flow cache te voltooien: het staat voor "Static Flow Index" en het wijst op een strijd in de classificeer flow threads. Het is geen ramp op zich, maar het geeft aan dat de motor het plafond begint te raken en dat de prestaties beginnen af te nemen op het huidige niveau van het cf.

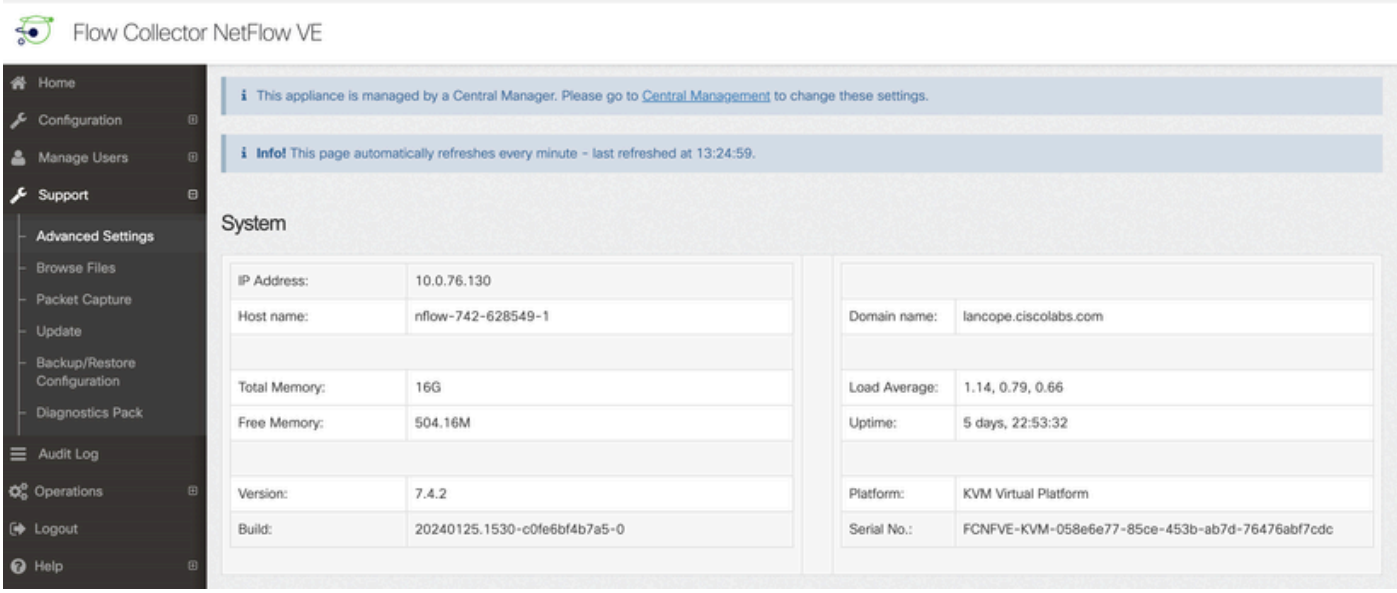
sw.log:16:09:49 I-flo-f1: classify_flows: sfi:base(8388608) (10522745 -> 11014427) max(16777215) cod(1) (491681/8388608)---------->(5%)
sw.log:16:09:49 I-flo-f3: classify_flows: sfi:base(25165824) (27269277 -> 27754304) max(33554431) cod(1) (485026/8388608)---------->(5%)
sw.log:16:09:49 I-flo-f4: classify_flows: sfi:base(33554432) (35652656 -> 36138422) max(41943039) cod(1) (485765/8388608)---------->(5%)
sw.log:16:09:49 I-flo-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-flo-f2: classify_flows: sfi:base(16777216) (19499308 -> 17522620) max(25165823) cod(0) (6411919/8388608)---------->(76%)
sw.log:16:10:49 I-flo-f1: classify_flows: sfi:base(8388608) (11014427 -> 8976309) max(16777215) cod(0) (6350489/8388608)---------->(75%)
sw.log:16:10:49 I-flo-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 I-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) kabeljauw(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%)

