Configura comportamento di attivazione eventi di sicurezza personalizzati del motore dell'agente di raccolta flusso avanzato

Sommario

Introduzione

In questo documento vengono descritte due impostazioni avanzate dell'agente di raccolta dei flussi che possono modificare il modo in cui l'agente di raccolta dei flussi SNA genera eventi di sicurezza personalizzati (CSE).

Introduzione

L'impostazione avanzata legacy early_check_age flow collector, insieme alla nuova impostazione avanzata cse_exec_interval_secs flow collector, determina il modo in cui gli eventi di sicurezza personalizzati vengono attivati dal motore del flow collector. Il Flow Collector è la prima appliance nell'architettura del sistema SNA a visualizzare il flusso sulla rete, quindi il motore del Flow Collector è responsabile del monitoraggio delle caratteristiche dei flussi nella cache di flusso e di determinare se il flusso soddisfa i criteri configurati di un determinato evento di sicurezza personalizzato. Queste impostazioni avanzate dell'agente di raccolta dei flussi NON modificano tuttavia le caratteristiche di attivazione di nessuno degli eventi di protezione di base incorporati.

Debug personalizzato degli eventi di protezione

Nella versione 7.5.0 e successive di SNA, l'impostazione avanzata dell'agente di raccolta di flusso debug_custom_events è stata migliorata per fornire diversi livelli di debug

- debug_custom_events 1 (debug minimo - progettato per essere eseguito in produzione e per fornire maggiori informazioni sui flussi esatti che generano i CSE)
- debug_custom_events 2 (ulteriori operazioni di debug)
- debug_custom_events 3 (debug più dettagliato)

Comportamento agente di raccolta flusso predefinito

Per impostazione predefinita, l'impostazione avanzata di early_check_age del raccoglitore di flusso è configurata su 160 secondi. Ciò significa che il motore di raccolta del flusso attende almeno 160 secondi prima di verificare se il flusso corrisponde a un evento di sicurezza personalizzato configurato. Per impostazione predefinita, questo controllo non viene ripetuto fino al termine del flusso.

Questo valore di controllo anticipato di 160 secondi è stato scelto in modo specifico perché, se si utilizzano le best practice, gli esportatori di telemetria devono essere configurati per inviare telemetria ogni 60 secondi. In un ambiente tipico, questo valore predefinito consente al raccoglitore di flussi di visualizzare le informazioni di flusso relative a entrambi i lati di una determinata conversazione o di un determinato flusso. Per questo motivo, early_check_age non è predefinito nell'elenco delle impostazioni avanzate. Questo è il risultato della progettazione e non è possibile modificare questo valore senza prima consultare il supporto tecnico. Questa progettazione iniziale non offre tuttavia risultati soddisfacenti se si considerano le caratteristiche di flusso lunghe e poco rumorose associate alla configurazione di eventi di sicurezza personalizzati che comportano l'accumulo di conteggi di byte o pacchetti. Per questo motivo è stato creato il parametro di impostazione avanzata cse_exec_interval_secs.

Impostazione avanzata cse_exec_interval_secs

Resa disponibile nella versione 7.4.2, l'aggiunta dell'impostazione avanzata del raccoglitore di flusso cse_exec_interval_secs ora consente al motore di controllare periodicamente i flussi nella relativa cache di flusso rispetto agli eventi di sicurezza personalizzati configurati. Questa impostazione avanzata è particolarmente utile nel caso di flussi lunghi, in cui un determinato flusso non corrisponde ai criteri CSE al valore predefinito di 160 secondi early_check_age, ma supera tale soglia in un secondo momento nel flusso. Senza questa impostazione avanzata, l'evento di protezione personalizzato non verrà attivato fino al termine del flusso, a volte questo può avvenire dopo giorni.

Impatto sulle prestazioni

L'esecuzione di questi criteri CSE per l'intervallo controlla i flussi più volte nella vita del flusso rispetto a quanto definito dai valori predefiniti richiede una CPU maggiore. Le istruzioni consentono di analizzare il contenuto del file sw.log nel motore di raccolta dei flussi per determinare una baseline delle prestazioni prima di abilitare il parametro cse_exec_interval_secs. Se si sta valutando l'abilitazione di questa impostazione avanzata e si desidera che TAC aiuti a confermare lo stato di salute del collettore di flusso in preparazione a questa modifica, è possibile aprire una richiesta di assistenza e collegare un pacchetto diagnostico del collettore di flusso alla

SR.

Misurazione della durata del thread classify_flows

Una misurazione rapida dell'impatto sulle prestazioni è quella di analizzare sw.log a partire dalla data odierna e confrontare i numeri elencati dopo le voci "cf-"log prima dell'attivazione dell'impostazione con i numeri dopo l'applicazione dell'impostazione.

