Configurar comportamiento de desencadenado de eventos de seguridad personalizada de Flow Collector Engine avanzado

Contenido

Introducción

Background

Comportamiento predeterminado del Flow Collector

Configuración avanzada de cse_exec_interval_secs

Impactos en el rendimiento

- Medición de la duración del subproceso classify_flows
- Estado del motor durante el período de rendimiento
- SFI - Índice de flujo estático

Configuración

Confirmación del cambio

¡Enhorabuena!

Introducción

Este documento describe dos configuraciones avanzadas del colector de flujo que pueden alterar la manera en que el colector de flujo SNA dispara los eventos de seguridad personalizados (CSE).

Background

La configuración avanzada del recopilador de flujo early_check_age heredado, junto con la nueva configuración avanzada del recopilador de flujo cse_exec_interval_secs, determinan la manera en que el motor del recopilador de flujo activa los eventos de seguridad personalizados. El recopilador de flujo es el primer dispositivo de la arquitectura del sistema SNA que ve el flujo en la red y, por lo tanto, el motor del recopilador de flujo es responsable de supervisar las características de los flujos mientras están en la caché de flujo y de determinar si el flujo cumple los criterios configurados de un evento de seguridad personalizado determinado. Sin embargo, estas configuraciones avanzadas del colector de flujo NO cambian las características de disparo de ninguno de los eventos de seguridad de núcleo incorporados.

Comportamiento predeterminado del Flow Collector

De forma predeterminada, la configuración avanzada del colector de flujo early_check_age se configura en 160 segundos. Esto significa que el motor del colector de flujo espera un mínimo de 160 segundos en un flujo antes de verificar si ese flujo coincide con un evento de seguridad

personalizado configurado. De forma predeterminada, esta verificación no se realiza de nuevo hasta después de que finalice el flujo.

Este valor de comprobación temprana de 160 segundos se eligió específicamente porque, si se utilizan las prácticas recomendadas, los exportadores de telemetría deben configurarse para enviar telemetría cada 60 segundos. Este valor predeterminado permite tiempo suficiente en un entorno típico para que el recolector de flujo vea la información de flujo relacionada con ambos lados de una conversación o flujo determinado. Por esta razón, early_check_age no está predefinido en la lista de configuraciones avanzadas. Esto es por diseño, y no debe alterar este valor sin consultar primero con el departamento de soporte técnico/ingeniería. Sin embargo, este diseño inicial no funciona de manera favorable cuando se consideran características de flujo largas y algo silenciosas junto con la configuración de eventos de seguridad personalizados que implican la acumulación de recuentos de bytes o paquetes. Esto fue por esta razón para la creación del parámetro de configuración avanzada cse_exec_interval_secs .

Configuración avanzada de cse_exec_interval_secs

Disponible en la versión 7.4.2, la adición de la configuración avanzada del colector de flujo cse_exec_interval_secs permite ahora indicar al motor que verifique periódicamente los flujos en su caché de flujo con respecto a los eventos de seguridad personalizados configurados. Esta configuración avanzada es particularmente útil en el caso de flujos largos, donde un flujo dado no ha coincidido con un criterio CSEs en la edad de comprobación temprana predeterminada de 160 segundos, pero cruza ese umbral más adelante en el flujo. Sin esta configuración avanzada, el evento de seguridad personalizado no se activaría hasta que finalice el flujo, a veces días después.

Impactos en el rendimiento

La ejecución de estos criterios CSE de intervalo comprueba los flujos más veces en la vida del flujo que lo que definen los valores por defecto requiere más CPU. Las instrucciones le guiarán en la investigación del contenido del archivo sw.log en el sistema de recopilación de flujos para determinar una línea base de rendimiento antes de activar el parámetro cse_exec_interval_secs. Si está considerando habilitar esta configuración avanzada y desea que TAC le ayude a confirmar el estado de su colector de flujo en preparación para este cambio, esto se puede hacer abriendo un caso de soporte y adjuntando un paquete de diagnóstico del colector de flujo al SR.

Medición de la duración del subproceso classify_flows

Una medición rápida del impacto en el rendimiento que puede hacer es investigar sw.log a partir de hoy y comparar los números que aparecen después de las entradas de registro "cf-"antes de la activación de la configuración con los números después de aplicar la configuración.

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

20:43:21 I-flo-f0: classify_flows: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos 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: flujos n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0 to-300 cf-22 ft-129255/770212/970360/15129

Las entradas cf significan "Clasificar flujos". Representa el número de segundos que el subproceso tardó en pasar por la sección de la caché de flujo de la que es responsable. Es en los hilos "Clasificar flujos" donde se aplican los CSE frente a los flujos. Si observa que estas cifras aumentan después de habilitar la función, se trata de una buena medida del impacto general en el rendimiento.

Se espera un aumento después de agregar esta configuración de intervalo avanzado, pero si este número se acerca a 60, quite la configuración porque el impacto es demasiado grande. Se espera un aumento de unos pocos segundos y se considera razonable.