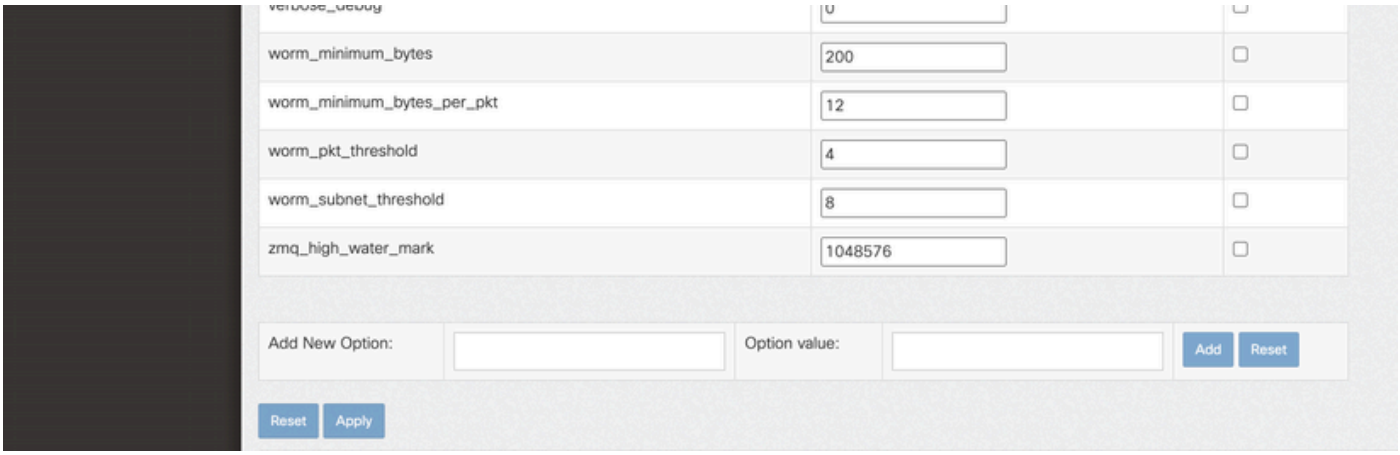
Configureren

Open een webbrowser en navigeer rechtstreeks naar het Flow Collector-apparaat IP. Aanmelden als lokale beheerder.

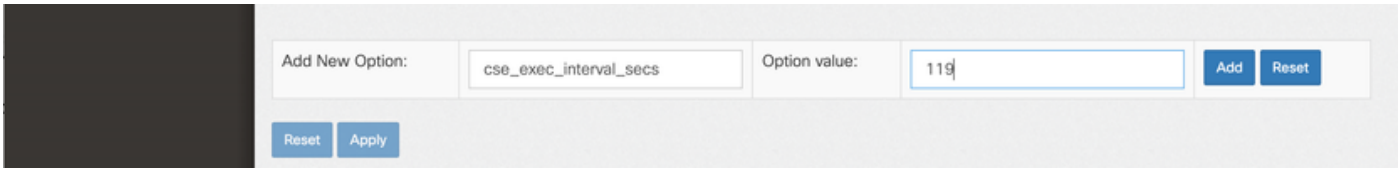
Naar ondersteuning navigeren -> Geavanceerde instellingen



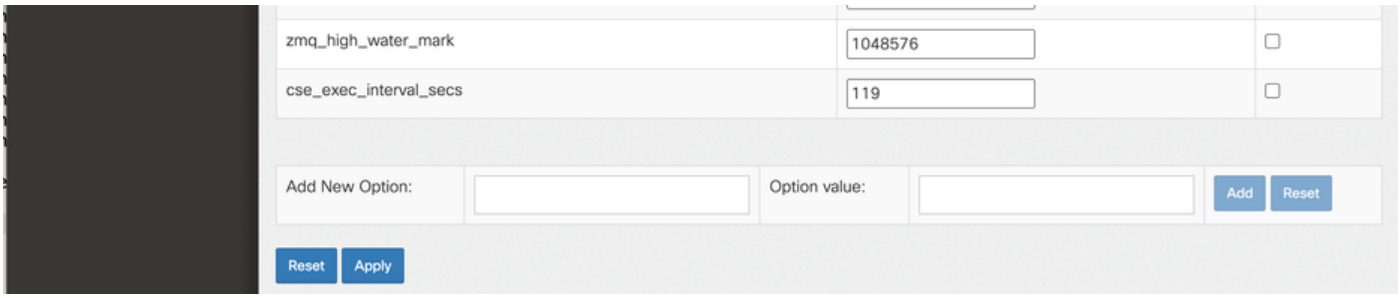
Blader door het scherm Geavanceerde instelling om het configuratievenster "Nieuwe optie toevoegen" onder in de lijst weer te geven



