Configuration du comportement de déclenchement d'événements de sécurité personnalisés du moteur de collecteur de flux avancé

Table des matières

- Introduction
- Fond
- Débogage des événements de sécurité personnalisés
- Comportement du collecteur de flux par défaut
- Le paramètre avancé cse_exec_interval_secs
- Impacts sur les performances
  - Mesure de la durée du thread classify_flows
  - État du moteur sur la période de performances
  - SFI - Indice de flux statique
- Configuration
- Confirmation de la modification
- Félicitations !

Introduction

Ce document décrit deux paramètres avancés du collecteur de flux qui peuvent modifier la façon dont le collecteur de flux SNA déclenche les événements de sécurité personnalisés (CSE).

Fond

Le paramètre avancé du collecteur de flux early_check_age hérité, ainsi que le nouveau paramètre avancé du collecteur de flux cse_exec_interval_secs déterminent la manière dont les événements de sécurité personnalisés sont déclenchés par le moteur du collecteur de flux. Le collecteur de flux est le premier dispositif de l'architecture du système SNA à voir le flux sur le réseau, et par conséquent le moteur de collecteur de flux est chargé de surveiller les caractéristiques du ou des flux lorsqu'il se trouve dans le cache de flux, et de déterminer si le flux répond aux critères configurés d'un événement de sécurité personnalisé donné. Cependant, ces paramètres avancés du collecteur de flux ne modifient PAS les caractéristiques de déclenchement de l'un des événements de sécurité principaux intégrés.

Débogage des événements de sécurité personnalisés

Dans les versions 7.5.0 et ultérieures de SNA, le paramètre avancé du collecteur de flux debug_custom_events a été amélioré pour fournir différents niveaux de débogage

- debug_custom_events 1 (débogage minimal - conçu pour pouvoir s'exécuter en production et fournir plus d'informations sur les flux exacts qui génèrent des CSE)
- debug_custom_events 2 (plus de débogage)
- debug_custom_events 3 (débogage le plus prolixe)

Comportement du collecteur de flux par défaut

Par défaut, le paramètre avancé du collecteur de flux early_check_age est configuré sur 160 secondes. Cela signifie que le moteur de collecteur de flux attend au moins 160 secondes dans un flux avant de vérifier si ce flux correspond à un événement de sécurité personnalisé configuré. Par défaut, cette vérification n'est pas effectuée à nouveau avant la fin du flux.

Cette valeur de contrôle anticipé de 160 secondes a été choisie spécifiquement parce que si vous utilisez les meilleures pratiques, les exportateurs de télémétrie doivent être configurés pour envoyer la télémétrie toutes les 60 secondes. Cette valeur par défaut permet au collecteur de flux d'afficher suffisamment de temps dans un environnement standard pour afficher les informations de flux relatives aux deux côtés d'une conversation/d'un flux donné. Pour cette raison, le early_check_age n'est pas prédéfini dans la liste des paramètres avancés. Cela est prévu dès la conception et vous ne devez pas modifier cette valeur sans avoir au préalable consulté l'assistance/l'ingénierie. Cependant, cette conception initiale ne donne pas de bons résultats si l'on considère les caractéristiques de flux longs et relativement silencieux associées à la configuration d'événements de sécurité personnalisés impliquant l'accumulation de nombres d'octets ou de paquets. C'est pour cette raison que le paramètre de paramètre avancé cse_exec_interval_secs a été créé .

Le paramètre avancé cse_exec_interval_secs

Disponible dans la version 7.4.2, l'ajout du paramètre avancé du collecteur de flux cse_exec_interval_secs permet maintenant de demander au moteur de vérifier régulièrement les flux dans son cache de flux par rapport aux événements de sécurité personnalisés configurés. Ce paramètre avancé est particulièrement utile dans le cas des flux longs, où un flux donné n'a pas correspondu sur un critère CSEs à la valeur par défaut de 160 secondes early_check_age, mais dépasse ce seuil plus tard dans le flux. Sans ce paramètre avancé, l'événement de sécurité personnalisé ne se déclenche qu'après la fin du flux, parfois plusieurs jours plus tard.

Impacts sur les performances

L'exécution de ces critères CSE d'intervalle vérifie les flux plus de fois dans la vie du flux que ce que les valeurs par défaut définissent ne nécessite plus de CPU. Les instructions vous guident tout au long de l'analyse du contenu du fichier sw.log sur le moteur de collecteur de flux afin de déterminer une ligne de base de performances avant d'activer le paramètre cse_exec_interval_secs. Si vous envisagez d'activer ce paramètre avancé et souhaitez que le

centre d'assistance technique vous aide à confirmer l'état de votre collecteur de flux en préparation de ce changement, vous pouvez le faire en ouvrant un dossier d'assistance et en attachant un pack de diagnostic de collecteur de flux au SR.