/lancope/var/sw/oggi/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-12261/783375/946651/15423

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-122713/78446/954149/16320

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-129553/76677/964933/14864

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

Le voci cf stanno per "Classifica flussi". Rappresenta il numero di secondi impiegati dal thread per passare attraverso la sezione della Flow Cache di cui è responsabile. È nei thread "Classify Flows" dove i CSE vengono applicati ai flussi. Se questi numeri aumentano dopo l'attivazione della funzione, si otterrà una buona misurazione dell'impatto complessivo sulle prestazioni.

È previsto un aumento dopo l'aggiunta di questa impostazione di intervallo avanzata, ma se questo numero si avvicina a 60, rimuovere l'impostazione poiché l'impatto è troppo grande. Ci si aspetta un aumento di qualche secondo, che è ritenuto ragionevole.

Stato del motore nel periodo di prestazioni

Un'altra misurazione delle prestazioni "prima e dopo" è la sezione "Periodo di prestazioni" nel file sw.log che viene registrata ogni 5 minuti per misurare l'impatto dell'impostazione sull'elaborazione del flusso. È possibile cercare questi blocchi utilizzando anche grep. Se il motore è sovraccarico, la verifica dell'intervallo di impostazione avanzato deve essere disattivata.

/lancope/var/sw/oggi/logs/ grep -A3 "Periodo prestazioni" sw.log

Prendere nota di qualsiasi stato diverso da "Stato motore normale".

Uno stato quale "Velocità di input dello stato del motore troppo alta" indica che il thread classify_flows sta consumando troppa CPU.

SFI - Indice di flusso statico

Significa che i thread di classificazione non sono stati in grado di completare i passaggi attraverso la cache di flusso: sta per "Static Flow Index" e indica un problema nei thread di classificazione dei flussi. Non è un disastro di per sé, ma indica che il motore sta iniziando a colpire il soffitto e che le prestazioni stanno iniziando a peggiorare ai livelli attuali di cf.

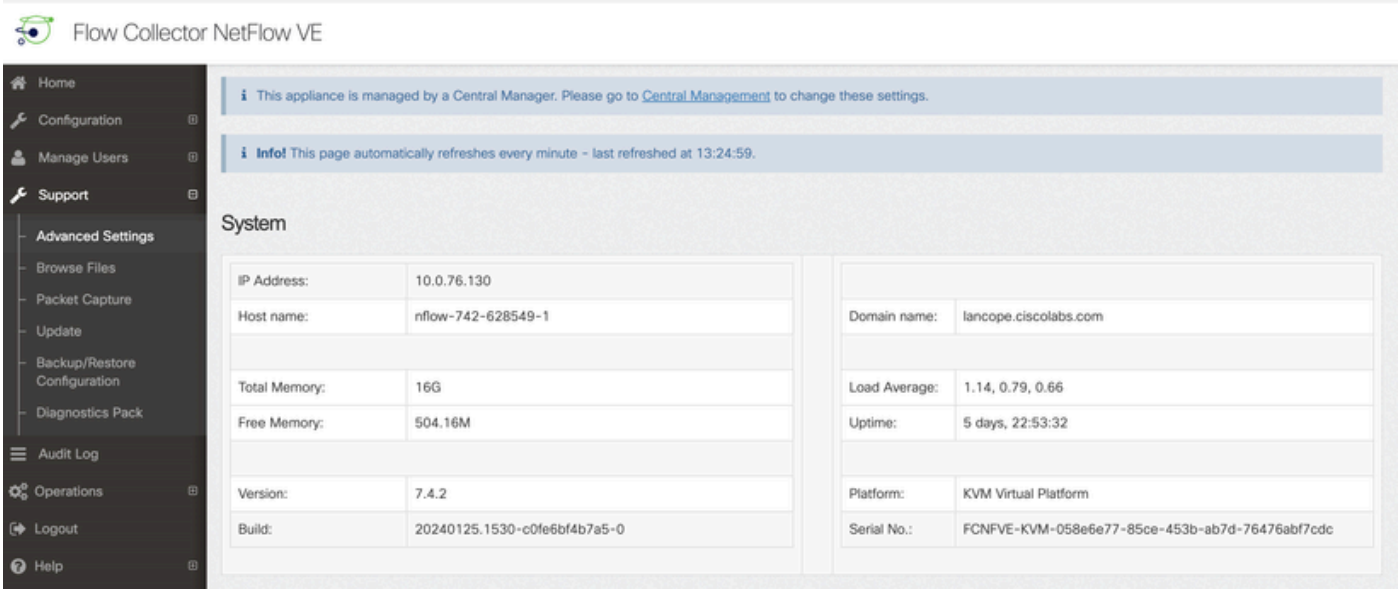
sw.log:16:09:49 I-flo-f1: classify_flows: sfi:base(8388608) (10522745 -> 11014427) max(1677215) cod(1) (491681/8388608)—>(5%)
sw.log:16:09:49 I-flo-f3: classify_flows: sfi:base(25165824) (27269277 -> 27754304) max(33554431) cod(1) (485026/8388608)—>(5%)
sw.log:16:09:49 I-flo-f4: classify_flows: sfi:base(33554432) (35652656 -> 36138422) max(41943039) cod(1) (485765/8388608)—>(5%)
sw.log:16:09:49 I-flo-f2: classify_flows: sfi:base(1677216) (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(1677216) (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(1677215) 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 -> 5244661) 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) (5244661 -> 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(1677215) 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(1677216) (17522620 -> 18202249) max(25165823) cod(1) (679628/8388608)—>(8%)

