

高度なフローコレクタエンジンのカスタムセキュリティイベント起動動作の構成

内容

[はじめに](#)

[背景](#)

[カスタムセキュリティイベントデバッグ](#)

[デフォルトのフローコレクタの動作](#)

[cse_exec_interval_secsの詳細設定](#)

[パフォーマンスへの影響](#)

[classify_flowsスレッドの持続時間の測定](#)

[パフォーマンス期間中のエンジンステータス](#)

[SFI : スタティックフローインデックス](#)

[Fast SSID Changing の設定](#)

[変更の確認](#)

[おめでとうございます。](#)

はじめに

このドキュメントでは、SNAフローコレクタがカスタムセキュリティイベント(CSE)を起動する方法を変更できる2つのフローコレクタの詳細設定について説明します。

背景

フローコレクタエンジンによって起動されるカスタムセキュリティイベントの方法は、新しいcse_exec_interval_secsフローコレクタの高度な設定であるearly_check_ageフローコレクタの従来の高度な設定によって決まります。 フローコレクタは、SNAシステムアーキテクチャ内の最初のアプライアンスで、ネットワーク上のフローを参照します。したがって、フローコレクタエンジンは、フローキャッシュ内にあるフローの特性を監視し、そのフローが特定のカスタムセキュリティイベントに設定された基準を満たしているかどうかを判断する役割を担います。 ただし、これらのフローコレクタの詳細設定では、組み込み型のコアセキュリティイベントの起動特性は変更されません。

カスタムセキュリティイベントデバッグ

バージョン7.5.0以降のSNAでは、debug_custom_eventsフローコレクタの詳細設定が拡張され、異なるレベルのデバッグが提供されるようになりました

- debug_custom_events 1 (最小限のデバッグ : 実稼働環境で実行し、CSEを生成している正確なフローをより詳細に把握できるようにすることを目的としています)
- debug_custom_events 2 (デバッグの詳細)

- debug_custom_events 3 (最も詳細なデバッグ)

デフォルトのフローコレクタの動作

デフォルトでは、フローコレクタのearly_check_age高度な設定は160秒に設定されています。つまり、フローコレクタエンジンは、フローに160秒以上待機してから、そのフローが設定されたカスタムセキュリティイベントに一致するかどうかを確認します。デフォルトでは、このチェックはフローが終了するまで再度行われません。

この160秒の早期チェック値が特に選択されたのは、ベストプラクティスを使用する場合、テレメトリエクスポータはテレメトリを60秒ごとに送信するように設定する必要があるためです。このデフォルト値を使用すると、通常的环境では、フローコレクタが特定のカンバセーション/フローの両側に関連するフロー情報を確認するのに十分な時間を確保できます。このため、early_check_ageは高度な設定のリストで事前に定義されていません。これは設計上の問題であり、最初にサポートやエンジニアリングに相談しない限り、この値を変更することはできません。ただし、この初期設計は、バイト数またはパケット数の累積を伴うカスタムセキュリティイベント設定と組み合わせて、長くてやや静かなフロー特性を考慮する場合には適していません。これが、cse_exec_interval_secs高度な設定パラメータを作成する理由です(下記の例を参照)。

cse_exec_interval_secsの詳細設定

7.4.2で使用可能になったため、cse_exec_interval_secsフローコレクタの高度な設定が追加され、フローキャッシュ内のフローを、設定されているカスタムセキュリティイベントと定期的に照合するようにエンジンに指示できるようになりました。この高度な設定は、特定のフローがデフォルトの160秒のearly_check_ageでCSE基準に一致しなかったが、そのフローの後半でしきい値を超える長いフローの場合に特に役立ちます。この詳細設定を使用しないと、フローが終了するまでカスタムセキュリティイベントは発生しません。数日後に発生する場合があります。