Estado del motor durante el período de rendimiento

Otra medición del rendimiento "antes y después" que puede hacer es consultar las secciones "Período de rendimiento" en el archivo sw.log que se registran cada 5 minutos para medir el impacto de la configuración en el procesamiento de flujo. Puede buscar estos bloques utilizando grep también. Si el motor está saturado, la comprobación del intervalo de configuración avanzada debe desactivarse.

/lancope/var/sw/today/logs/ grep -A3 "Performance Period" sw.log

Tenga en cuenta cualquier estado que no sea "Estado normal del motor".

Un estado como "Velocidad de entrada de estado del motor demasiado alta" indicaría que el subproceso classify_flows está consumiendo demasiada CPU.

SFI - Índice de flujo estático

Significa que los subprocesos de clasificación no pudieron completar sus pasadas a través de la caché de flujo: significa "Índice de flujo estático" e indica una lucha en la clasificación de subprocesos de flujo. No es un desastre en sí mismo, pero indica que el motor está empezando a golpear el techo y que el rendimiento está empezando a degradarse en los niveles actuales de cf.

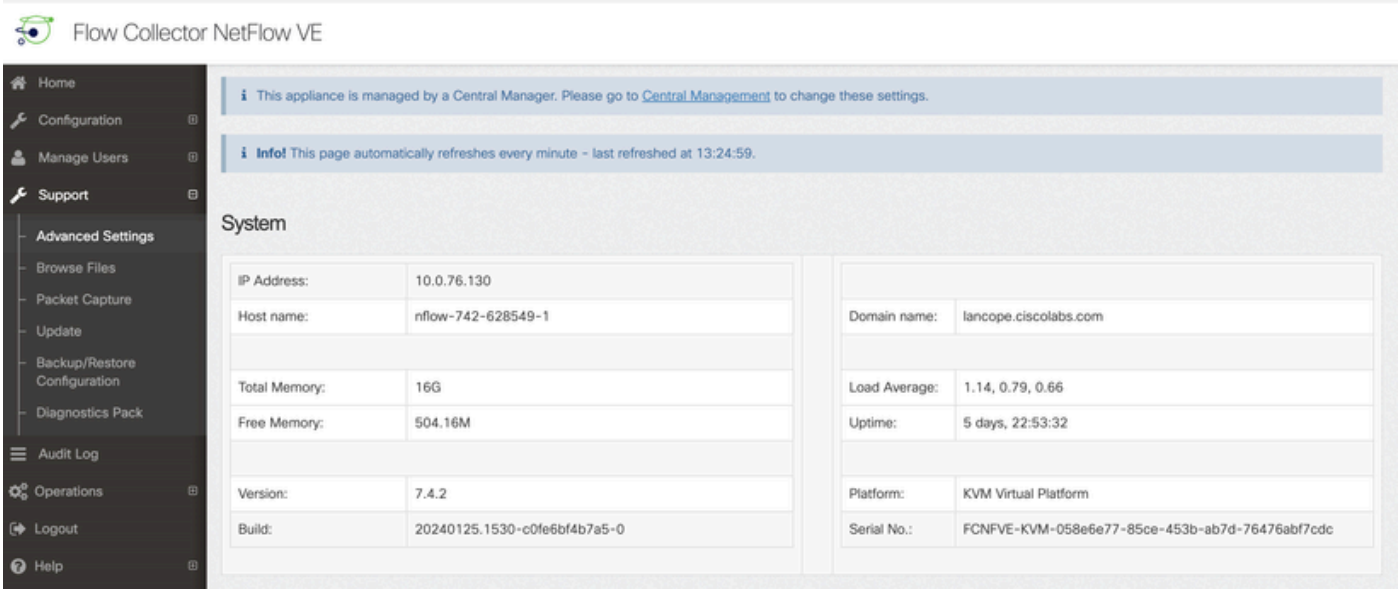
sw.log:16:09:49 I-flo-f1: classify_flows: sfi:base(8388608) (10522745 -> 11014427) max(16777215) cod(1) (491681/8388608)---------->(5%)
sw.log:16:09:49 I-flo-f3: classify_flows: sfi:base(25165824) (27269277 -> 27754304) max(33554431) cod(1) (485026/8388608)---------->(5%)
sw.log:16:09:49 I-flo-f4: classify_flows: sfi:base(33554432) (35652656 -> 36138422) max(41943039) cod(1) (485765/8388608)---------->(5%)
sw.log:16:09:49 I-flo-f2: classify_flows: sfi:base(16777216) (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(16777216) (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(16777215) cod(0) (6350489/8388608)---------->(75%)
sw.log:16:10:49 I-flo-f3: classify_flows: sfi:base(25165824) (27754304 -> 25702968) max(33554431) cod(0) (6337271/8388608)---------->(75%)
sw.log:16:10:49 I-flo-f7: classify_flows: sfi:base(58720256) (58848913 -> 59630528) max(67108863) cod(0) (781614/8388608)---------->(9%)
sw.log:16:10:49 I-flo-f4: classify_flows: sfi:base(33554432) (36138422 -> 34064015) max(41943039) cod(1) (6314200/8388608)---------->(75%)
sw.log:16:10:49 I-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%)