Mesure de la durée du thread classify_flows

Une mesure rapide de l'impact sur les performances que vous pouvez effectuer est d'examiner le fichier sw.log à partir d'aujourd'hui et de comparer les numéros répertoriés après les entrées de journal « cf-« avant l'activation du paramètre aux numéros après l'application du paramètre.

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

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

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

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

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

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

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

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

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

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

20:45:22 I-flo-f4 : classify_flows : flux n-1780277 ns-177512 ne-149843 nq-0 nd-0 nx-0 to-300 cf-21 ft-129553/766777/964933/14864

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

20:45:22 I-flo-f3: classify_flows : flux n-1774883 ns-177085 ne-149715 nq-0 nd-0 nx-0 to-300 cf-22 ft-129067/764272/962000/15090

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

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

Les entrées cf signifient « Classifier les flux ». Cela représente le nombre de secondes que le thread a mis pour passer à travers la section du cache de flux dont il est responsable. C'est dans les threads « Classifier les flux » que les CSE sont appliqués par rapport aux flux. Si vous constatez que ces chiffres augmentent après l'activation de la fonction, cela constitue une bonne mesure de l'impact global sur les performances.

Une augmentation est attendue après l'ajout de ce paramètre d'intervalle avancé, mais si ce nombre approche 60, supprimez le paramètre car l'impact est trop important. Une augmentation de quelques secondes est attendue et considérée comme raisonnable.

État du moteur sur la période de performances

Une autre mesure des performances « avant/après » que vous pouvez effectuer consiste à consulter les sections « Période de performances » du fichier sw.log qui sont consignées toutes les 5 minutes pour évaluer l'impact du paramètre sur le traitement du flux. Vous pouvez rechercher ces blocs en utilisant grep aussi bien. Si le moteur est saturé, cette vérification de l'intervalle de réglage avancé doit être désactivée.

/lancope/var/sw/today/logs/ grep -A3 "Période de performances" sw.log

Prenez note de tout état autre que « État du moteur normal ».

Un état tel que « Engine status Input rate too high » indique que le thread classify_flows consomme trop de CPU.

SFI - Indice de flux statique

Signifie que les threads de classification n'ont pas pu terminer leur passage dans le cache de flux : il s'agit de « Static Flow Index » et indique une difficulté dans les threads de classification. Ce n'est pas un désastre en soi, mais cela indique que le moteur commence à atteindre le plafond et que les performances commencent à se dégrader aux niveaux actuels des fc.

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)

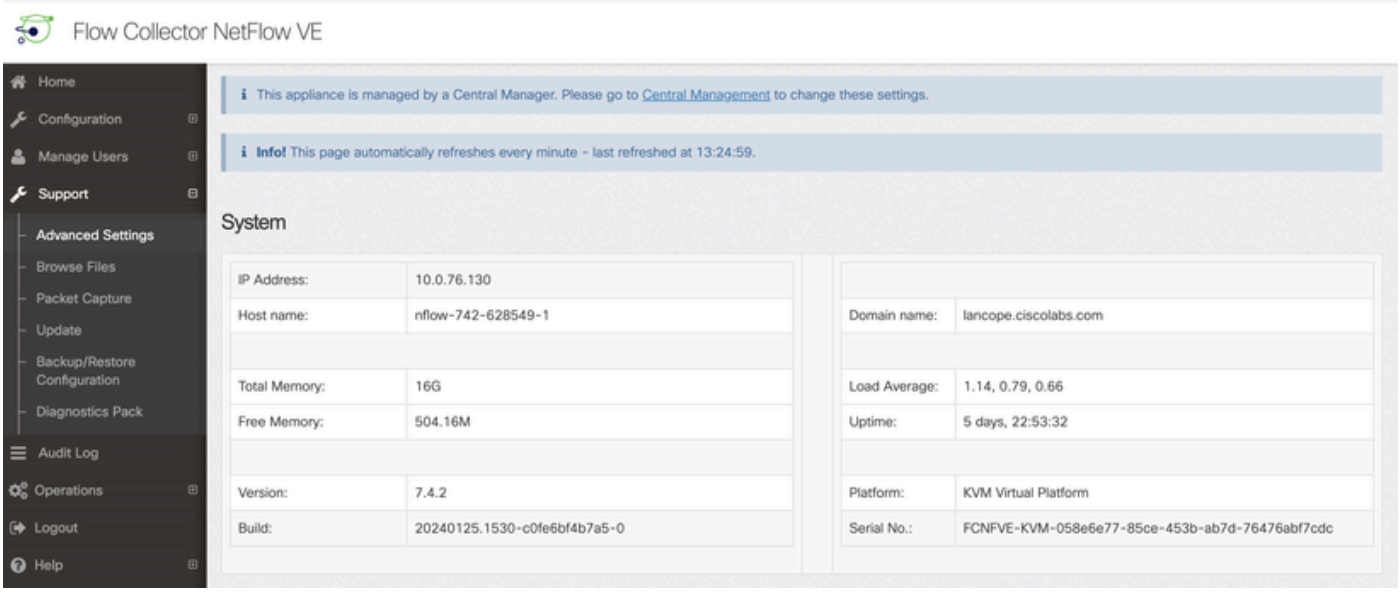
max(25165823) cod(0) (6411919/8388608)---------->(76 %)
sw.log:16:10:49 l-flo-f1: classify_flows : sfi : base(8388608) (11014427 -> 8976309)
max(16777215) cod(0) (6350489/8388608)---------->(75 %)
sw.log:16:10:49 l-flo-f3: classify_flows : sfi : base(25165824) (27754304 -> 25702968)
max(33554431) cod(0) (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 %)