パフォーマンスへの影響

これらの間隔CSE基準チェックをフローの存続期間に実行すると、デフォルト定義よりも多くの時間フローでCPUが必要になります。この手順では、cse_exec_interval_secsパラメータを有効にする前に、フローコレクタエンジンのsw.logファイルの内容を調査してパフォーマンスベースラインを決定します。この高度な設定の有効化を検討していて、この変更に合わせてTACによるフローコレクタの健全性の確認を希望する場合は、サポートケースをオープンし、フローコレクタ診断パックをSRに添付してください。

classify_flowsスレッドの持続時間の測定

パフォーマンスへの影響を簡単に測定するには、今日のsw.logを調べ、設定をアクティブ化する前の「cf-」ログエントリの後に表示される数値を、設定の適用後の数値と比較します。

```
/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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows 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:flows n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0 to-300 cf-22 ft-129255/770212/970360/15129

cfエントリは「Classify Flows」を表します。これは、スレッドが担当するフローキャッシュのセクションを通過するのに要した秒数を表します。CSEがフローに適用されるのは、「フローの分類」スレッドです。この数値が機能を有効にした後で上昇している場合は、パフォーマンスに対する全体的な影響を測定するのに適しています。

この高度な間隔設定を追加した後の上昇が予想されますが、この数値が60に近づくと、影響が大きすぎるため設定を削除します。数秒増加することが予想され、妥当と考えられます。

パフォーマンス期間中のエンジンステータス

測定の前後にパフォーマンスを測定するもう1つの方法として、sw.logファイルの「Performance

Period」セクションを確認する方法があります。このセクションには5分ごとにログが記録され、この設定がフロー処理に与える影響を調べます。grepを使用して、これらのブロックを検索することもできます。エンジンが過負荷の場合は、この高度な設定間隔チェックを無効にする必要があります。

```
/lancope/var/sw/today/logs/ grep -A3 「Performance Period」 sw.log
```

「Engine status Normal」以外のステータスに注意します。

「Engine status Input rate too high」などのステータスは、classify_flowsスレッドがCPUを過度に消費していることを示します。

SFI : スタティックフローインデックス

分類スレッドがフローキャッシュ内でパスを完了できなかったことを意味します。これは「静的フローインデックス」を表し、分類フロースレッドの処理に問題があることを示します。それ自体は災害ではありませんが、エンジンが天井に達し始め、現在のcfレベルでパフォーマンスが低下し始めていることを示しています。

```
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 I-flo-f0: classify_flows: sfi:base(0) (1402189 -> 2373792) max(8388607) cod(1) (971602/8388608)----->(11%)
sw.log:16:11:49 I-flo-f6: classify_flows: sfi:base(50331648) (52444661 -> 50483491) max(58720255) cod(1) (6427437/8388608)----->(76%)
sw.log:16:11:49 I-flo-f3: classify_flows: sfi:base(25165824) (25702968 -> 26385879) max(33554431) cod(1) (682910/8388608)----->(8%)
sw.log:16:11:49 I-flo-f1: classify_flows: sfi:base(8388608) (8976309 -> 9662167) max(16777215) cod(1) (685857/8388608)----->(8%)
sw.log:16:11:49 I-flo-f4: classify_flows: sfi:base(33554432) (34064015 -> 34742593) max(41943039) cod(1) (678577/8388608)----->(8%)
sw.log:16:11:50 I-flo-f7: classify_flows: sfi:base(58720256) (59630528 -> 60298366) max(67108863) cod(1) (667837/8388608)----->(7%)
sw.log:16:11:50 I-flo-f2: classify_flows: sfi:base(16777216) (17522620 -> 18202249) max(25165823) cod(1) (679628/8388608)----->(8%)

Fast SSID Changing の設定

Webブラウザを開き、Flow CollectorアプライアンスIPに直接ナビゲートします。 ローカル管理者ユーザとしてログインします。



The image shows a login page for Cisco Secure Network Analytics. The page features the Cisco logo and the text "SECURE Network Analytics". Below the logo, it says "Flow Collector NetFlow VE 7.4.2". There are two input fields: "Username:" and "Password:". A blue button labeled "Login >>" is located at the bottom right of the page.