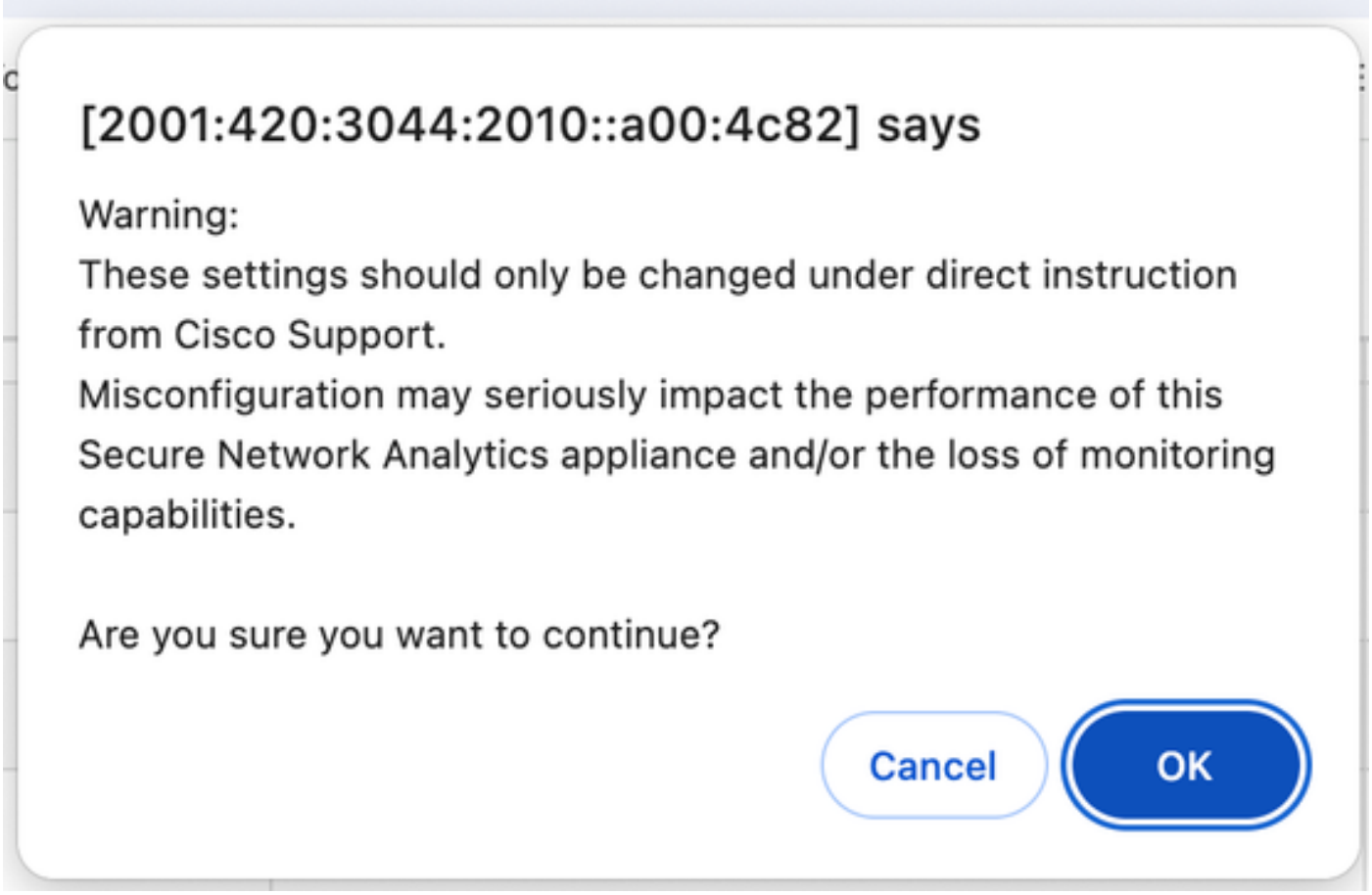
In het veld Nieuwe optie toevoegen: bewerkingsvak invoeren case_exec_interval_secs en in de waarde Optie: bewerkingsvak invoeren 119. Bewerken van deze vakjes schakelt de knop Toevoegen in. Druk op de knop Add nadat u case_exec_interval_secs hebt ingevoerd in het vak Add New Option: edit en 119 in het vak Option Value: edit.