Configuration

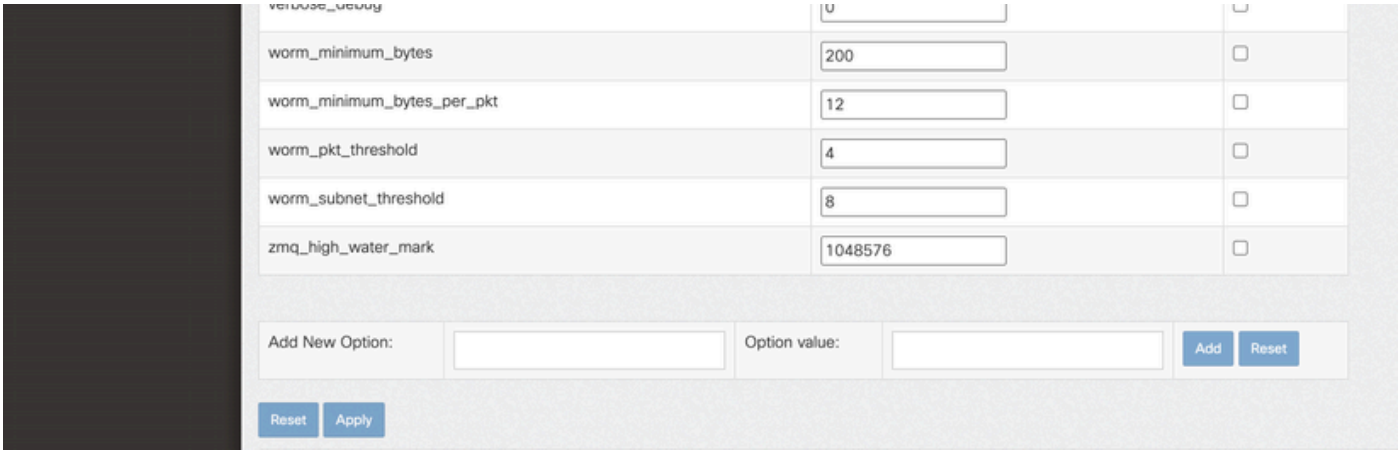
Ouvrez un navigateur Web et accédez directement à l'adresse IP de l'appliance Flow Collector. Connectez-vous en tant qu'administrateur local.



