

# 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 d'UC. Les instructions vous guident tout au long de l'analyse du contenu du fichier `sw.log` sur le moteur du 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 l-flo-f0: classify_flows: flows n-1744317 ns-178613 ne-188095 nq-0 nd-0 nx-0 to-300 cf-21 ft-126473/792802/940383/14216/
```

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

```
20:45:22 l-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 l-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 l-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 l-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 il 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.

# **SECURE** Network Analytics

Flow Collector NetFlow VE  
7.4.2

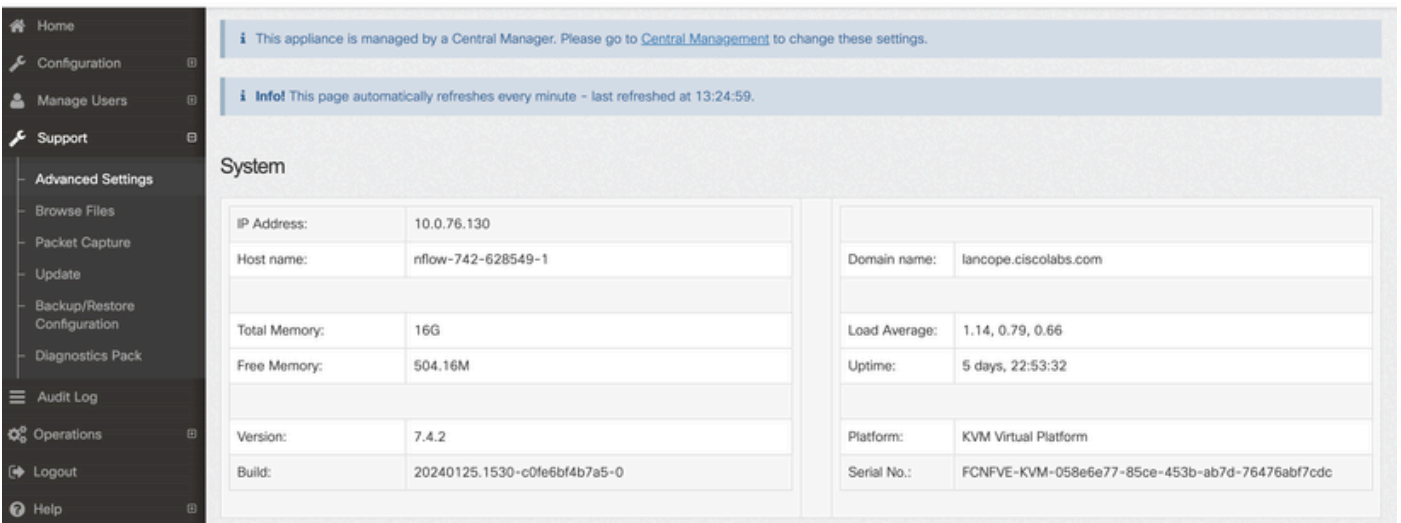
Username:

Password:

Login >>

Accédez à Support -> Advanced Settings

 Flow Collector NetFlow VE



The screenshot shows the Cisco Secure Network Analytics Flow Collector NetFlow VE interface. The left sidebar contains a navigation menu with the following items: Home, Configuration, Manage Users, Support, Advanced Settings (highlighted), Browse Files, Packet Capture, Update, Backup/Restore Configuration, Diagnostics Pack, Audit Log, Operations, Logout, and Help. The main content area displays system information under the heading "System".

System

IP Address:	10.0.76.130
Host name:	nflow-742-628549-1
Total Memory:	16G
Free Memory:	504.16M
Version:	7.4.2
Build:	20240125.1530-c0fe6bf4b7a5-0
Domain name:	lancope.ciscolabs.com
Load Average:	1.14, 0.79, 0.66
Uptime:	5 days, 22:53:32
Platform:	KVM Virtual Platform
Serial No.:	FCNFVE-KVM-058e6e77-85ce-453b-ab7d-76476abf7cdc

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

verbose_debug	<input type="text" value="0"/>	<input type="checkbox"/>
worm_minimum_bytes	<input type="text" value="200"/>	<input type="checkbox"/>
worm_minimum_bytes_per_pkt	<input type="text" value="12"/>	<input type="checkbox"/>
worm_pkt_threshold	<input type="text" value="4"/>	<input type="checkbox"/>
worm_subnet_threshold	<input type="text" value="8"/>	<input type="checkbox"/>
zmq_high_water_mark	<input type="text" value="1048576"/>	<input type="checkbox"/>

Add New Option:  Option value:

Dans la zone Ajouter une nouvelle option : modifier, entrez cse\_exec\_interval\_secs et dans la zone Valeur de l'option : modifier, entrez 119. La modification de ces zones active le bouton Ajouter. Appuyez sur le bouton Ajouter après avoir entré cse\_exec\_interval\_secs dans la zone Ajouter une nouvelle option : modifier et 119 dans la zone Valeur de l'option : modifier.