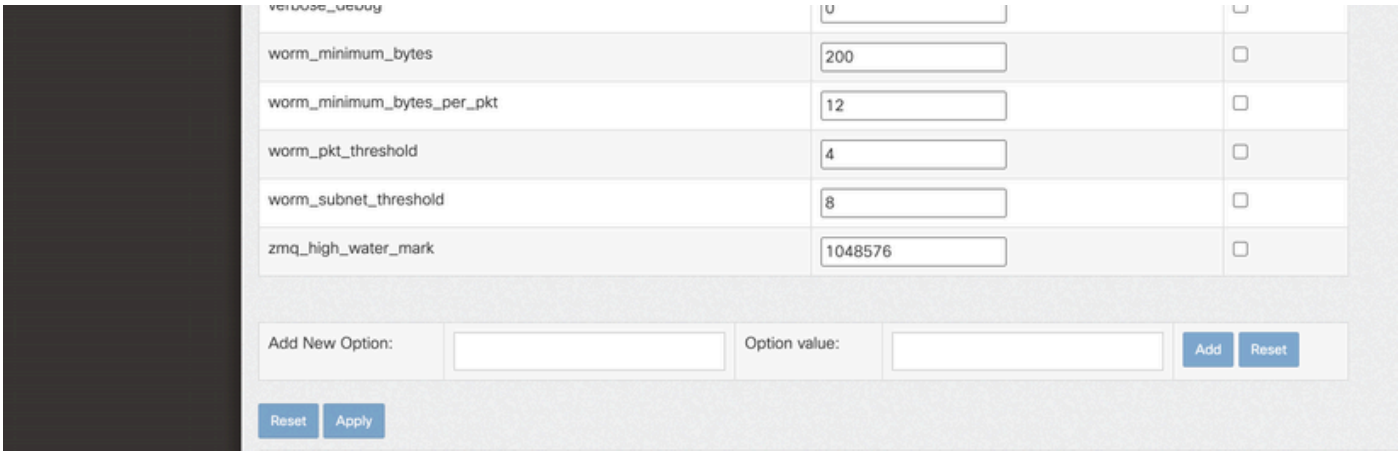
Configuración

Abra un navegador web y navegue directamente a la dirección IP del dispositivo Flow Collector. Inicie sesión como el usuario administrador local.

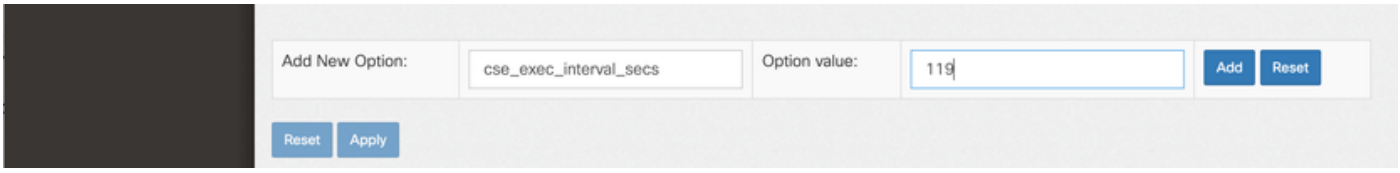
Vaya a Asistencia -> Configuración avanzada



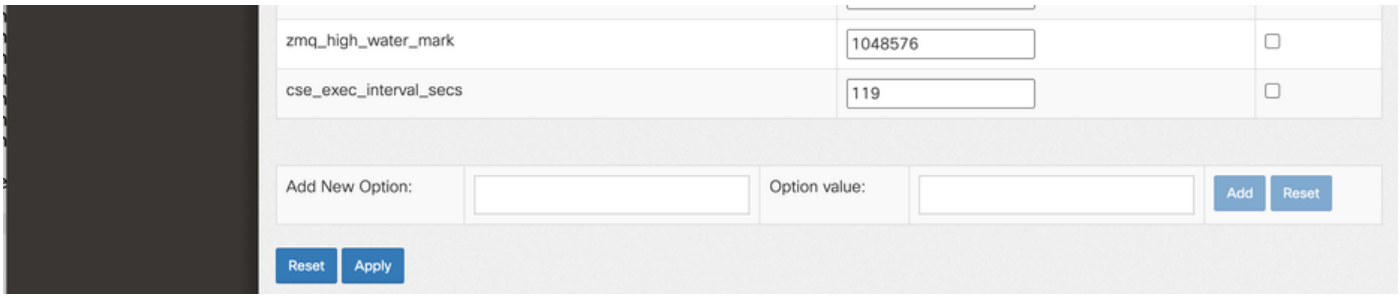
Desplácese hacia abajo en la pantalla Advanced Setting (Parámetros avanzados) para mostrar el cuadro de configuración "Add New Option" (Agregar nueva opción) en la parte inferior de la lista