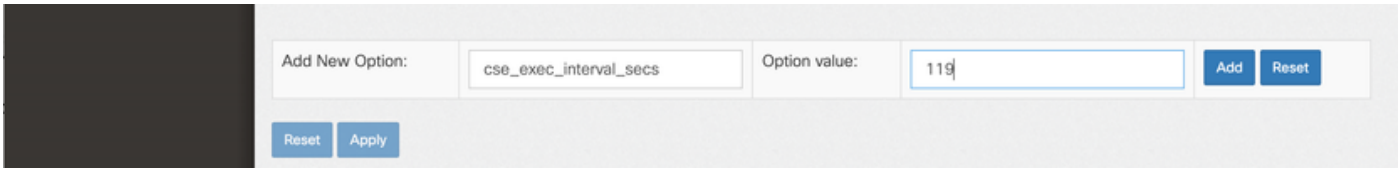
Accédez à Support -> Advanced Settings



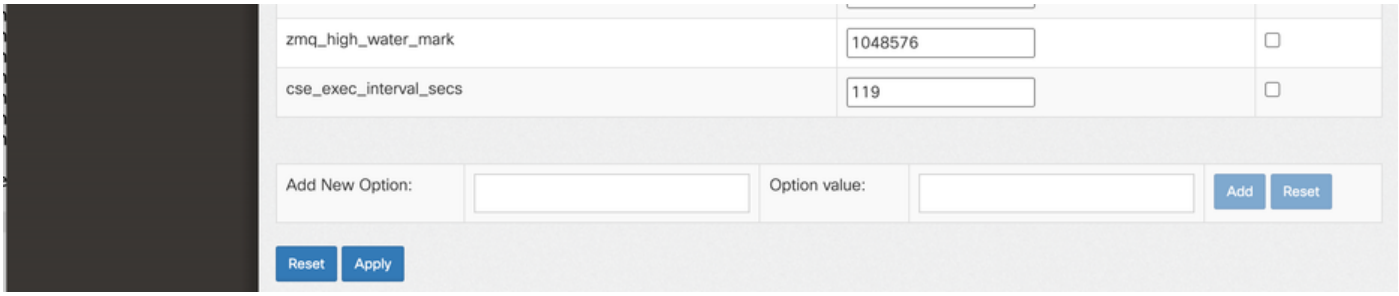
Faites défiler l'écran Advanced Setting (Paramètres avancés) pour afficher la zone de configuration Add New Option (Ajouter une nouvelle option) au bas de la liste



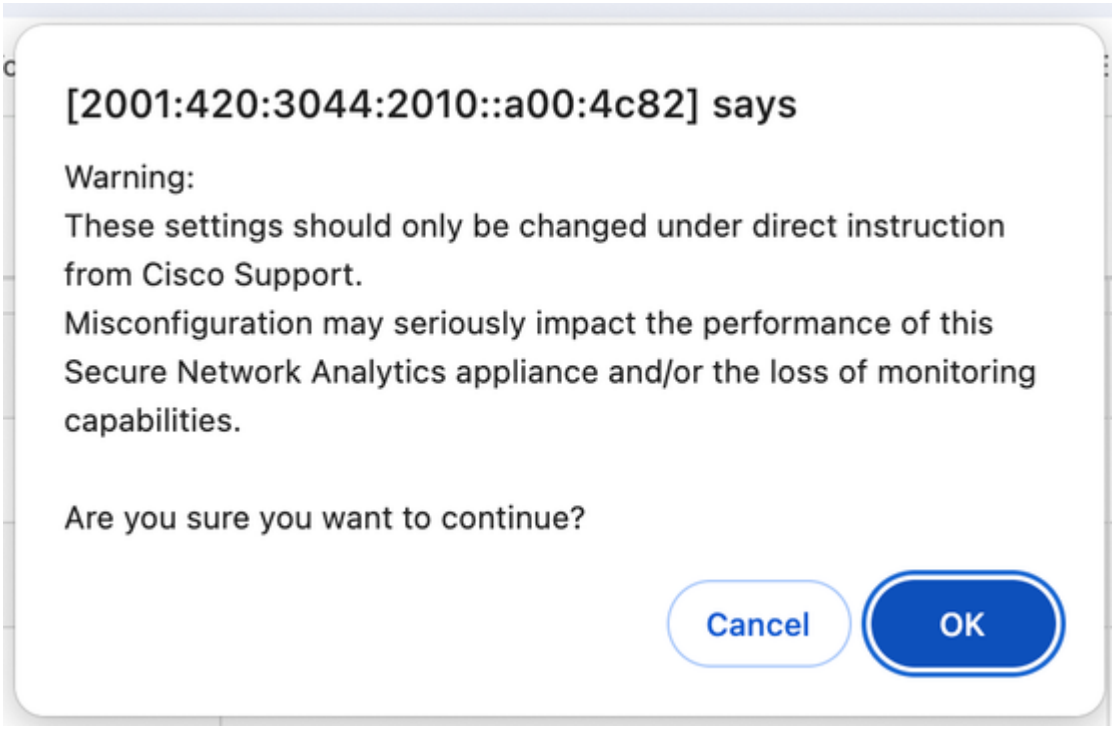
Dans l'option Add New : entrez cse_exec_interval_secs et dans la zone Option : saisissez 119 dans la zone de texte. La modification de ces zones active le bouton Ajouter. Appuyez sur le bouton Add après avoir entré cse_exec_interval_secs dans la zone Add New Option : et 119 dans la zone Valeur de l'option : de l'Aide.



L'option Add New : et Valeur d'option : effacer les zones de modification en vue d'une autre entrée au cas où plusieurs nouveaux paramètres avancés seraient entrés. Les nouveaux paramètres avancés sont placés en bas de la liste au fur et à mesure de leur ajout. L'utilisateur a ainsi la possibilité d'inspecter l'entrée. L'orthographe exacte du paramètre avancé est importante, tout comme la casse. Tous les paramètres avancés sont en minuscules.



