

Configurar Comportamento de Disparo de Evento de Segurança Personalizado do Mecanismo do Coletor de Fluxo Avançado

Contents

[Introdução](#)

[Background](#)

[Depuração de Evento de Segurança Personalizada](#)

[Comportamento do coletor de fluxo padrão](#)

[A configuração avançada cse_exec_interval_secs](#)

[Impactos no desempenho](#)

[Medindo a duração do segmento classify_flows](#)

[Status do Mecanismo no Período de Desempenho](#)

[SFI - índice de fluxo estático](#)

[Configurando](#)

[Confirmando a alteração](#)

[Parabéns!](#)

Introdução

Este documento descreve duas configurações avançadas do coletor de fluxo que podem alterar a forma como o SNA Flow Collector dispara Eventos de Segurança Personalizados (CSEs).

Background

A configuração avançada do coletor de fluxo `early_check_age` legado, junto com a nova configuração avançada do coletor de fluxo `cse_exec_interval_secs` determinam a maneira como os Eventos de Segurança Personalizados são acionados pelo mecanismo do coletor de fluxo. O coletor de fluxo é o primeiro dispositivo na arquitetura do sistema SNA a ver o fluxo na rede e, portanto, o mecanismo do coletor de fluxo é responsável por monitorar as características do(s) fluxo(s) no cache de fluxo e determinar se o fluxo atende aos critérios configurados de um determinado evento de segurança personalizado. No entanto, essas configurações avançadas do coletor de fluxo NÃO alteram as características de acionamento de nenhum dos eventos de segurança principal embutidos.

Depuração de Evento de Segurança Personalizada

Na versão 7.5.0 e posterior do SNA, a configuração avançada do coletor de fluxo `debug_custom_events` foi aprimorada para fornecer diferentes níveis de depuração

- `debug_custom_events 1` (menor depuração - destinado a ser capaz de ser executado em produção e fornecer mais informações sobre os fluxos exatos que estão gerando CSEs)
- `debug_custom_events 2` (mais depurações)
- `debug_custom_events 3` (depuração mais detalhada)

Comportamento do coletor de fluxo padrão

Por padrão, a configuração avançada do coletor de fluxo `early_check_age` está configurada como 160 segundos. Isso significa que o mecanismo do coletor de fluxo espera um mínimo de 160 segundos em um fluxo antes de verificar se esse fluxo corresponde a um evento de segurança personalizado configurado. Por padrão, essa verificação não é feita novamente até que o fluxo termine.

Esse valor de verificação antecipada de 160 segundos foi escolhido especificamente porque, se estiver usando as melhores práticas, os exportadores de telemetria devem ser configurados para enviar telemetria a cada 60 segundos. Esse valor padrão permite tempo suficiente em um ambiente típico para que o coletor de fluxo veja as informações de fluxo relacionadas aos dois lados de uma determinada conversa/fluxo. Por esse motivo, a `early_check_age` não é predefinida na lista de configurações avançadas. Isso ocorre por projeto, e você não deve alterar esse valor sem consultar primeiro o suporte/engenharia. Esse projeto inicial, no entanto, não tem um desempenho favorável ao considerar características de fluxo longas e um pouco silenciosas associadas à configuração do evento de segurança personalizado que envolve o acúmulo de contagens de bytes ou pacotes. Por esse motivo, foi criado o parâmetro de configuração avançado `cse_exec_interval_secs`.

A configuração avançada `cse_exec_interval_secs`

Disponibilizado no 7.4.2, a adição da configuração avançada do coletor de fluxo `cse_exec_interval_secs` agora possibilita instruir o mecanismo a verificar periodicamente os fluxos em seu cache de fluxo em relação aos eventos de segurança personalizados configurados. Essa configuração avançada é particularmente útil no caso de fluxos longos, em que um determinado fluxo não correspondeu aos critérios de um CSEs no padrão de 160 segundos `early_check_age`, mas ultrapassa esse limite posteriormente no fluxo. Sem essa configuração avançada, o evento de segurança personalizado não será acionado até que o fluxo termine. Às vezes, isso pode acontecer dias depois.