CISCO SECURE
Network Analytics

Flow Collector NetFlow VE
7.4.2

Username:

Password:

Login >>

Support -> Advanced Settingsの順に移動します

The screenshot shows the 'System' configuration page in the Flow Collector NetFlow VE interface. The left sidebar contains navigation options: Home, Configuration, Manage Users, Support, Advanced Settings, Browse Files, Packet Capture, Update, Backup/Restore Configuration, Diagnostics Pack, Audit Log, Operations, Logout, and Help. The main content area displays system information in two columns. The left column includes IP Address (10.0.76.130), Host name (nflow-742-628549-1), Total Memory (16G), Free Memory (504.16M), Version (7.4.2), and Build (20240125.1530-c0fe6bf4b7a5-0). The right column includes Domain name (lancpe.cisco labs.com), Load Average (1.14, 0.79, 0.66), Uptime (5 days, 22:53:32), Platform (KVM Virtual Platform), and Serial No. (FCNFVE-KVM-058e6e77-85ce-453b-ab7d-76476abf7cdc). A notification bar at the top states: 'This appliance is managed by a Central Manager. Please go to Central Management to change these settings.' and another bar below it says: 'Info! This page automatically refreshes every minute - last refreshed at 13:24:59.'

詳細設定の画面を下にスクロールして、リストの下部にある[新しいオプションの追加]構成ボックスを表示します

This screenshot shows a list of system options with their current values and checkboxes for editing. The options are: worm_minimum_bytes (200), worm_minimum_bytes_per_pkt (12), worm_pkt_threshold (4), worm_subnet_threshold (8), and zmq_high_water_mark (1048576). Below the list is an 'Add New Option' section with two input fields: 'Add New Option:' and 'Option value:'. The 'Add' button is currently disabled. At the bottom of the section are 'Reset' and 'Apply' buttons.

Add New Option:編集ボックスにcse_exec_interval_secsと入力し、Option value:編集ボックスに119と入力します。これらのボックスを編集すると、Addボタンが有効になります。 Add New Option:編集ボックスにcse_exec_interval_secsと入力し、Option Value:編集ボックスに119と入力した後でAddボタンを押します。

This screenshot shows the 'Add New Option' section after the option name and value have been entered. The 'Add New Option:' field contains 'cse_exec_interval_secs' and the 'Option value:' field contains '119'. The 'Add' button is now active (highlighted in blue), and the 'Reset' button is also visible. The 'Apply' button remains at the bottom.

複数の新しい詳細設定を入力する場合に、別の入力に備えて新しいオプションの追加：とオプション値：の編集ボックスがクリアされます。新しく追加された詳細設定は、追加中にリストの一番下に表示されます。これにより、ユーザはエントリを調べることができます。詳細設定の正確なスペルは、大文字と小文字の区別だけでなく重要です。すべての詳細設定は小文字で表記されます。

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:

Advanced Settingが正しく入力されたら、Applyボタンを押します。 Applyボタンが有効になっていない場合があることに注意してください。 これを有効にするには、Add New Option:編集ボックスをクリックし、Applyボタンでクリックできるようにします。 このポップアップが表示されたら、OKボタンを押して新しい詳細設定と値を送信します。

[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?