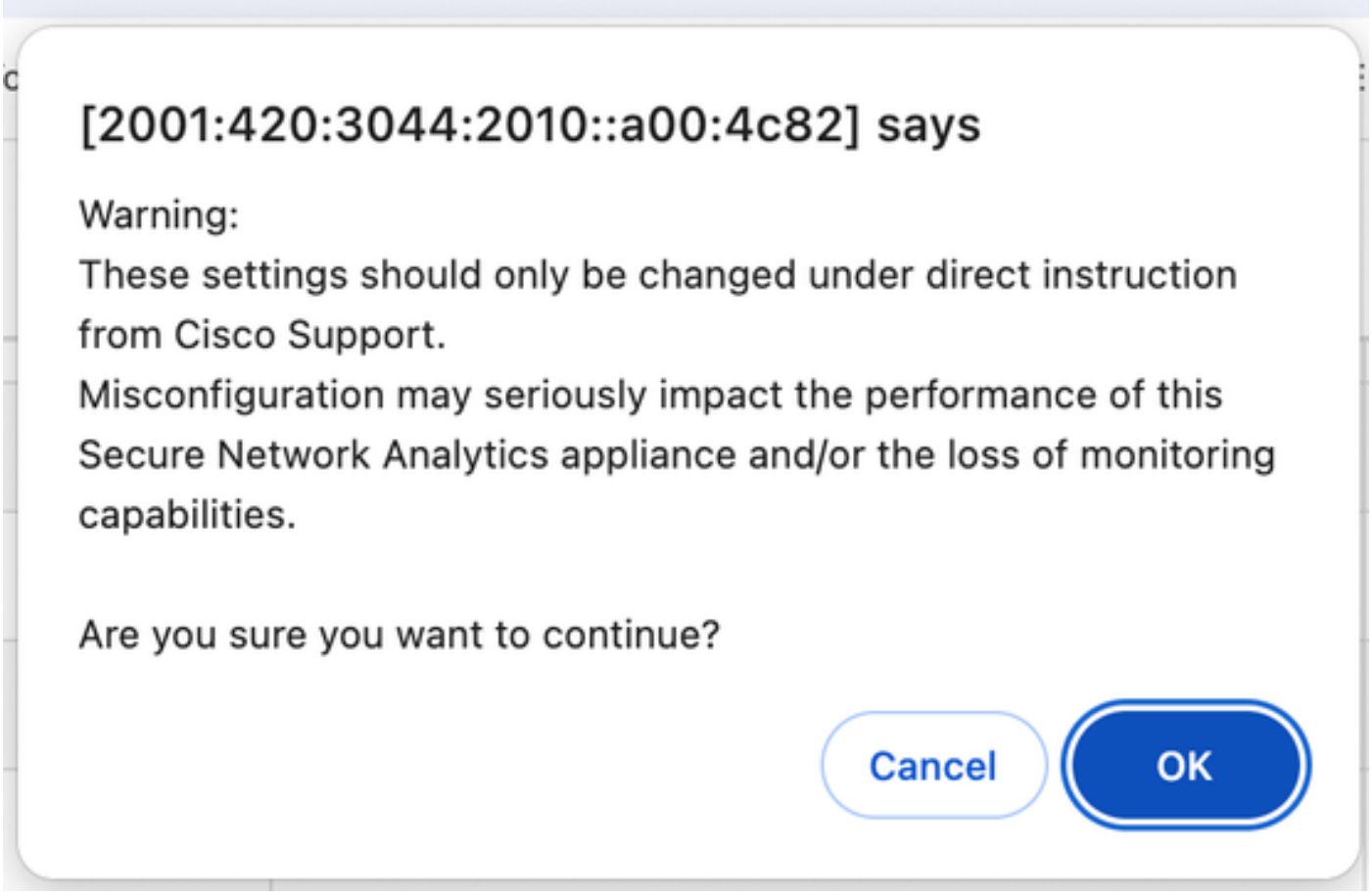
En el cuadro de edición Agregar nueva opción: escriba cse_exec_interval_secs y en el valor de opción: cuadro de edición escriba 119. La edición de estos cuadros habilita elbotón Agregar. Pulse el botón Agregar después de introducir cse_exec_interval_secs en el cuadro de edición Agregar nueva opción: y 119 en el cuadro de edición Valor de la opción: edit.



Los cuadros Add New Option: y Option value: edit se borran para preparar otra entrada en el caso de que se vayan a introducir varias configuraciones avanzadas nuevas. Las configuraciones avanzadas recién agregadas se colocan en la parte inferior de la lista a medida que se agregan. Esto da al usuario la oportunidad de inspeccionar la entrada. La ortografía exacta de la configuración avanzada es importante, así como el caso. Todos los parámetros avanzados están en minúsculas.