De waarde Optie toevoegen: en Optie: bewerk vakken die worden gewist ter voorbereiding van een andere vermelding in het geval dat meerdere nieuwe Geavanceerde Instellingen worden ingevoerd. De nieuwe geavanceerde instellingen worden onderaan de lijst geplaatst terwijl ze worden toegevoegd. Dit geeft de gebruiker een kans om de ingang te inspecteren. De exacte spelling van de geavanceerde instelling is belangrijk, evenals de case. Alle geavanceerde instellingen zijn in kleine letters.



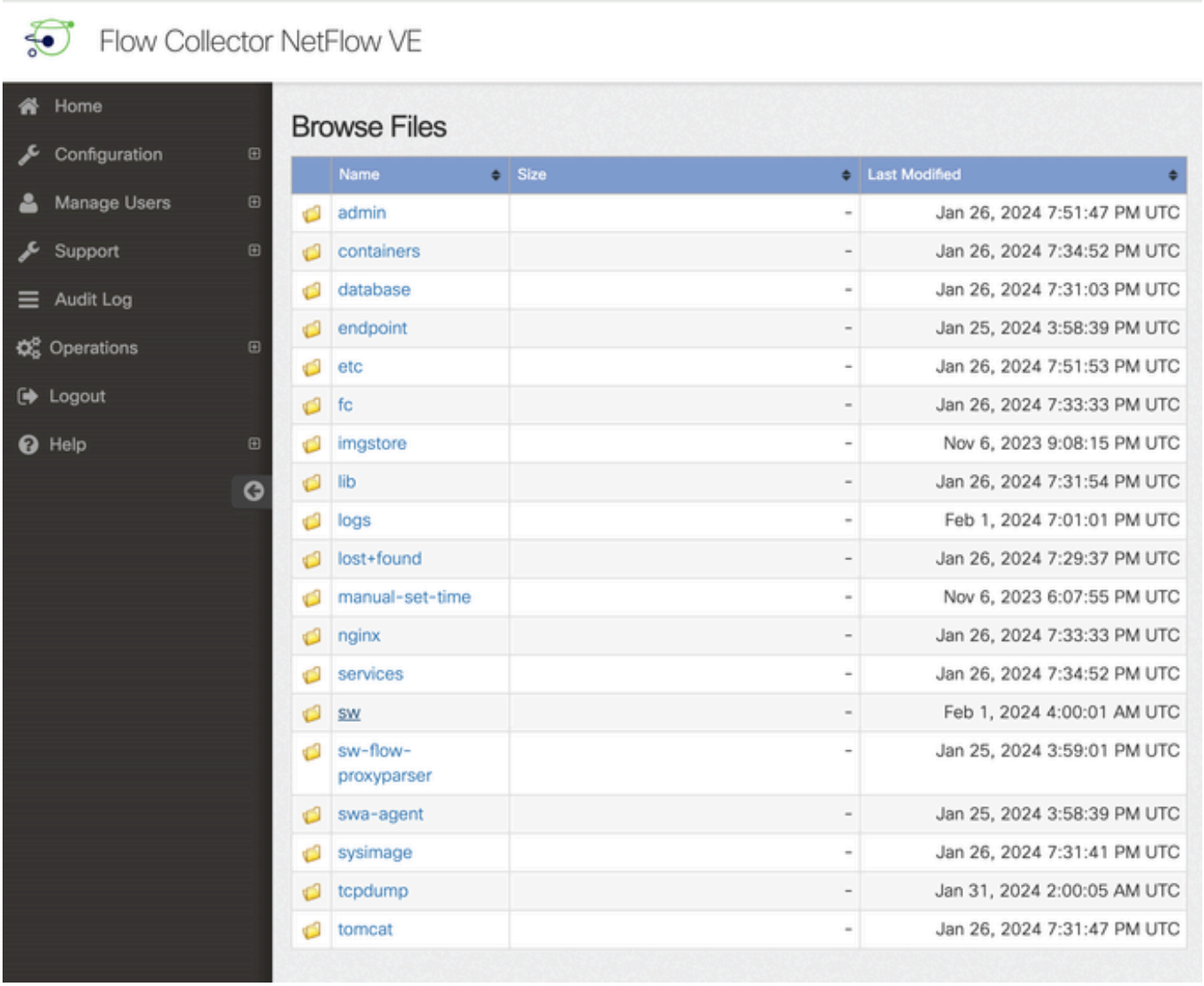
Nu de geavanceerde instelling op de juiste manier is ingevoerd, drukt u op de knop Toepassen. Merk op dat soms de knop Toepassen niet is ingeschakeld. Als u deze optie wilt inschakelen, klikt u op in het veld Nieuwe optie toevoegen: bewerk het veld en vervolgens wordt de knop Toepassen ingeschakeld om te klikken. Wanneer deze pop-up wordt weergegeven, drukt u op de knop OK om de nieuwe geavanceerde instelling en waarde in te dienen.