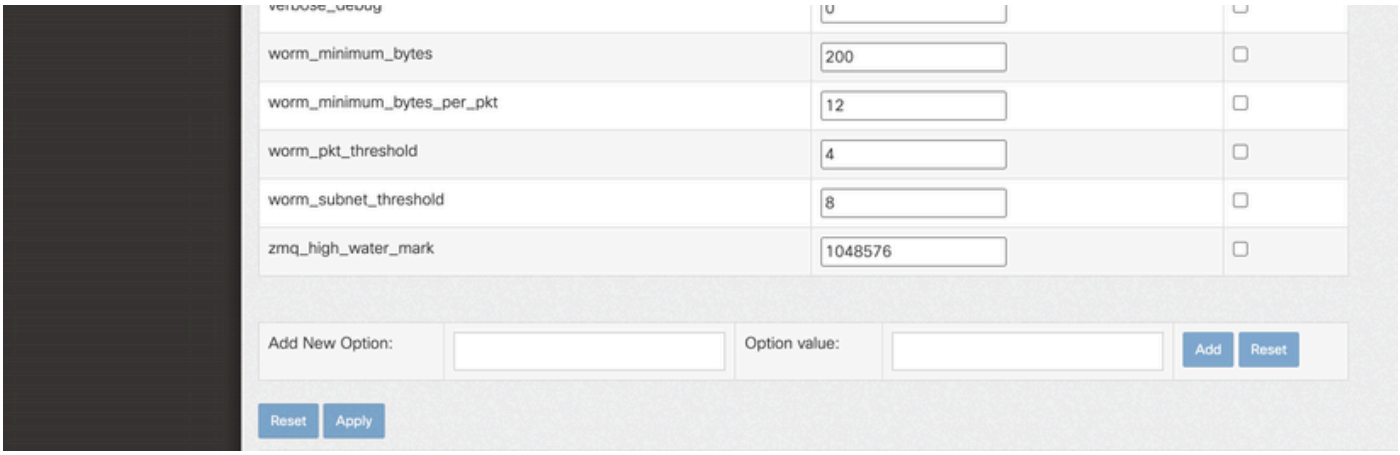
Configurazione

Aprire un browser Web e passare direttamente all'indirizzo IP dell'accessorio Flow Collector. Eseguire il login come utente amministratore locale.

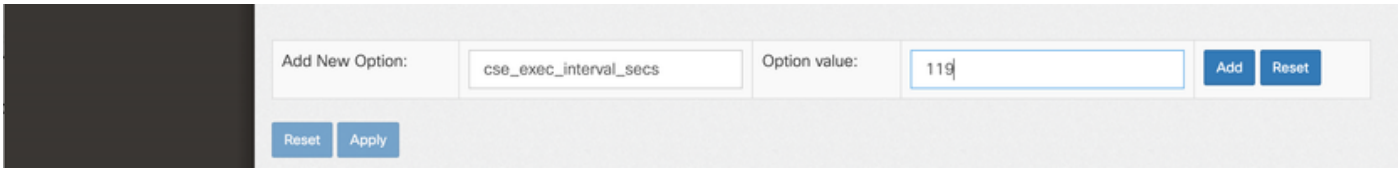
Passare a Supporto -> Impostazioni avanzate



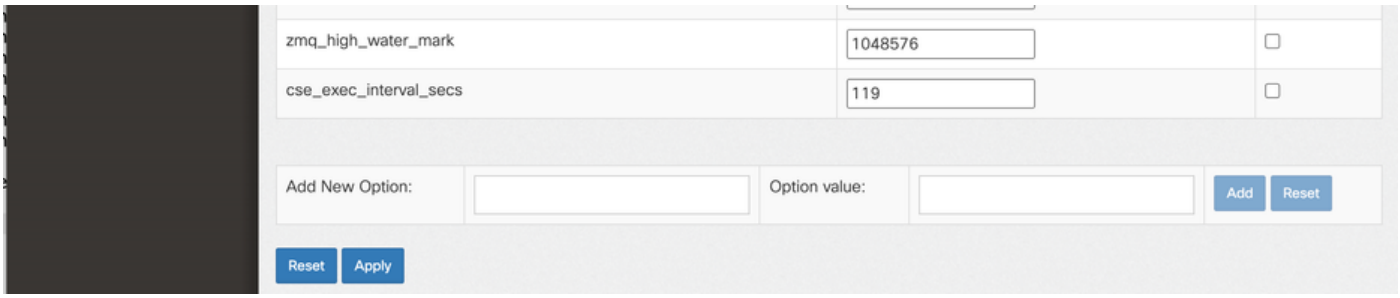
Scorrere verso il basso la schermata Advanced Setting (Impostazioni avanzate) per visualizzare la casella di configurazione "Add New Option" (Aggiungi nuova opzione) in fondo all'elenco