Impactos no desempenho

A execução desses critérios de intervalo do CSE verifica os fluxos mais vezes na vida útil do fluxo do que o que os padrões definem exige mais CPU. As instruções orientam você na investigação do conteúdo do arquivo `sw.log` no mecanismo do coletor de fluxo para determinar uma linha de base de desempenho antes de ativar o parâmetro `cse_exec_interval_secs`. Se você estiver considerando habilitar essa configuração avançada e quiser que o TAC ajude a confirmar a integridade do coletor de fluxo na preparação para essa alteração, isso pode ser feito abrindo um caso de suporte e anexando um pacote de diagnóstico do coletor de fluxo ao SR.

Medindo a duração do thread classify_flows

Uma medida rápida de impacto no desempenho que você pode fazer é investigar o sw.log a partir de hoje e comparar os números listados após as entradas de "cf-"log antes da ativação da configuração com os números após a configuração ser aplicada.

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

```
20:43:21 l-flo-f0: classify_flows: fluxos 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: fluxos 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: fluxos 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: fluxos n-1750066 ns-189197 ne-165940 nq-0 nd-0 nx-0 a 300 cf-20 ft-122563/779792/944192/15154
```

```
20:44:21 l-flo-f5: classify_flows: fluxos 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: fluxos n-1763952 ns-191342 ne-169518 nq-0 nd-0 nx-0 a 300 cf-20 ft-122782/786822/955997/15175
```

```
20:44:21 l-flo-f7: classify_flows: fluxos 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: fluxos 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: fluxos 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: fluxos 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: fluxos 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: fluxos n-1774883 ns-177085 ne-149715 nq-0 nd-0 nx-0 a 300 cf-22 ft-129067/764272/962000/15090
```

```
20:45:22 l-flo-f5: classify_flows: fluxos 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: fluxos n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0 a 300 cf-22 ft-129255/770212/970360/15129
```

As entradas cf significam "Classificar fluxos". Isso representa o número de segundos que o thread levou para fazer sua passagem pela seção do Cache de Fluxo pela qual é responsável. Ele está nos threads "Classificar fluxos" onde os CSEs são aplicados contra os fluxos. Se você observar o aumento desses números após ativar o recurso, essa será uma boa medida do impacto geral sobre o desempenho.

É esperado um aumento após a adição dessa configuração de intervalo avançada, mas se esse número se aproximar de 60, remova a configuração, pois o impacto é muito grande. Um aumento de alguns segundos seria de esperar e é considerado razoável.

Status do Mecanismo no Período de Desempenho

Outra medida de desempenho "antes vs depois" que você pode fazer é observar as seções "Performance Period" no arquivo sw.log que são registradas a cada 5 minutos para medir o impacto da configuração no processamento de fluxo. Você pode procurar esses blocos usando o grep também. Se o Engine estiver sobrecarregado, esta verificação de intervalo de configuração avançada deverá ser desativada.

```
/lancope/var/sw/today/logs/ grep -A3 "Período de Desempenho" sw.log
```

Tome nota de qualquer estado diferente de "Estado do motor normal".

Um status como "Taxa de entrada de status do mecanismo muito alta" indicaria que o thread classify_flows está consumindo muita CPU.