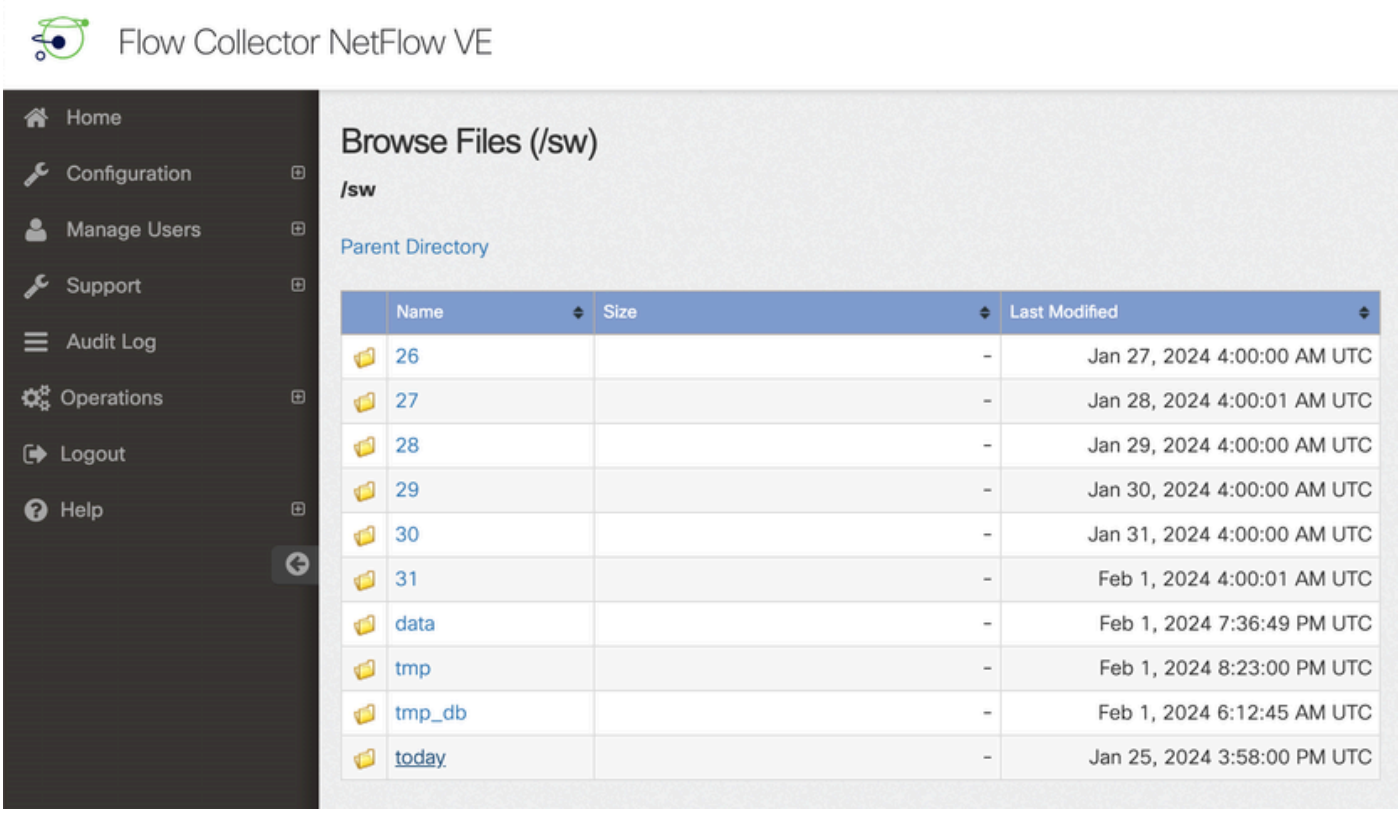
De wijziging bevestigen

Deze definitieve validatie is het belangrijkste. Klik nogmaals op het menu