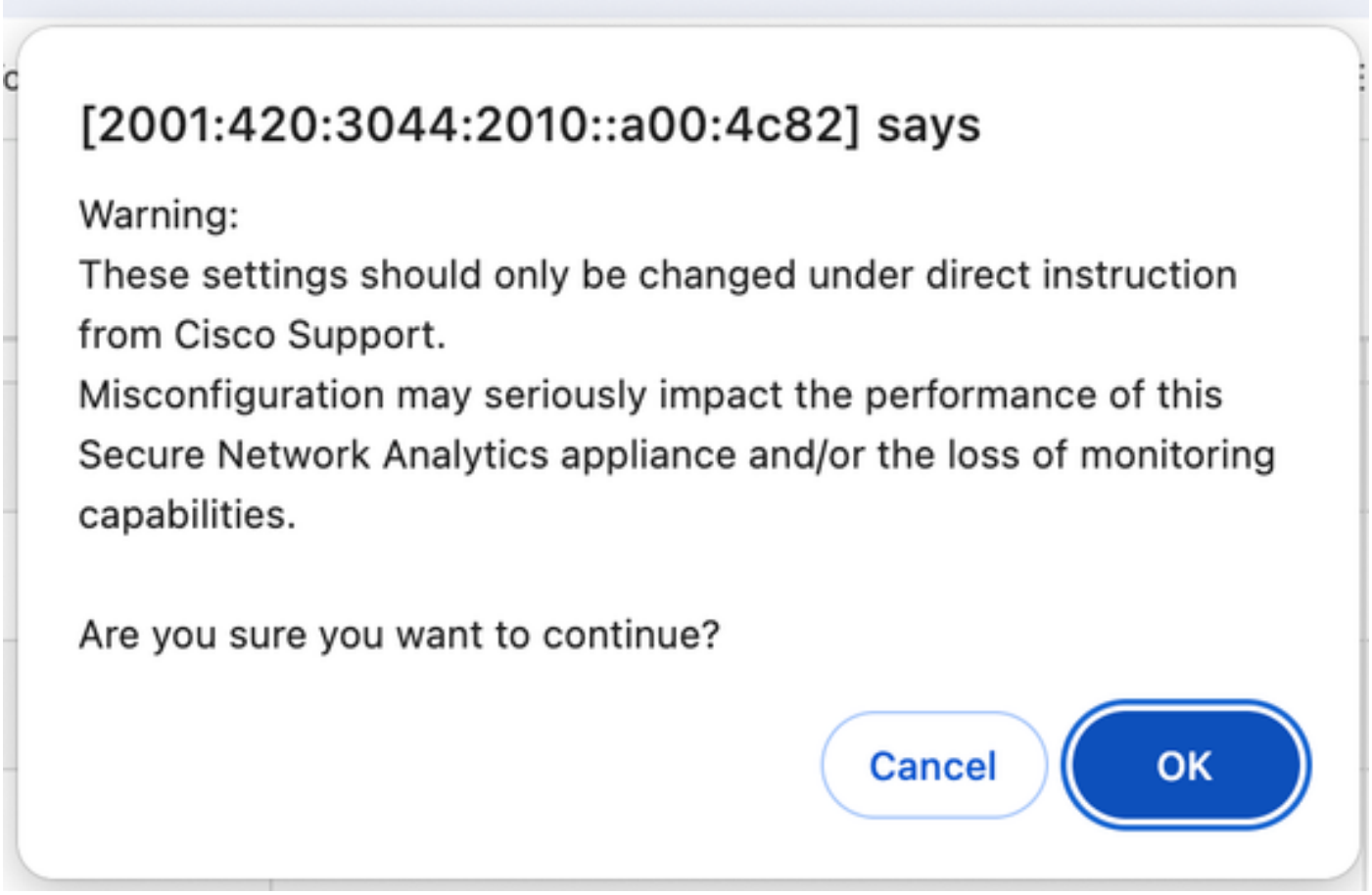
Nella casella Aggiungi nuova opzione: modifica immettere cse_exec_interval_secs e nella casella Valore opzione: modifica immettere 119. La modifica di queste caselle attiva il pulsante Aggiungi. Premere il pulsante Add dopo aver immesso cse_exec_interval_secs nella casella Add New Option: edit e 119 nella casella Option Value: edit.