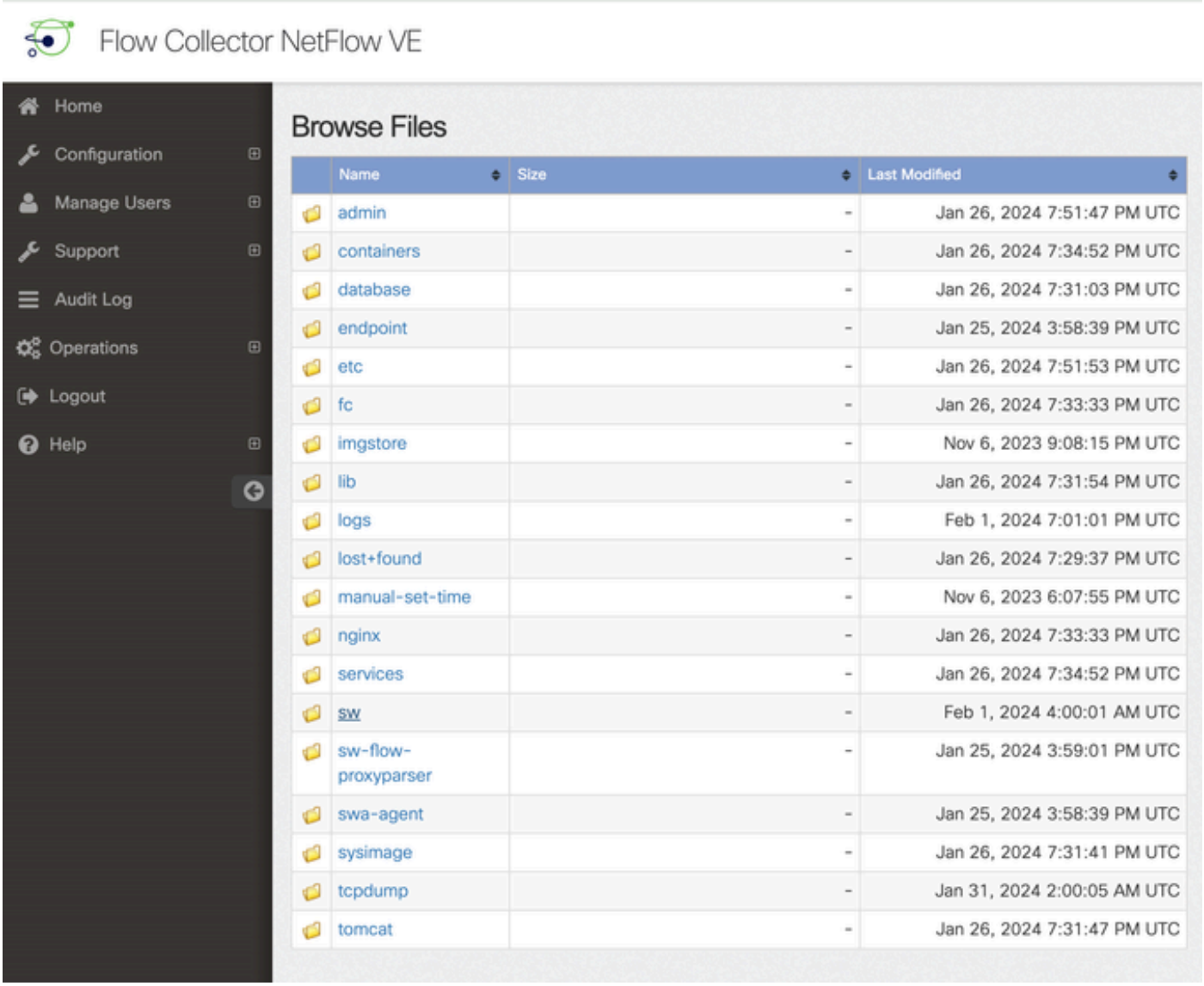
Ahora que la configuración avanzada se ha introducido correctamente, pulse el botón Aplicar. Tenga en cuenta que a veces el botón Apply no está habilitado. Para activarlo, haga clic en el cuadro de edición Add New Option: y, a continuación, el botón Apply se activará para hacer clic. Cuando aparezca esta ventana emergente, pulse el botón OK (Aceptar) para enviar la nueva configuración avanzada y el valor.