Add New Option:  Option value:

Les zones d'édition Add New Option: et Option value: s'effacent en préparation d'une autre entrée dans le cas où plusieurs nouveaux paramètres avancés vont être 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.

zmq_high_water_mark	<input type="text" value="1048576"/>	<input type="checkbox"/>
cse_exec_interval_secs	<input type="text" value="119"/>	<input type="checkbox"/>

Add New Option:  Option value:

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 dans la zone Ajouter une nouvelle option : modifier, puis le bouton Appliquer devient activé. Lorsque cette fenêtre contextuelle s'affiche, appuyez sur le bouton OK pour envoyer les nouveaux paramètres avancés et la valeur.

[2001:420:3044:2010::a00:4c82] says

Warning:

These settings should only be changed under direct instruction from Cisco Support.

Misconfiguration may seriously impact the performance of this Secure Network Analytics appliance and/or the loss of monitoring capabilities.

Are you sure you want to continue?

Cancel

OK

## 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.





- 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

Cliquez sur aujourd'hui

- [Home](#)
- [Configuration](#)
- [Manage Users](#)
- [Support](#)
- [Audit Log](#)
- [Operations](#)
- [Logout](#)
- [Help](#)

## Browse Files (/sw)

**/sw**

Parent Directory

Name	Size	Last Modified
<a href="#">26</a>	-	Jan 27, 2024 4:00:00 AM UTC
<a href="#">27</a>	-	Jan 28, 2024 4:00:01 AM UTC
<a href="#">28</a>	-	Jan 29, 2024 4:00:00 AM UTC
<a href="#">29</a>	-	Jan 30, 2024 4:00:00 AM UTC
<a href="#">30</a>	-	Jan 31, 2024 4:00:00 AM UTC
<a href="#">31</a>	-	Feb 1, 2024 4:00:01 AM UTC
<a href="#">data</a>	-	Feb 1, 2024 7:36:49 PM UTC
<a href="#">tmp</a>	-	Feb 1, 2024 8:23:00 PM UTC
<a href="#">tmp_db</a>	-	Feb 1, 2024 6:12:45 AM UTC
<a href="#">today</a>	-	Jan 25, 2024 3:58:00 PM UTC

Cliquez sur logs.

← → ↻ Not Secure [https://\[2001:420:3044:2010::a00:4c82\]/swa/files/sw/today](https://[2001:420:3044:2010::a00:4c82]/swa/files/sw/today)

📁 Mozilla Firefox
📁 Bookmarks Toolbar
📁 Unsorted Bookma...
📁 YouTube to Mp3 C...
📁 Youtube to MP3 -...
📁 YtMp3 - YouTube t...
📁 SAP C...

- [Home](#)
- [Configuration](#)
- [Manage Users](#)
- [Support](#)
- [Audit Log](#)
- [Operations](#)
- [Logout](#)
- [Help](#)

## Browse Files (/sw/today)

**/sw/today**

Parent Directory

Name	Size	Last Modified
<a href="#">config</a>	-	Feb 1, 2024 8:27:00 PM UTC
<a href="#">data</a>	-	Feb 1, 2024 4:00:01 AM UTC
<a href="#">logs</a>	-	Feb 1, 2024 7:36:36 PM UTC

7.4.2 20240125.1530-c0fe6bf4b7a5-0 FCNFVE-KVM-058e6e77-85  
 Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and for

Cliquez sur sw.log

**Browse Files (/sw/today/logs)**

**/sw/today/logs**

Parent Directory

Name	Size	Last Modified
<a href="#">sw.err</a>	0	Feb 1, 2024 4:00:01 AM UTC
<a href="#">sw.log</a>	363.93k	Feb 1, 2024 8:30:45 PM UTC
<a href="#">webLog.txt</a>	0	Feb 1, 2024 4:00:01 AM UTC

7.4.2 20240125.1530-c0fe6bf4b7a5-0 FCNFVE-KVM-058e6e77-85ce-  
Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign

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

Not Secure [https://\[2001:420:3044:2010::a00:4c82\]/swa/files/sw/today/logs/sw.log](https://[2001:420:3044:2010::a00:4c82]/swa/files/sw/today/logs/sw.log)