Le caselle Aggiungi nuova opzione: e Valore opzione: modifica vengono eliminate in preparazione di un'altra voce nell'evento in cui verranno immesse più nuove impostazioni avanzate. Le Impostazioni avanzate appena aggiunte vengono evidenziate in fondo all'elenco durante l'aggiunta. In questo modo, l'utente ha la possibilità di controllare la voce. L'ortografia esatta dell'impostazione avanzata è importante come il caso. Tutte le impostazioni avanzate sono in lettere minuscole.



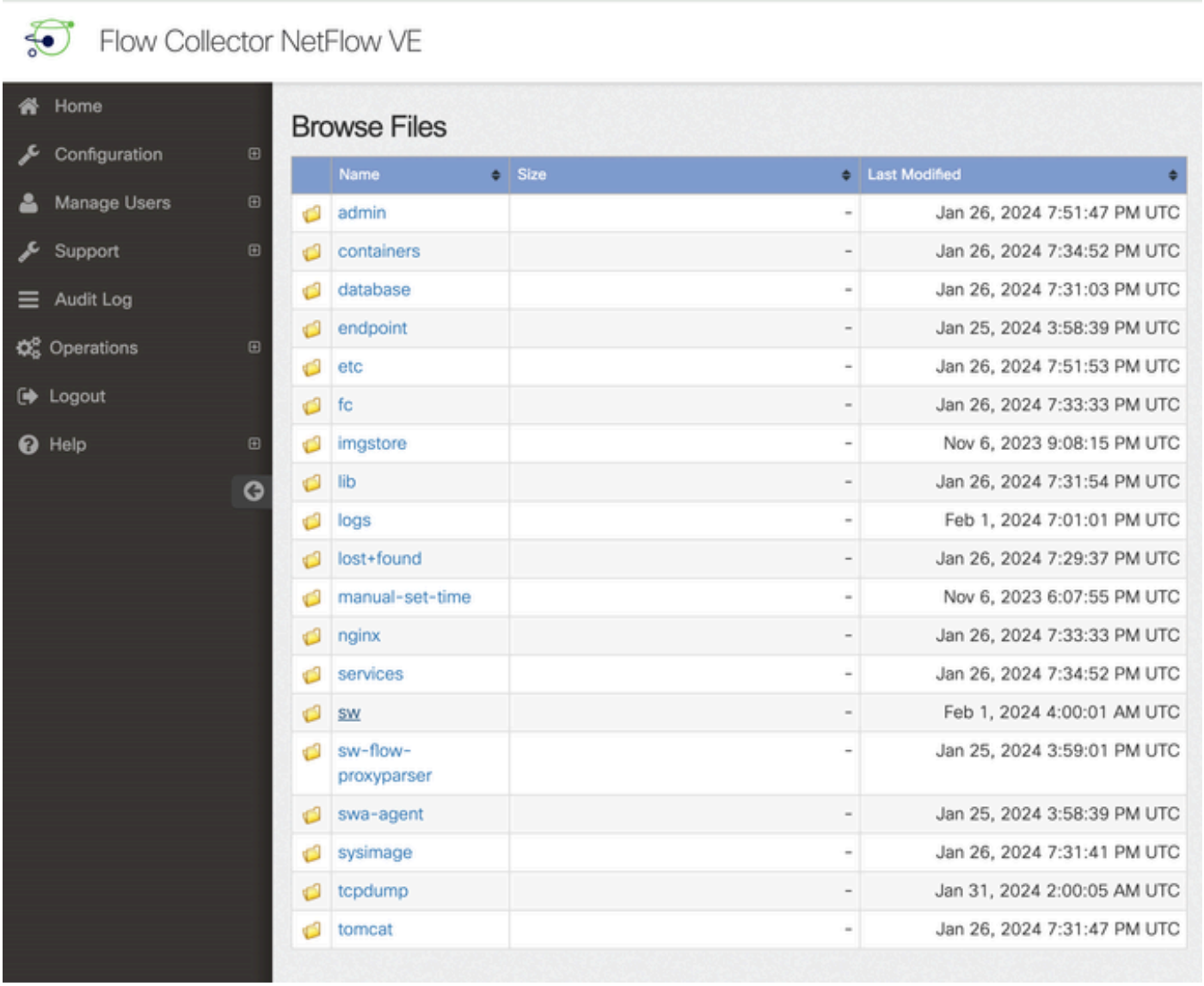
Una volta immessa correttamente l'impostazione avanzata, premere il pulsante Apply. A volte il pulsante Applica non è abilitato. Per attivarla, fare clic nella casella di modifica Aggiungi nuova opzione:, quindi il pulsante Applica diventa attivo. Quando viene visualizzato questo popup, premere il pulsante OK per inviare le nuove impostazioni avanzate e il nuovo valore.