変更の確認

この最終的な検証が最も重要です。 Supportメニューをもう一度クリックして、Browse Filesを選択します。

これにより、FC上のファイルシステムに移動します。 swをクリックします。

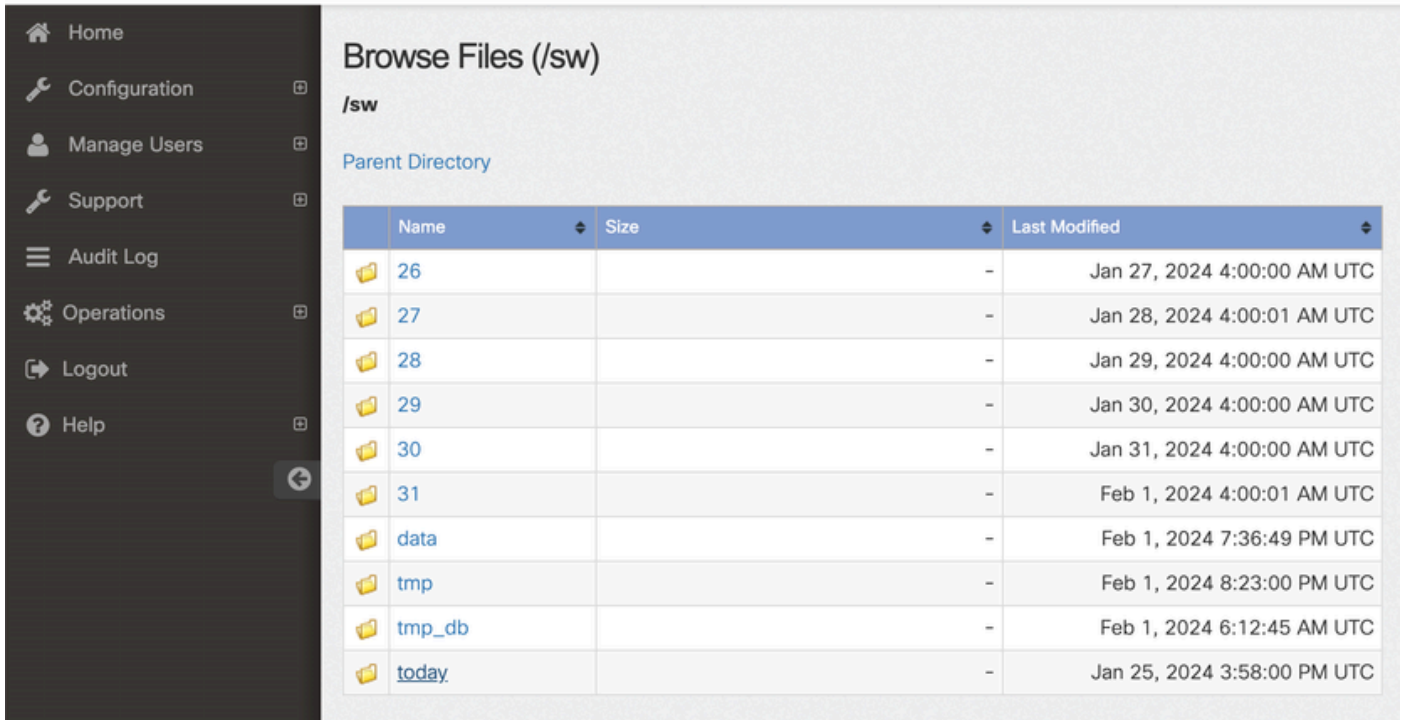


- Home
- Configuration
- Manage Users
- Support
- Audit Log
- Operations
- Logout
- Help