SFI - índice de fluxo estático

Significa que os threads de classificação não foram capazes de concluir suas passagens pelo cache de fluxo: Representa o "Índice de Fluxo Estático" e indica uma luta nos threads de classificação de fluxos. Não é um desastre por si só, mas indica que o motor está começando a atingir o teto e que o desempenho está começando a degradar-se nos níveis atuais de cf.

```
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%)

Configurando

Abra um navegador da Web e navegue diretamente para o IP do dispositivo Flow Collector. Faça login como o usuário administrador local.

SECURE Network Analytics

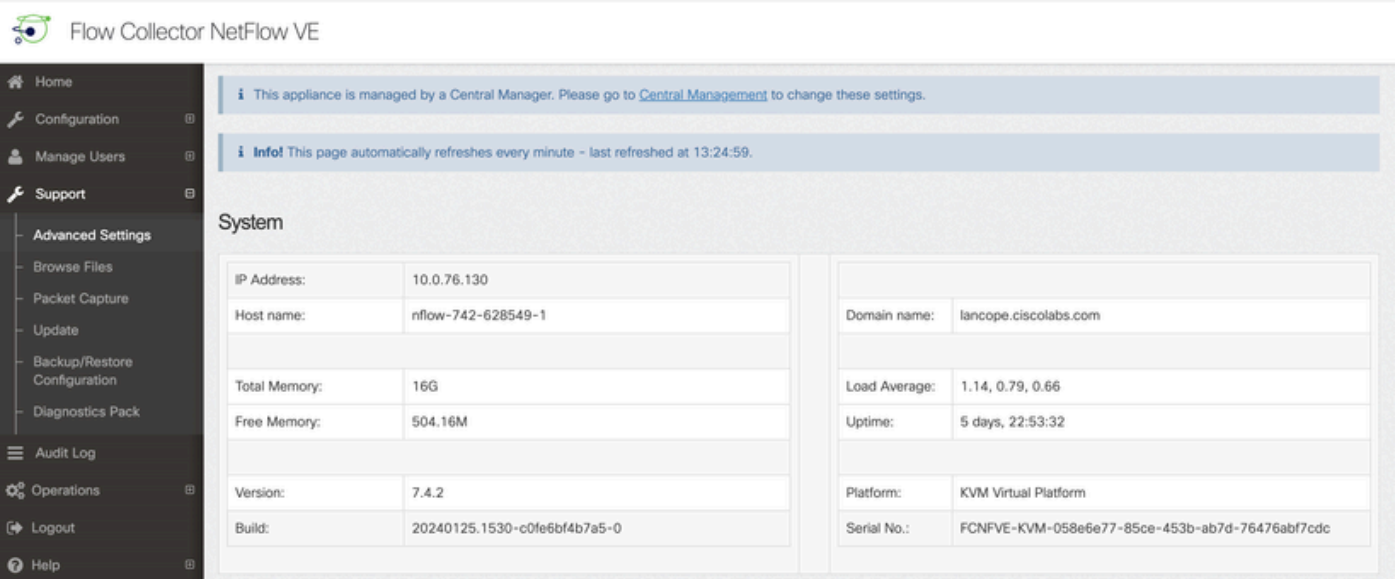
Flow Collector NetFlow VE
7.4.2

Username:

Password:

Login >>

Navegue até Suporte -> Configurações avançadas



Flow Collector NetFlow VE

Home Configuration Manage Users Support

Advanced Settings
Browse Files
Packet Capture
Update
Backup/Restore Configuration
Diagnostics Pack

Audit Log
Operations
Logout
Help

This appliance is managed by a Central Manager. Please go to [Central Management](#) to change these settings.

Info! This page automatically refreshes every minute - last refreshed at 13:24:59.

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

Desça até a tela Advanced Setting (Configuração avançada) para expor a caixa de configuração "Add New Option" (Adicionar nova opção) na parte inferior da lista

verbose_logging	<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:

Na caixa de edição Add New Option: digite cse_exec_interval_secs e, na caixa de edição Option value:, digite 119. A edição dessas caixas habilita o botão Adicionar. Pressione o botão Adicionar depois de inserir cse_exec_interval_secs na caixa de edição Adicionar nova opção: e 119 na caixa de edição Valor da opção: .