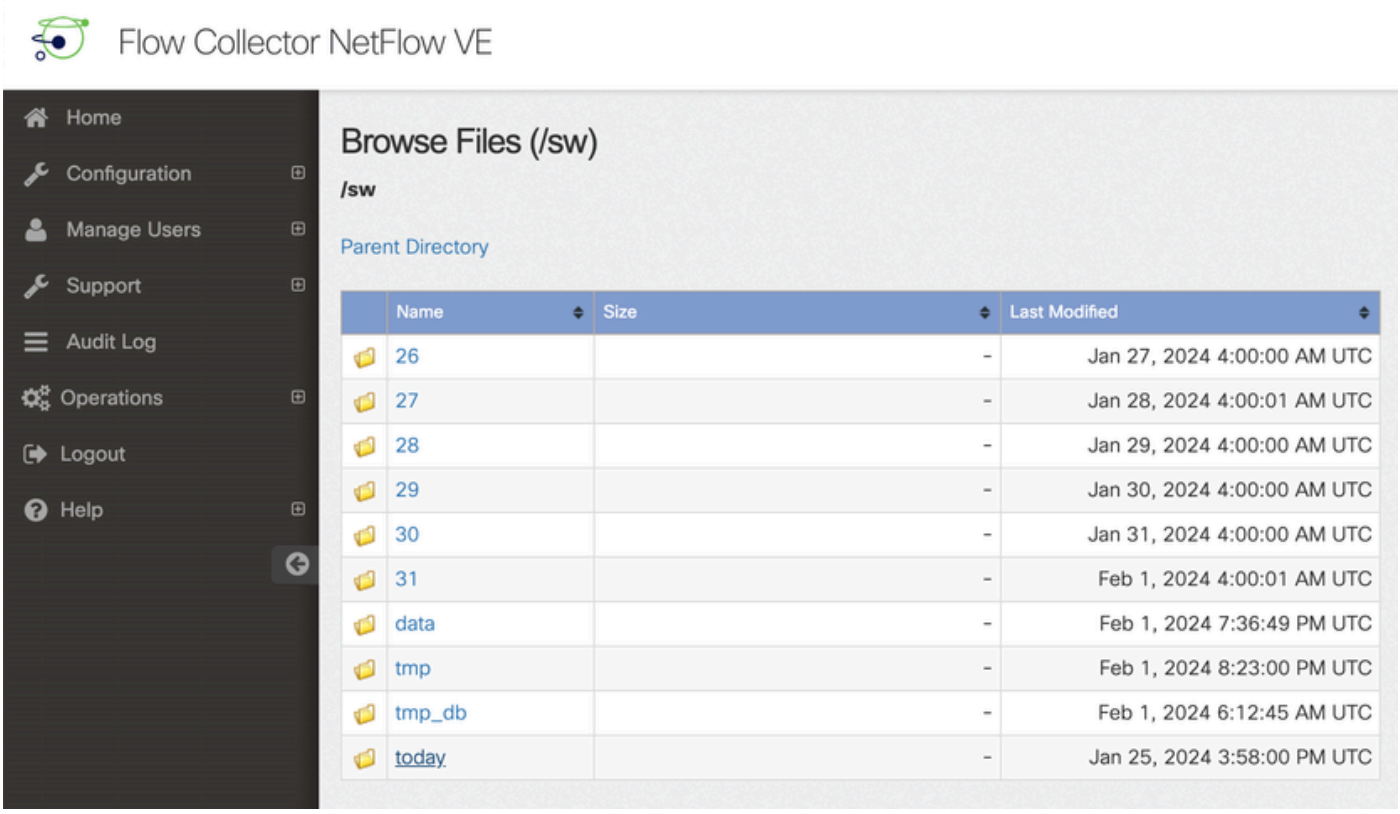
Conferma della modifica

Questa convalida finale è la più importante. Fare di nuovo clic sul menu Support e selezionare Browse Files.