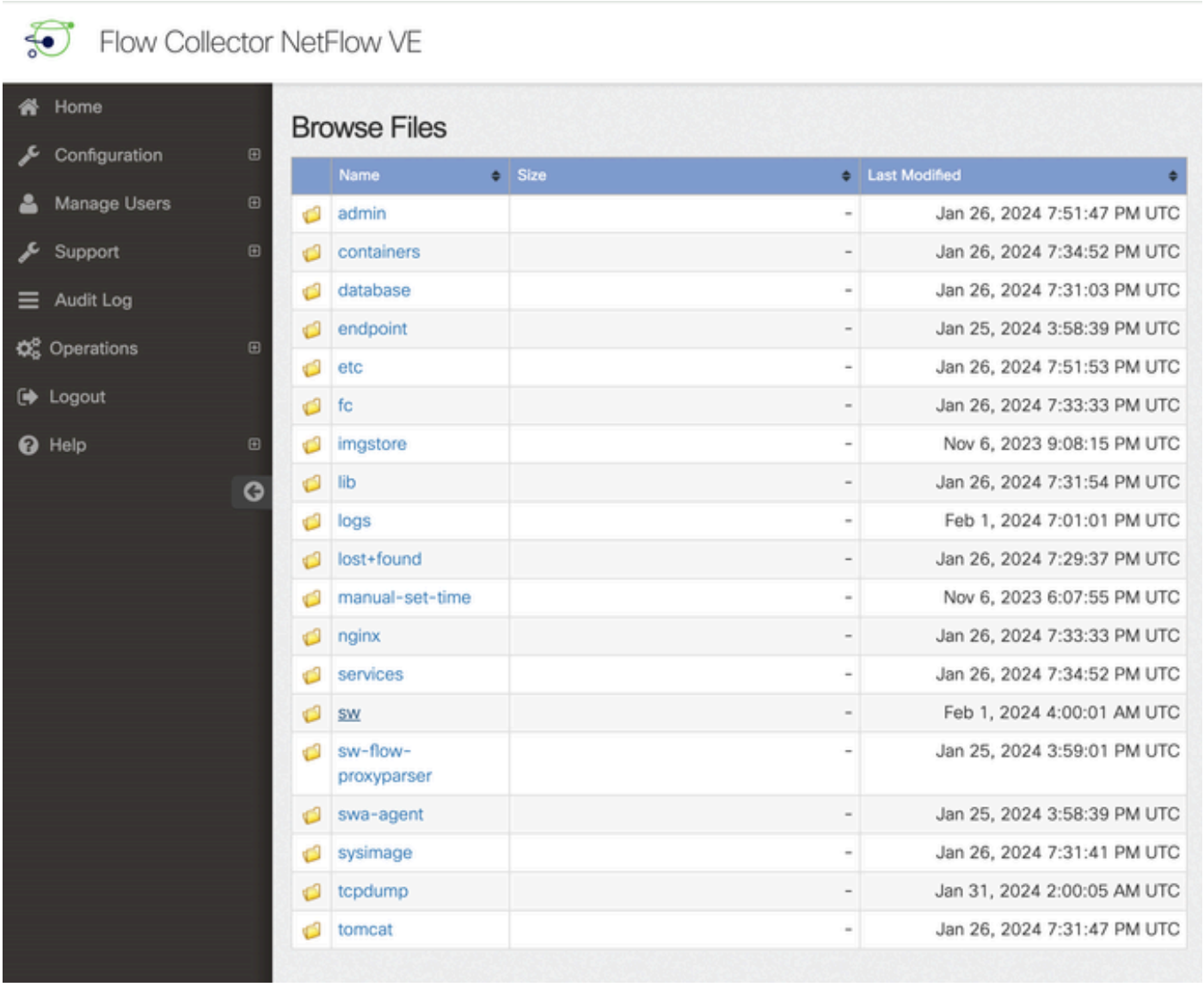
Maintenant que le paramètre avancé est entré correctement, appuyez sur le bouton Appliquer. Notez que le bouton Appliquer n'est parfois pas activé. Pour l'activer, cliquez sur Add New Option: puis le bouton Apply (Appliquer) est activé pour le clic. Lorsque cette fenêtre contextuelle s'affiche, appuyez sur le bouton OK pour envoyer les nouveaux paramètres avancés et la valeur.