Ondersteuning en kies Bestanden bladeren.

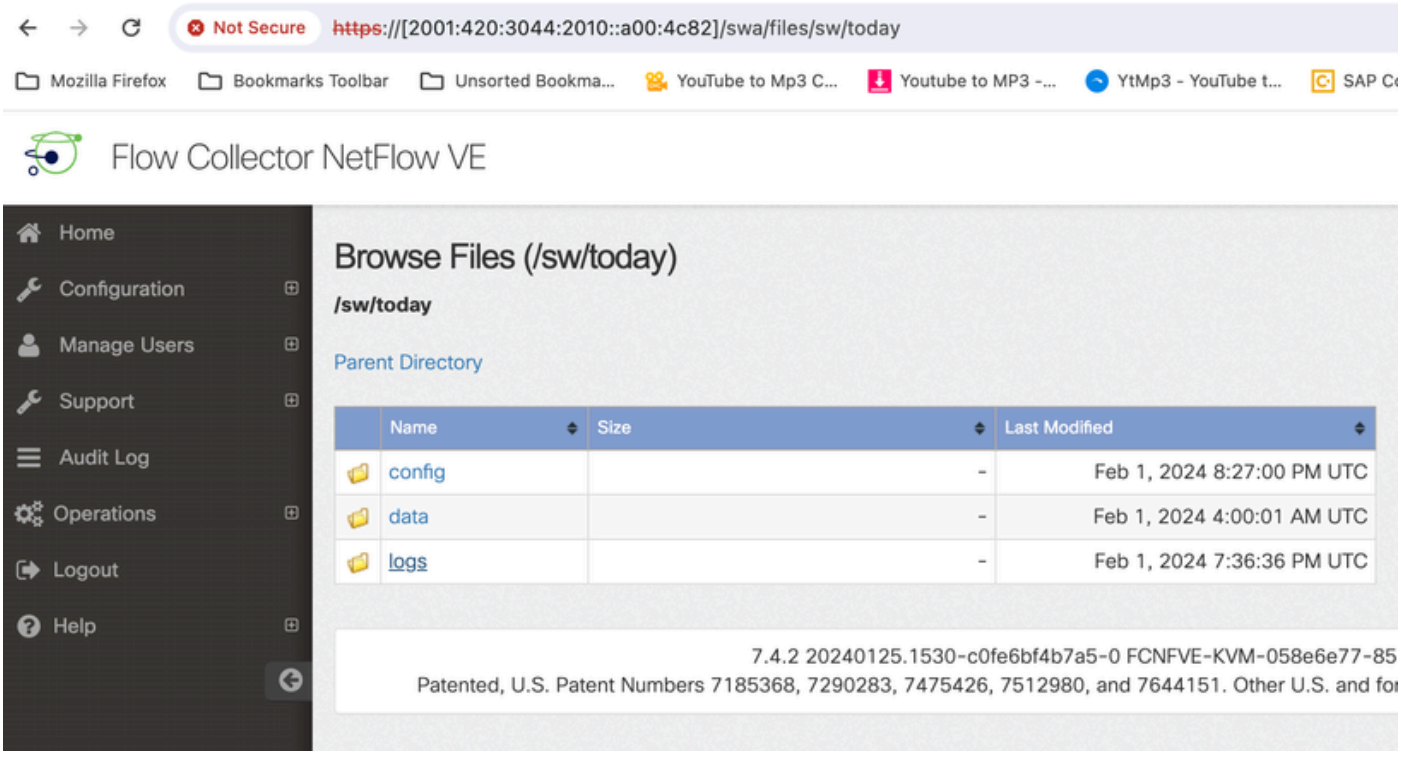
Dit brengt u naar het bestandssysteem op de FC. Klik op sw.