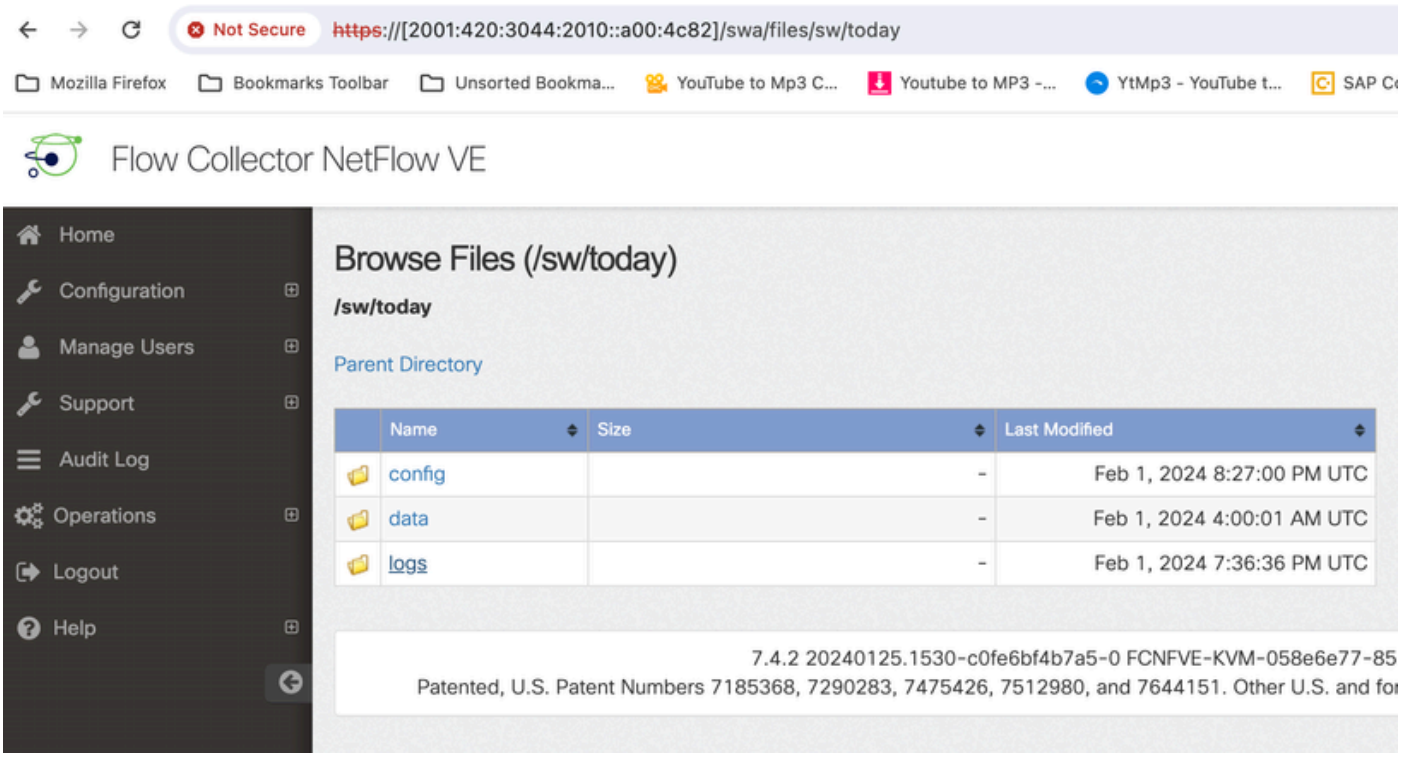
In questo modo è possibile passare al file system della FC. Fare clic su software.