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

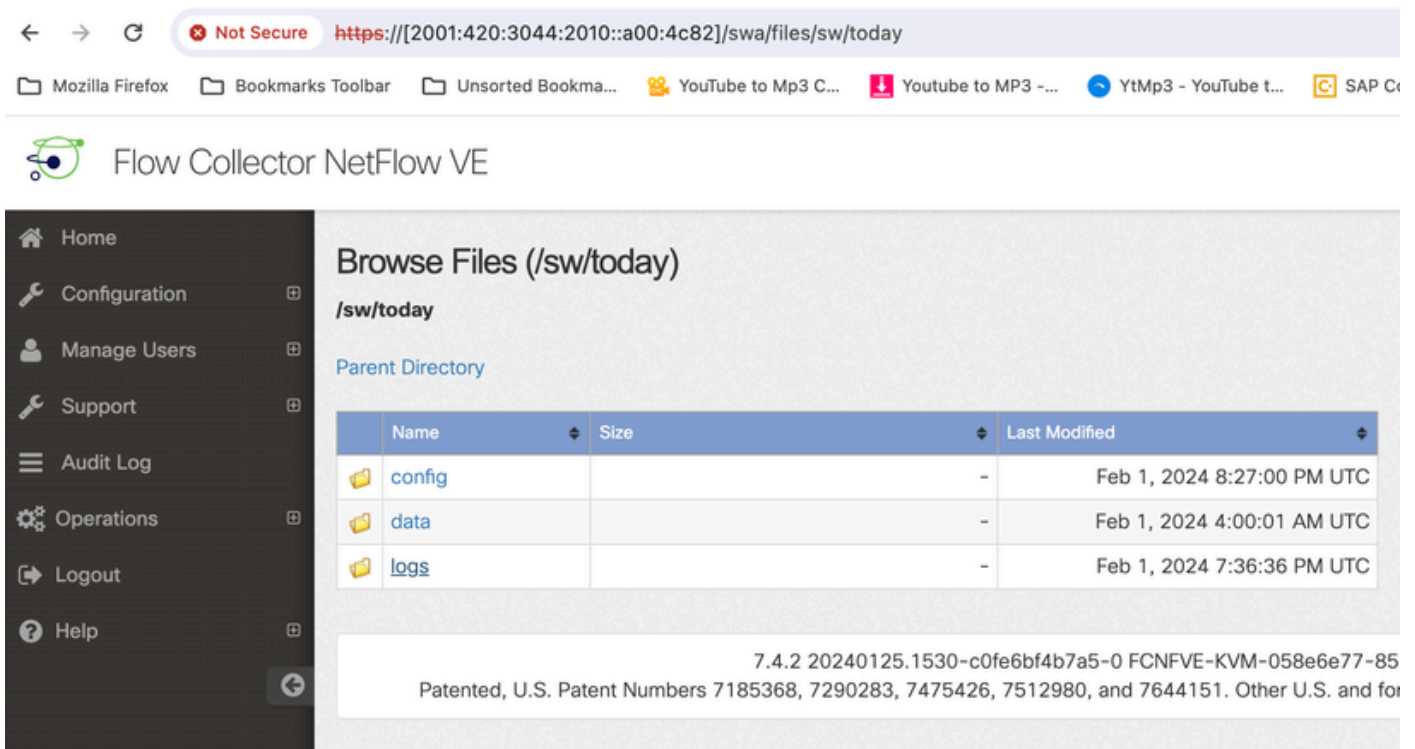
今日をクリック



The screenshot shows the 'Browse Files (/sw)' interface. The left sidebar contains navigation options: Home, Configuration, Manage Users, Support, Audit Log, Operations, Logout, and Help. The main content area displays the directory structure for /sw, including a 'Parent Directory' link and a table of files and folders.

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

logsをクリックします。



The screenshot shows the 'Browse Files (/sw/today)' interface. The left sidebar is the same as in the previous screenshot. The main content area displays the directory structure for /sw/today, including a 'Parent Directory' link and a table of files and folders.

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

sw.logをクリックします

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

ブラウザページで検索を実行し、検索ボックスにcse_exec_interval_secsと入力して詳細設定を見つけてます

Not Secure 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_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
19:57:29 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): nxt-scan(19:58:45) nxt-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: /lancpe/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: begin
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)
    
```

許可された詳細設定は、スクリーンショットのように表示されます。

許可されないものは「not part of input configuration」として表示されます。この場合、ユーザによる設定のスペルミスが原因です。このため、このような設定変更を行った後でログを確認することが重要です。

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

おめでとうございます。

新しい詳細設定を入力し、エンジンによる承認を検証しました。

現在は、フローがearly_check_age(デフォルトは160秒)に達してから約2分ごとにフローでCSEロジックを実行する機能が有効になっています。

CSEルールに時間の経過に伴うバイトカウントの累積が含まれている場合、この機能により、定義した基準に一致するフローでCSEがトリガーするタイミングが改善されます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。