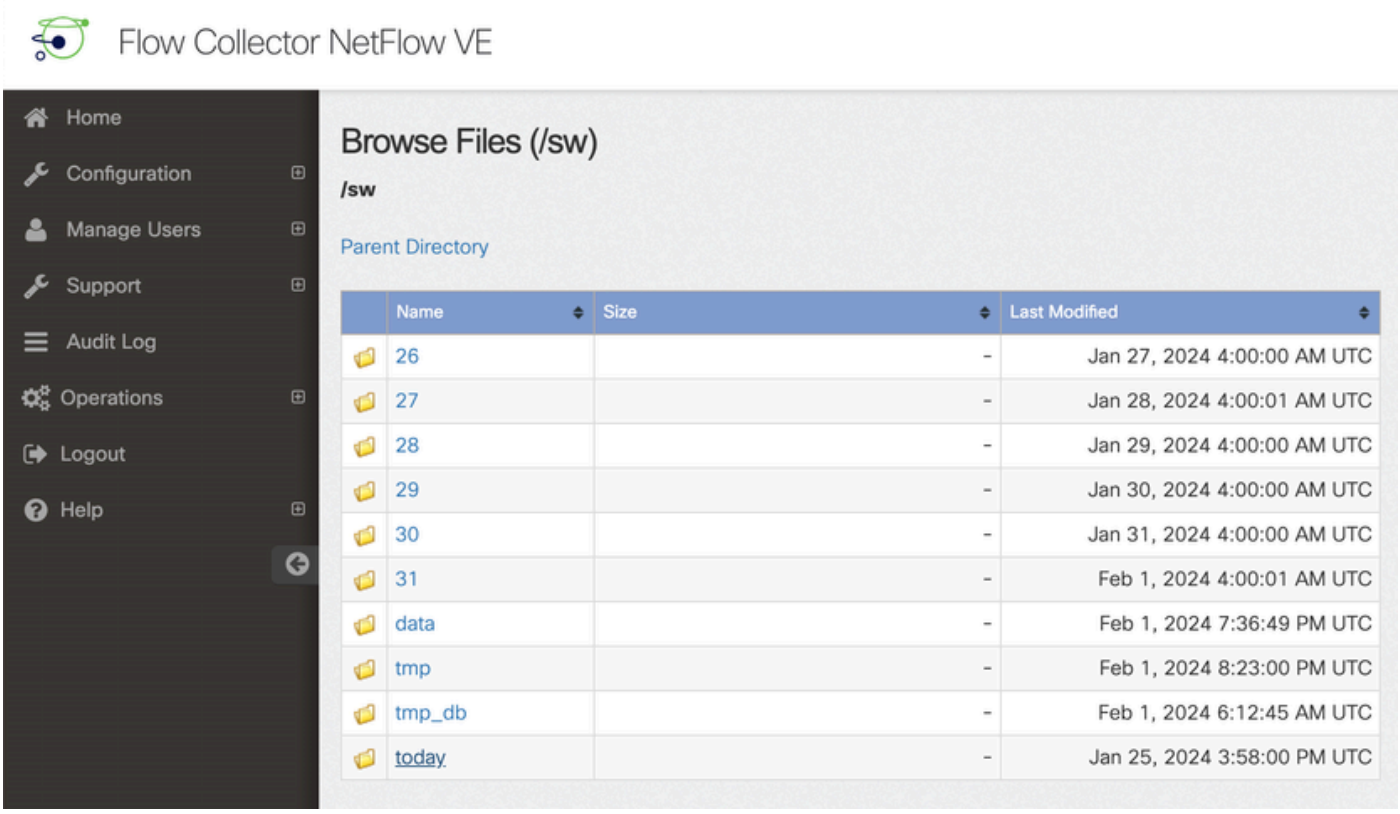
Confirmation de la modification

Cette validation finale est la plus importante. Cliquez à nouveau sur le menu Support et choisissez Browse Files.