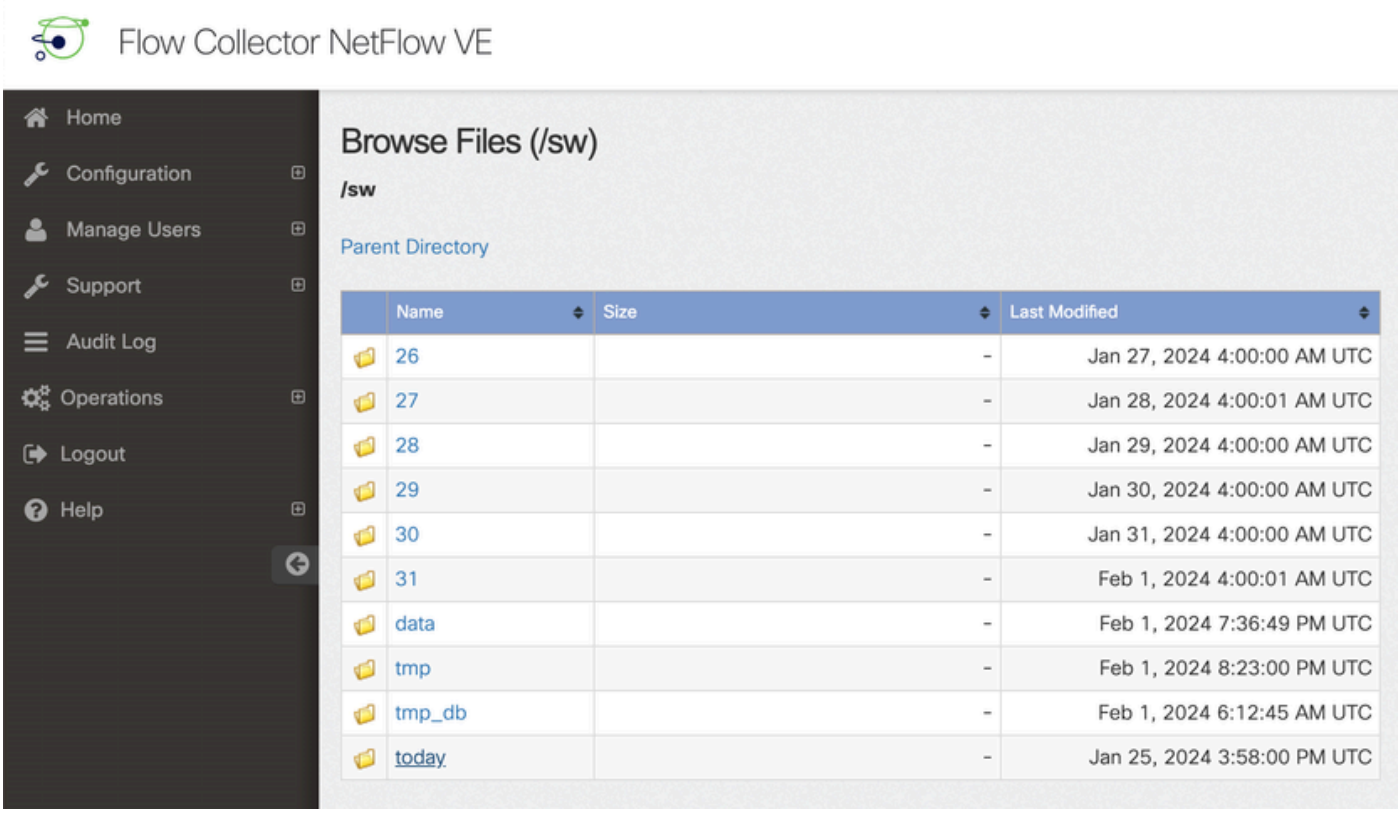
Confirmación del cambio

Esta validación final es la más importante. Haga clic en el menú Support nuevamente y elija Browse Files.