Add New Option: Option value:

As caixas de edição Add New Option: e Option value: se apagam em preparação para outra entrada no caso de serem inseridas várias Advanced Settings novas. As Configurações avançadas recém-adicionadas são empilhadas na parte inferior da lista à medida que são adicionadas. Isso dá ao usuário uma chance de inspecionar a entrada. A ortografia exata da Configuração avançada é importante, assim como o caso. Todas as configurações avançadas estão em minúsculas.

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:

Agora que a Configuração avançada foi inserida corretamente, pressione o botão Aplicar. Observe que, às vezes, o botão Apply não está ativado. Para ativá-lo, clique na caixa de edição Add New Option: e o botão Apply será ativado para clicar. Quando este pop-up for exibido, pressione o botão OK para enviar o novo valor e a nova Configuração avançada.

[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

Confirmando a alteração

Esta validação final é a mais importante. Clique no menu Suporte novamente e escolha Procurar arquivos.

Isso o leva ao sistema de arquivos no FC. Clique em sw.

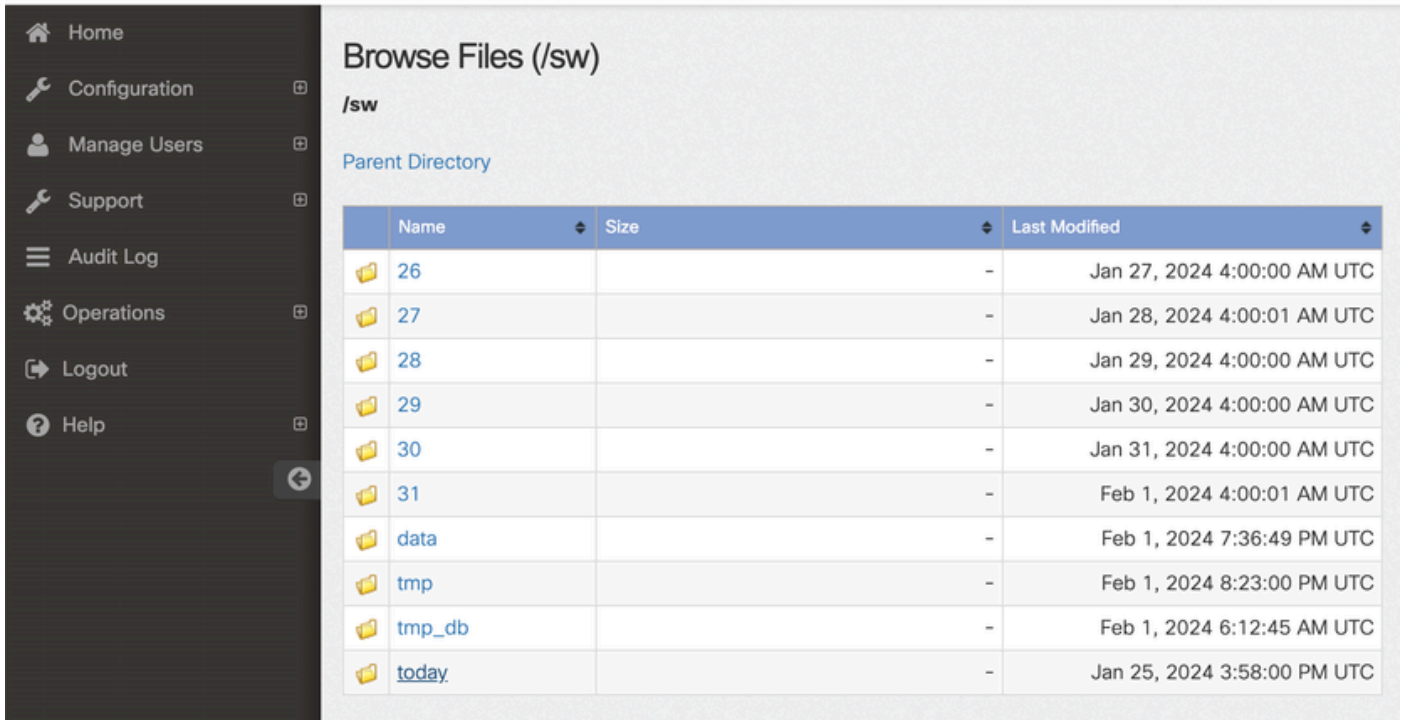


- Home
- Configuration
- Manage Users
- Support
- Audit Log
- Operations
- Logout
- Help

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

Clique hoje



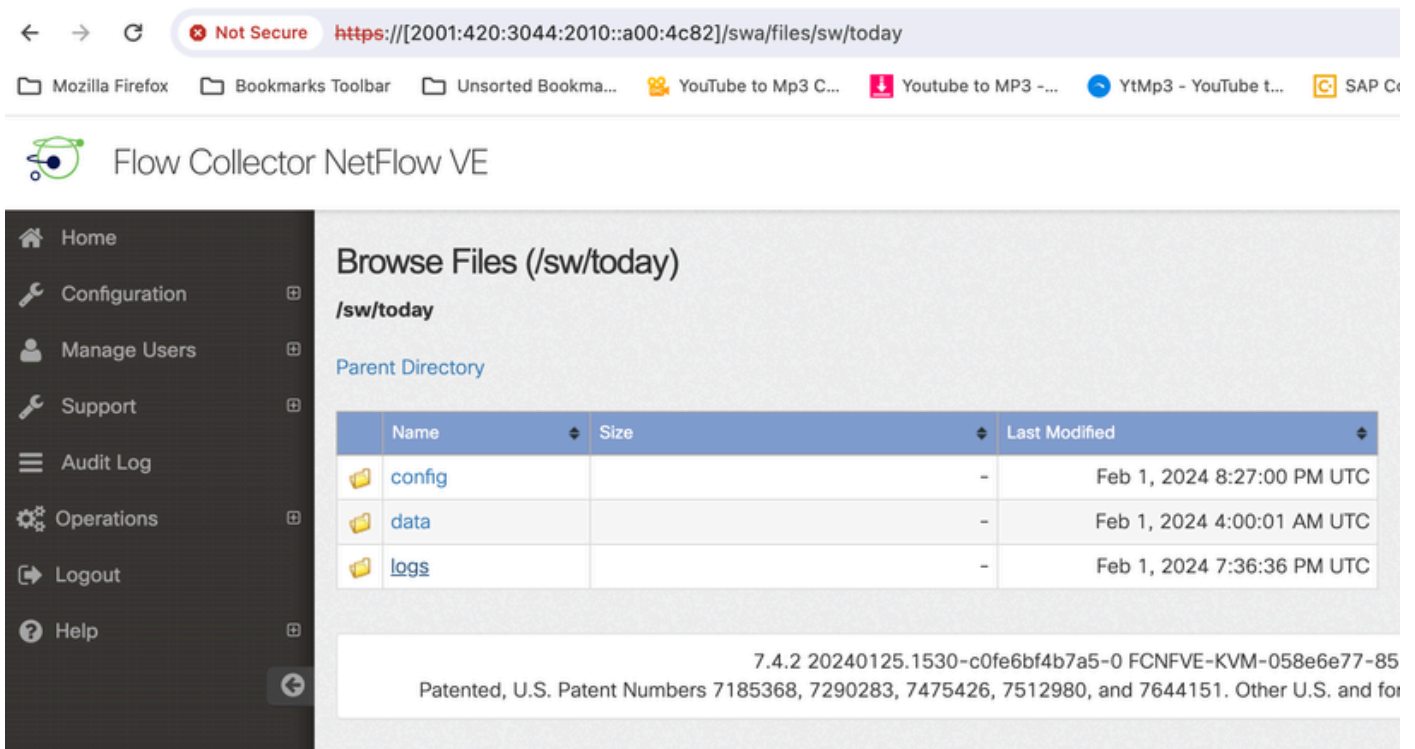
Browse Files (/sw)

/sw

Parent Directory

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

Clique em 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 Co

Flow Collector NetFlow VE

Browse Files (/sw/today)

/sw/today

Parent Directory

Name	Size	Last Modified