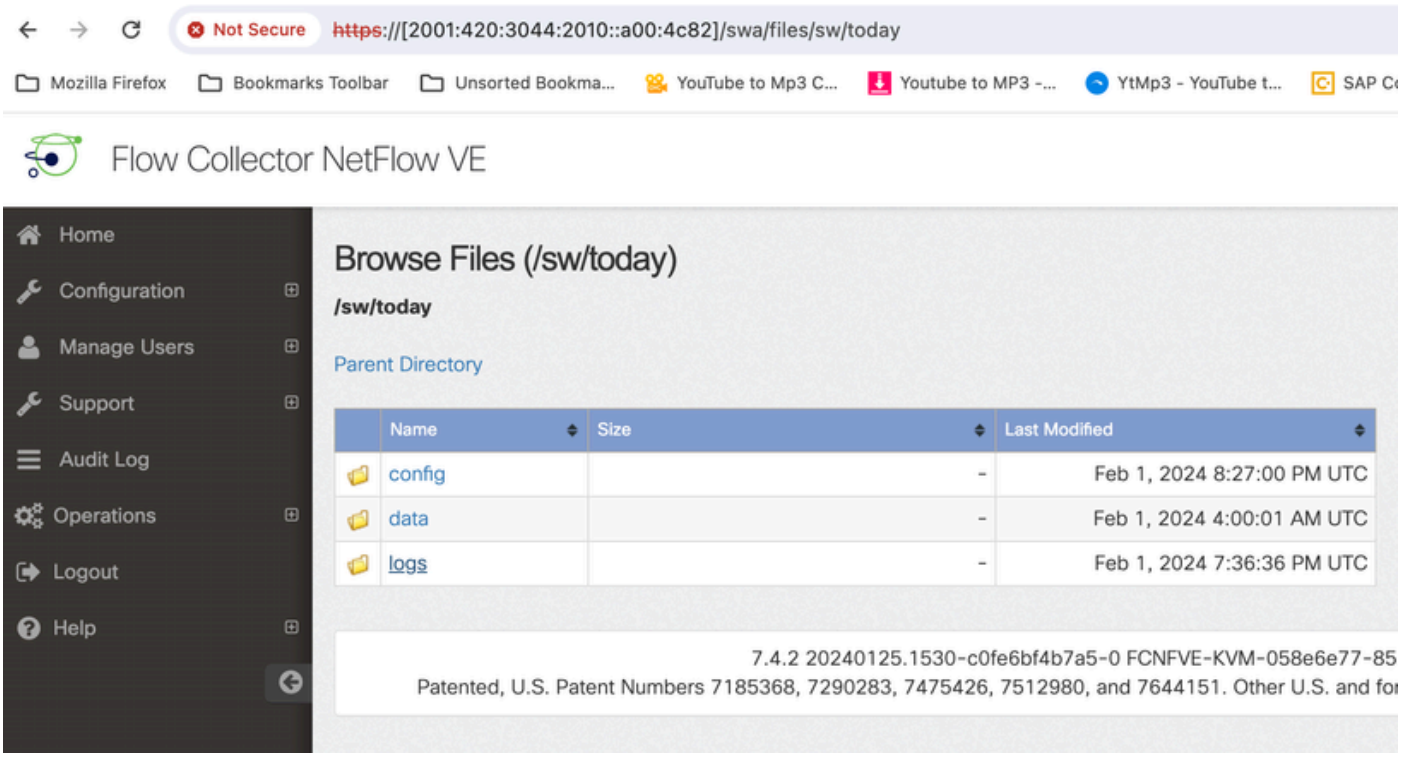
Vous accédez ainsi au système de fichiers sur le FC. Cliquez sur log.