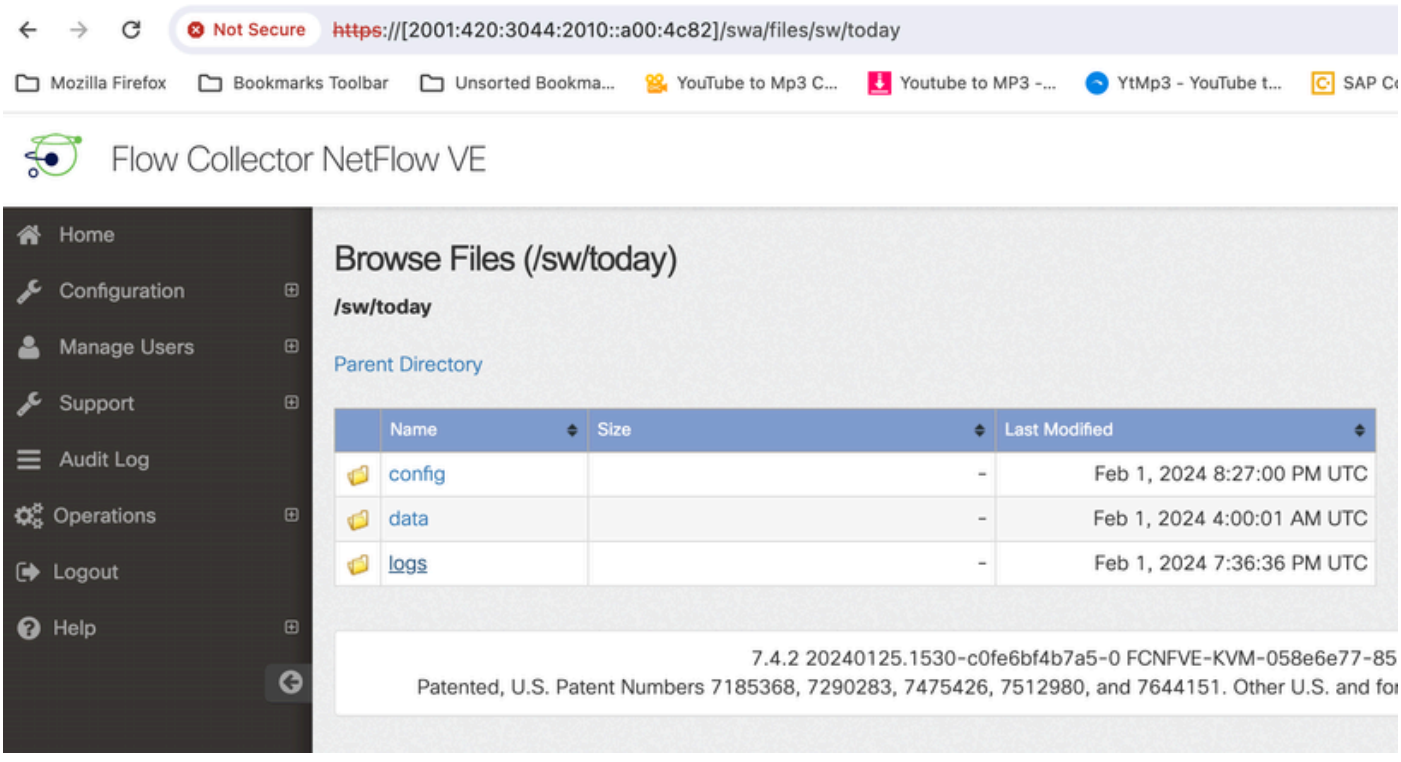
Esto lo lleva al sistema de archivos en el FC. Haga clic en sw.