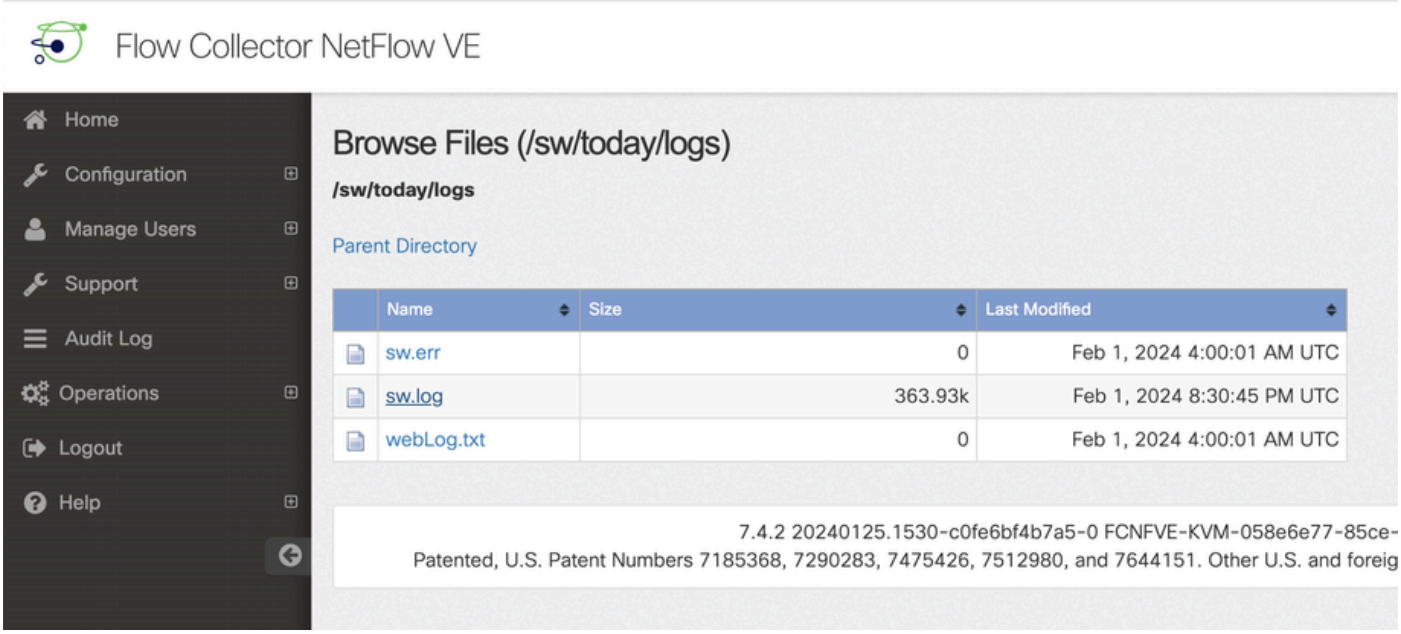
Fai clic su oggi



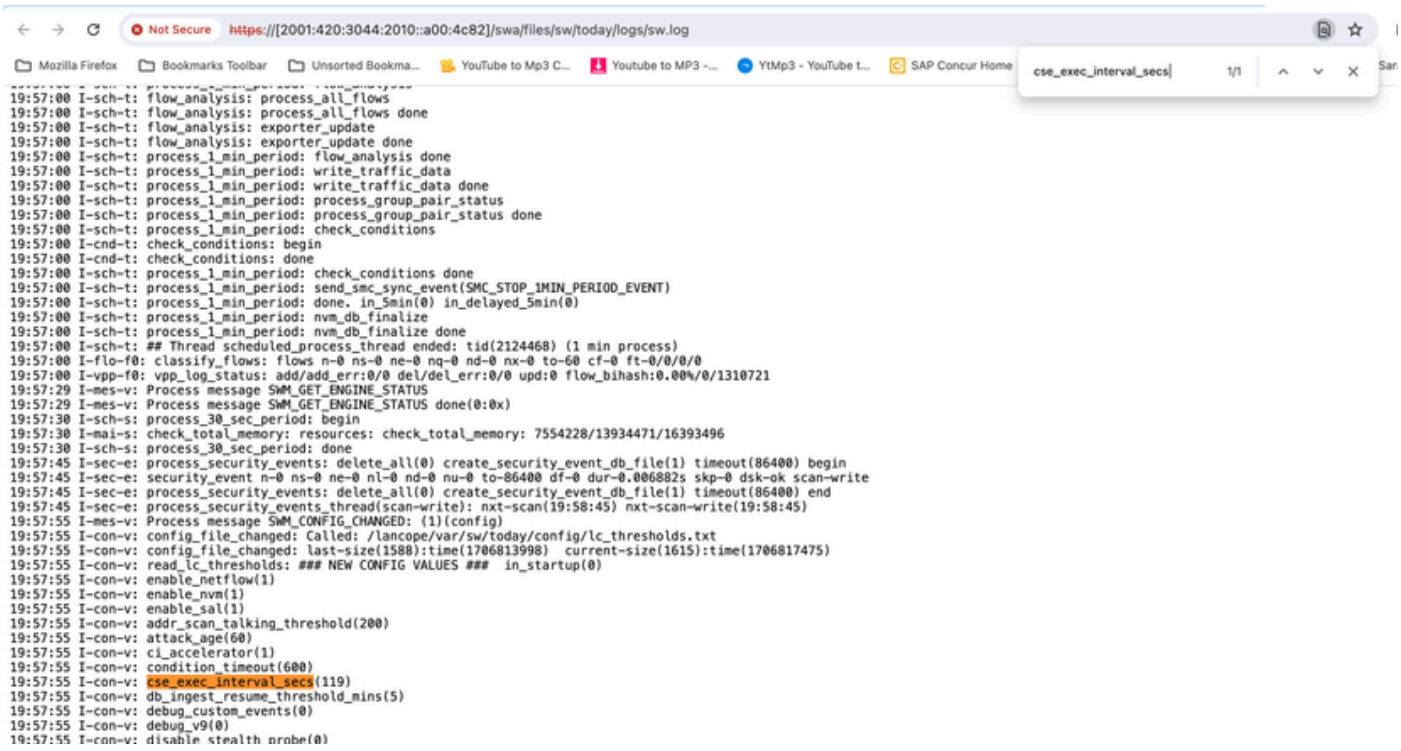
Fare clic sui registri.



Fare clic su sw.log



Eseguire una ricerca nella pagina del browser e immettere cse_exec_interval_secs nella casella di ricerca per trovare l'impostazione avanzata



Le impostazioni avanzate accettate sono elencate come mostrato nella schermata.

Quelli non accettati sono elencati come "non parte della configurazione di input", in questo caso è dovuto all'errata ortografia dell'impostazione da parte dell'utente. Per questo motivo è importante controllare il registro dopo aver apportato tali modifiche alla configurazione.

```
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)
```

Congratulazioni!

È stata appena immessa una nuova impostazione avanzata e ne è stata convalidata l'accettazione da parte del motore.

A questo punto, la funzione è abilitata per eseguire la logica CSE sui flussi circa ogni 2 minuti dopo che il flusso ha raggiunto il valore predefinito di early_check_age pari a 160 secondi.

Se le regole CSE prevedono l'accumulo di conteggi di byte nel tempo, questa funzione migliora i tempi di attivazione dei CSE sui flussi che corrispondono ai criteri definiti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).