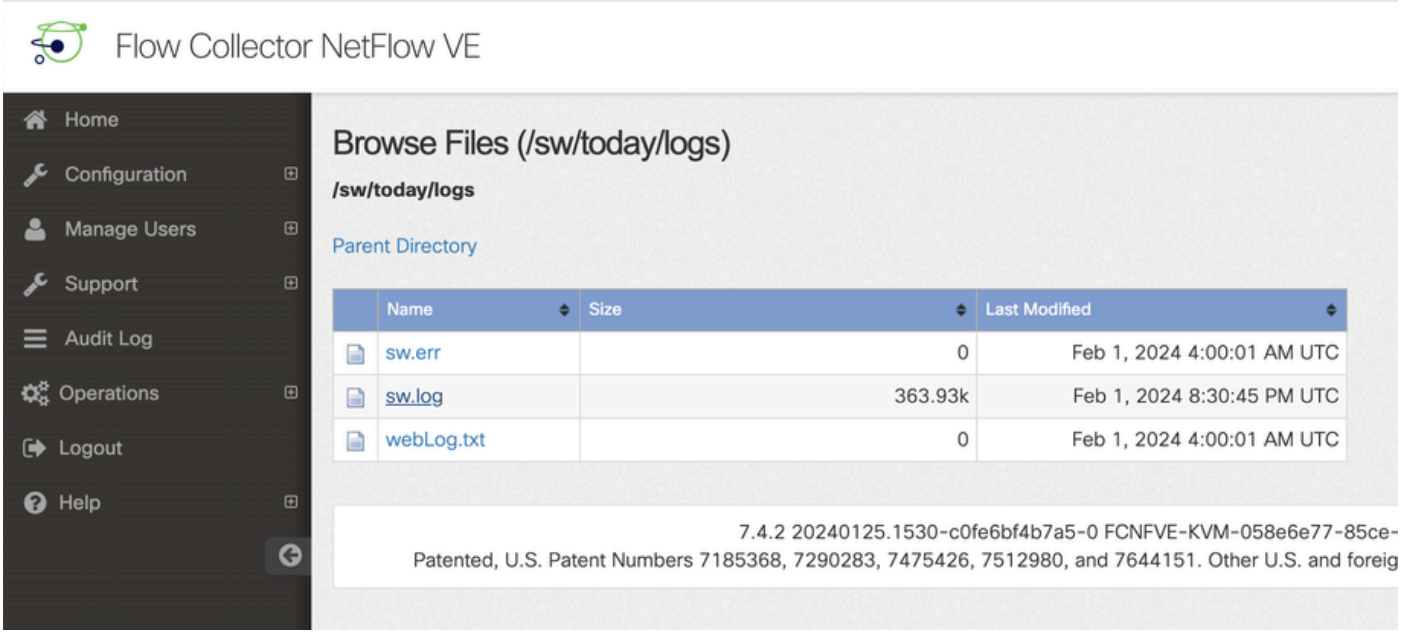
Cliquez sur aujourd'hui



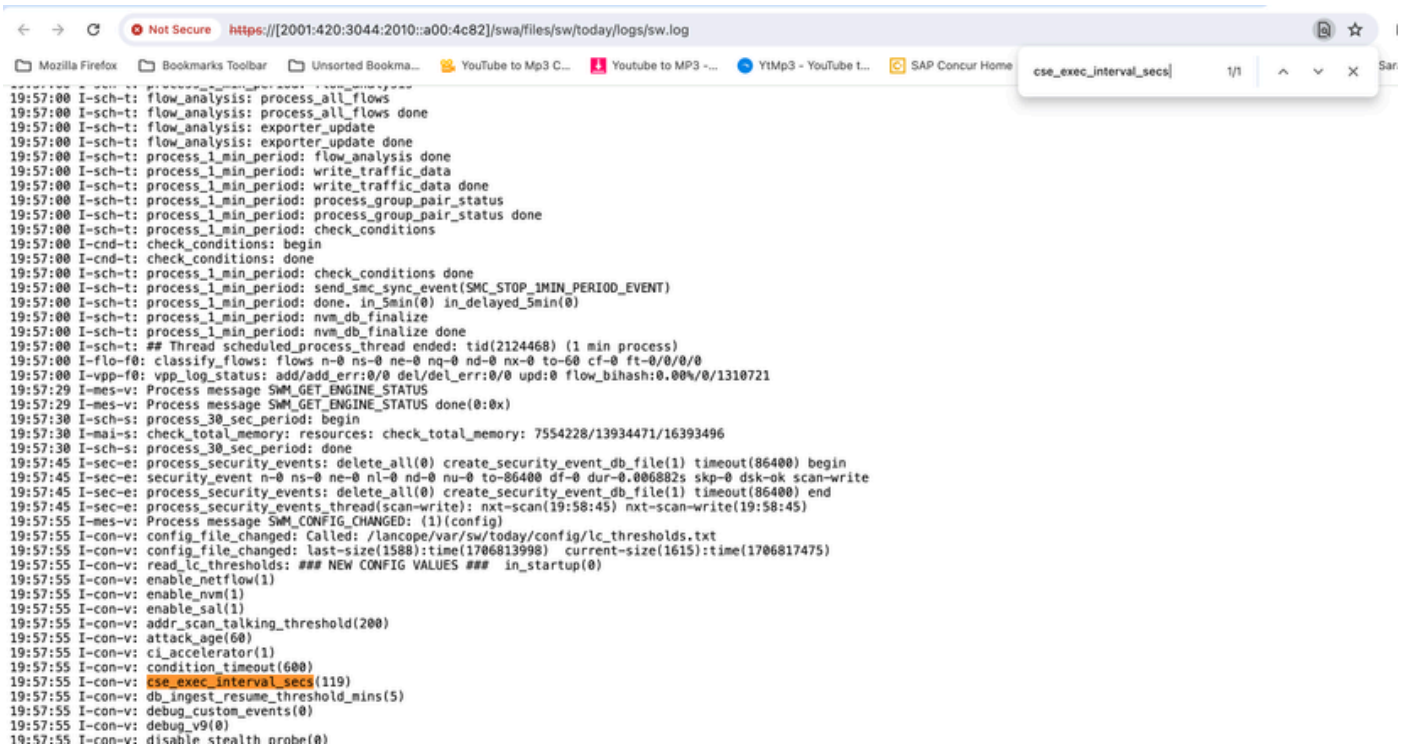
Cliquez sur logs.



Cliquez sur sw.log



Effectuez une recherche dans la page du navigateur, Entrez cse_exec_interval_secs dans la zone de recherche pour trouver le paramètre avancé



Les paramètres avancés acceptés sont répertoriés comme indiqué dans la capture d'écran.

Ceux qui ne sont pas acceptés sont listés comme "ne font pas partie de la configuration d'entrée", dans ce cas c'était à cause d'une faute d'orthographe du paramètre par l'utilisateur. C'est pourquoi il est important de vérifier le journal après avoir fait de telles modifications de configuration.

```
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)
```

Félicitations !

Vous venez d'entrer un nouveau paramètre avancé et de valider son acceptation par le moteur.

Maintenant, la fonctionnalité est activée pour exécuter la logique CSE sur les flux environ toutes les 2 minutes après que le flux atteigne la valeur early_check_age qui est par défaut de 160 secondes.

Si les règles CSE impliquent l'accumulation du nombre d'octets dans le temps, cette fonctionnalité améliore le moment auquel les CSE se déclenchent sur les flux qui correspondent aux critères que vous avez définis.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.