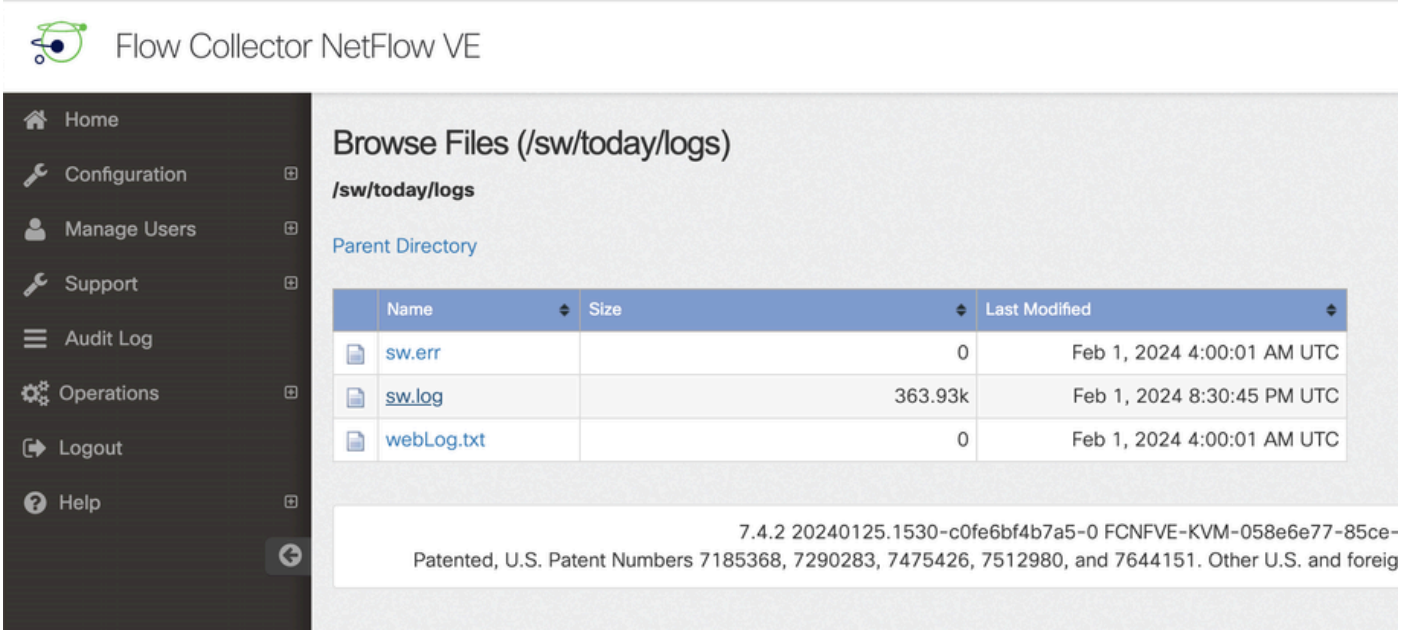
Haga clic en hoy



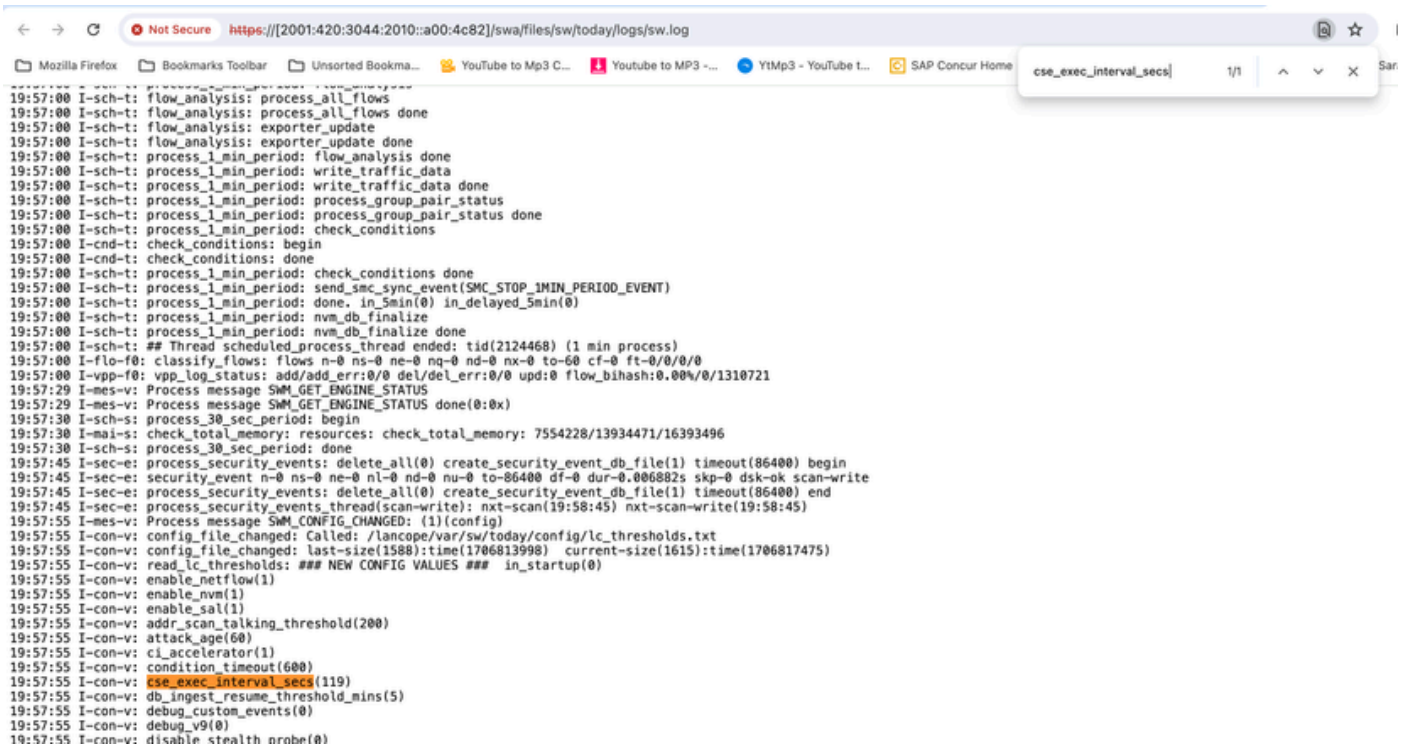
Haga clic en logs.



Haga clic en sw.log



Realice una búsqueda en la página del navegador e introduzca cse_exec_interval_secs en el cuadro de búsqueda para buscar la configuración avanzada



Las opciones de configuración avanzadas aceptadas aparecen como se muestra en la captura de pantalla.

Los que no se aceptan se muestran como "no forman parte de la configuración de entrada", en este caso se debió a que el usuario no escribió correctamente la configuración. Por este motivo, es importante comprobar el registro después de realizar dichos cambios en la configuración.

```
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)
```

¡Enhorabuena!

Acaba de introducir una nueva configuración avanzada y validar su aceptación por parte del motor.

Ahora, la función está habilitada para ejecutar la lógica CSE en los flujos aproximadamente cada 2 minutos después de que el flujo alcance early_check_age que se establece de forma predeterminada en 160 segundos.

Si las reglas CSE implican la acumulación de recuentos de bytes a lo largo del tiempo, esta función mejora el tiempo en el que se activan los CSE en flujos que coinciden con los criterios definidos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).