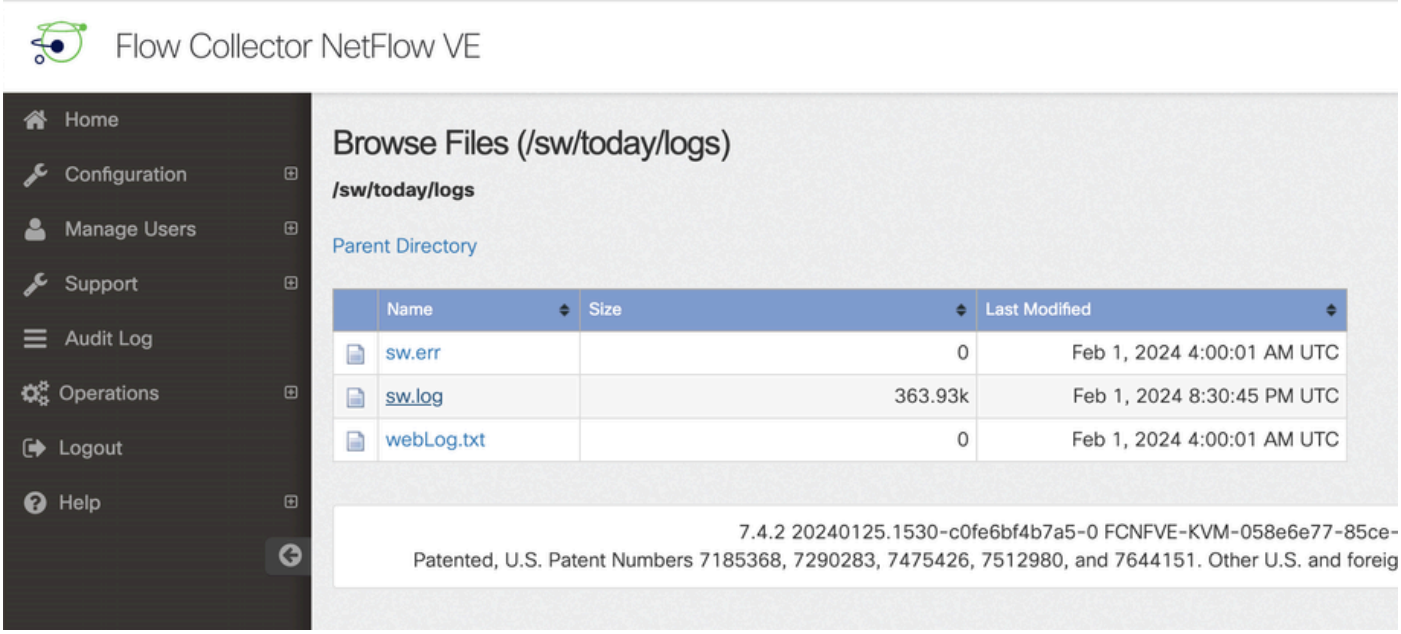
Klik op vandaag



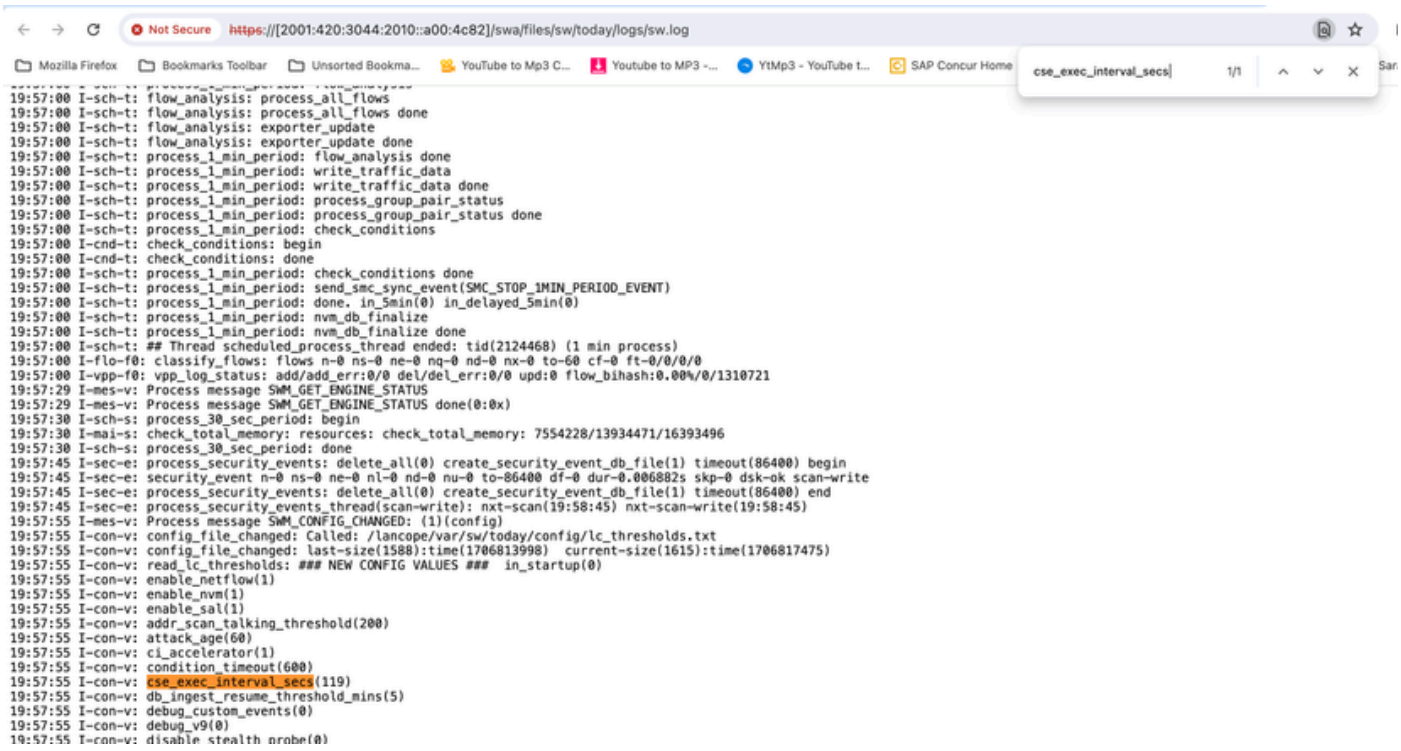
Klik op logboeken.



Klik op sw.log



Voer een zoekopdracht uit in de browser pagina, Voer case_exec_interval_secs in het zoekvak om de geavanceerde instelling te vinden



Geavanceerde instellingen die worden geaccepteerd, worden weergegeven zoals in de screenshot.

Degenen die niet worden geaccepteerd worden vermeld als "niet onderdeel van de invoerconfiguratie", in dit geval vanwege een spelfout bij de gebruiker van de instelling. Dit is waarom zijn belangrijk om het logboek te controleren na het aanbrengen van dergelijke configuratieveranderingen.

```
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)
```

Gefeliciteerd!

U hebt zojuist een nieuwe geavanceerde instelling ingevoerd en de acceptatie ervan door de motor gevalideerd.

Nu wordt de functie ingeschakeld om de CSE logic op de stromen uit te voeren ongeveer elke 2 minuten nadat de stroom de early_check_age bereikt die standaard 160 seconden.

Als de CSE-regels betrekking hebben op het verzamelen van bytellingen in de loop van de tijd, verbetert deze functie de timing waarbij de CSE's starten op stromen die overeenkomen met de criteria die u hebt gedefinieerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.