config	-	Feb 1, 2024 8:27:00 PM UTC
data	-	Feb 1, 2024 4:00:01 AM UTC
logs	-	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

Clique em sw.log

Browse Files (/sw/today/logs)

/sw/today/logs

Parent Directory

Name	Size	Last Modified
sw.err	0	Feb 1, 2024 4:00:01 AM UTC
sw.log	363.93k	Feb 1, 2024 8:30:45 PM UTC
webLog.txt	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

Faça uma pesquisa na página do navegador, insira `cse_exec_interval_secs` na caixa de pesquisa para localizar a Configuração avançada

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

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_smc_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
 19:57:30 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_arobe(0)

As configurações avançadas aceitas são listadas conforme mostrado na captura de tela.

Os que não foram aceitos são listados como "não fazem parte da configuração de entrada", nesse caso, foi devido ao erro de ortografia do usuário na configuração. É por isso que é importante verificar o registro depois de fazer essas alterações de configuração.

```
-----  
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)  
-----
```

Parabéns!

Você acabou de inserir uma nova Configuração avançada e validar sua aceitação pelo mecanismo.

Agora, o recurso está habilitado para executar a lógica do CSE nos fluxos aproximadamente a cada 2 minutos depois que o fluxo atingir a `early_check_age` que assume como padrão o 160 segundos.

Se as regras do CSE envolverem o acúmulo de contagens de bytes ao longo do tempo, esse recurso melhora a temporização na qual os CSEs disparam os fluxos que correspondem aos critérios definidos.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.