Mozilla Firefox Bookmarks Toolbar Unsorted Bookma... YouTube to Mp3 C... YouTube to MP3 ... Y1mp3 - YouTube L... SAP Concur Home

`cse_exec_interval_secs` 1/1

```

19:57:00 I-sch-t: flow_analysis: process_all_flows
19:57:00 I-sch-t: flow_analysis: process_all_flows done
19:57:00 I-sch-t: flow_analysis: exporter_update
19:57:00 I-sch-t: flow_analysis: exporter_update done
19:57:00 I-sch-t: process_1_min_period: flow_analysis done
19:57:00 I-sch-t: process_1_min_period: write_traffic_data
19:57:00 I-sch-t: process_1_min_period: write_traffic_data done
19:57:00 I-sch-t: process_1_min_period: process_group_pair_status
19:57:00 I-sch-t: process_1_min_period: process_group_pair_status done
19:57:00 I-sch-t: process_1_min_period: check_conditions
19:57:00 I-cnd-t: check_conditions: begin
19:57:00 I-cnd-t: check_conditions: done
19:57:00 I-sch-t: process_1_min_period: check_conditions done
19:57:00 I-sch-t: process_1_min_period: send_sm_sync_event(SMC_STOP_1MIN_PERIOD_EVENT)
19:57:00 I-sch-t: process_1_min_period: done. in_5min(0) in_delayed_5min(0)
19:57:00 I-sch-t: process_1_min_period: nvm_db_finalize
19:57:00 I-sch-t: process_1_min_period: nvm_db_finalize done
19:57:00 I-sch-t: ## Thread scheduled_process_thread ended: tid(2124468) (1 min process)
19:57:00 I-flt-f0: classify_flows: flows n-0 ns-0 ne-0 nq-0 nd-0 nx-0 to-60 cf-0 ft-0/0/0
19:57:00 I-vpp-f0: vpp_log_status: add/add_err:0/0 del/del_err:0/0 upd:0 flow_bihash:0.00%/0/1310721
19:57:29 I-mes-v: Process message SWM_GET_ENGINE_STATUS
19:57:29 I-mes-v: Process message SWM_GET_ENGINE_STATUS done(0:0x)
19:57:30 I-sch-s: process_30_sec_period: begin
19:57:30 I-mal-s: check_total_memory: resources: check_total_memory: 7554228/13934471/16393496
19:57:30 I-sch-s: process_30_sec_period: done
19:57:45 I-sec-e: process_security_events: delete_all(0) create_security_event_db_file(1) timeout(86400) begin
19:57:45 I-sec-e: security_event n-0 ns-0 ne-0 nl-0 nd-0 nu-0 to-86400 df-0 dur-0.006882s skp-0 dsk-ok scan-write
19:57:45 I-sec-e: process_security_events: delete_all(0) create_security_event_db_file(1) timeout(86400) end
19:57:45 I-sec-e: process_security_events_thread(scan-write): next-scan(19:58:45) next-scan-write(19:58:45)
19:57:55 I-mes-v: Process message SWM_CONFIG_CHANGED: (1)(config)
19:57:55 I-con-v: config_file_changed: Called: /lancopce/var/sw/today/config/lc_thresholds.txt
19:57:55 I-con-v: config_file_changed: last-size(1588):time(1706813998) current-size(1615):time(1706817475)
19:57:55 I-con-v: read_lc_thresholds: ### NEW CONFIG VALUES ### in_startup(0)
19:57:55 I-con-v: enable_netflow(1)
19:57:55 I-con-v: enable_nvm(1)
19:57:55 I-con-v: enable_sal(1)
19:57:55 I-con-v: addr_scan_talking_threshold(200)
19:57:55 I-con-v: attack_age(60)
19:57:55 I-con-v: ci_accelerator(1)
19:57:55 I-con-v: condition_timeout(600)
19:57:55 I-con-v: cse_exec_interval_secs (119)
19:57:55 I-con-v: db_ingest_resume_threshold_mins(5)
19:57:55 I-con-v: debug_custom_events(0)
19:57:55 I-con-v: debug_v9(0)
19:57:55 I-con-v: disable_stealth_probe(0)
    
```

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

Ceux qui ne sont pas acceptés sont répertoriés comme "ne font pas partie de la configuration d'entrée", dans ce cas, c'était en raison de l'orthographe erronée du paramètre par l'utilisateur. C'est pourquoi il est important de vérifier le journal après avoir effectué 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.