Comprensión de los perfiles de reglas de Snort 3 y CPU en la GUI de FMC

Contenido

Introducción

Este documento describe la regla Snort 3 y la función de generación de perfiles de CPU añadida en FMC 7.6.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

· Conocimiento de Snort 3
· Centro de gestión de Firepower (FMC) seguro
· Firepower Threat Defense (FTD) seguro

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este documento se aplica a todas las plataformas Firepower
- Secure Firewall Threat Defence Virtual (FTD) que ejecuta la versión de software 7.6.0
- Secure Firewall Management Center Virtual (FMC) que ejecuta la versión de software 7.6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de características

- La generación de perfiles de CPU y reglas ya existía en Snort, pero solo se podía acceder a ella a través de la CLI de FTD. El objetivo de esta función es ampliar las capacidades de creación de perfiles y hacerla más sencilla.
- Habilite los problemas de rendimiento de la regla de intrusión de debug y ajuste las configuraciones de la regla por su cuenta antes de ponerse en contacto con el TAC para obtener ayuda para la resolución de problemas.
- Comprender qué módulos tienen un rendimiento insatisfactorio cuando Snort 3 consume una gran cantidad de CPU.
- Cree una forma sencilla de depurar y ajustar las políticas de análisis de red y de intrusiones para obtener un mejor rendimiento.

Perfiles

- Tanto la generación de perfiles de reglas como la generación de perfiles de CPU se ejecutan en el FTD y sus resultados se almacenan en el dispositivo y FMC los extrae.
- Puede ejecutar varias sesiones de generación de perfiles simultáneamente en diferentes dispositivos.
- Puede ejecutar los perfiles de reglas y de CPU al mismo tiempo.
- En caso de alta disponibilidad, la creación de perfiles solo se puede iniciar en el dispositivo que está activo al inicio de la sesión.
  En el caso de las configuraciones agrupadas, la creación de perfiles se puede ejecutar en cada nodo del clúster.
- Si se activa una implementación mientras hay una sesión de generación de perfiles en curso, se muestra una advertencia al usuario.

Si el usuario elige ignorar la advertencia e implementar, esto cancela la sesión de generación de perfiles actual y el resultado del generador de perfiles muestra un mensaje relacionado con esto.

Es necesario iniciar una nueva sesión de generación de perfiles sin que la implementación la interrumpa para obtener los resultados reales de la generación de perfiles.

Analizador de reglas

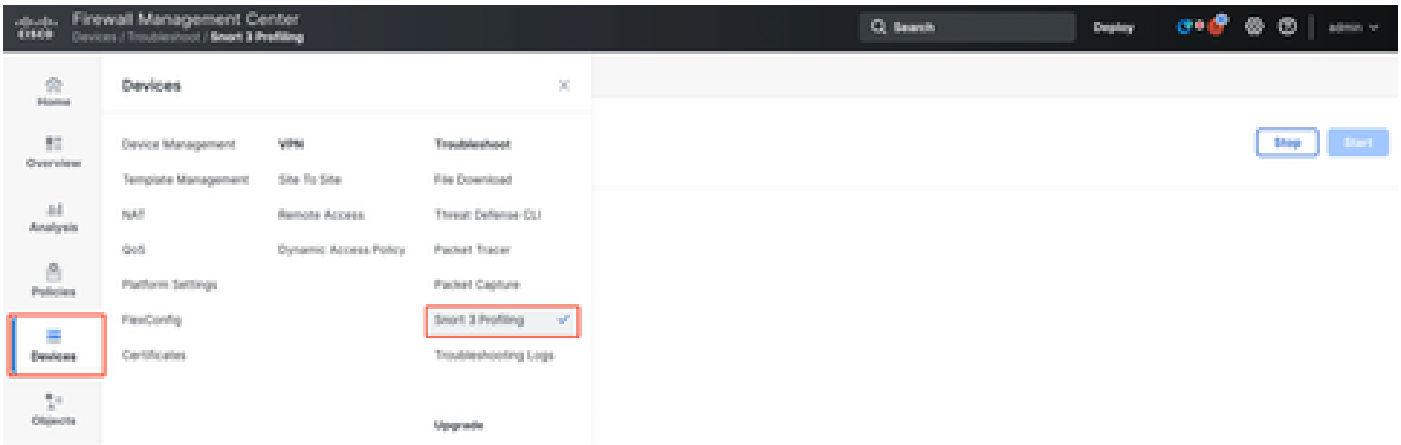
- El analizador de reglas de Snort 3 recopila datos sobre la cantidad de tiempo empleado en procesar un conjunto de reglas de intrusión de Snort 3, lo que resalta posibles problemas y muestra las reglas con un rendimiento insatisfactorio.
- Rule Profiler muestra las 100 reglas IPS que tardaron más tiempo en comprobarse.
- El analizador de reglas de desencadenado no requiere la recarga ni el reinicio de Snort 3.
- Los resultados de generación de perfiles de reglas se guardan en formato JSON en el directorio /ngfw/var/sf/sync/snort_profiling/ y se sincronizan en el FMC.
- El analizador de reglas se sitúa en el Snort 3 e inspecciona el tráfico con el mecanismo de detección de intrusiones del Snort 3. La activación de la generación de perfiles de reglas no tiene ningún impacto apreciable en el rendimiento.

Perfiles de reglas de operación

- El tráfico debe fluir a través del dispositivo
- Inicie la generación de perfiles de reglas seleccionando un dispositivo y haciendo clic en el botón Inicio
    - Al iniciar una sesión de generación de perfiles, se crea una tarea que se puede supervisar en Notificaciones, en Tareas
- La duración predeterminada de una sesión de generación de perfiles de reglas es de 120 minutos
    - La sesión de generación de perfiles de reglas se puede detener antes, antes de finalizar, pulsando el botón Detener
- Los resultados se pueden ver en la GUI y descargarse
- El historial de generación de perfiles muestra los resultados de las sesiones de generación de perfiles anteriores. El usuario puede inspeccionar un resultado de definición de perfiles específico haciendo clic en una tarjeta del panel izquierdo Historial de creación de perfiles.

Menú de perfiles de Snort 3

Se puede acceder a la página Profiling desde el menú Devices > Snort 3 Profiling. La página contiene los perfiles de regla y CPU, divididos en dos fichas.



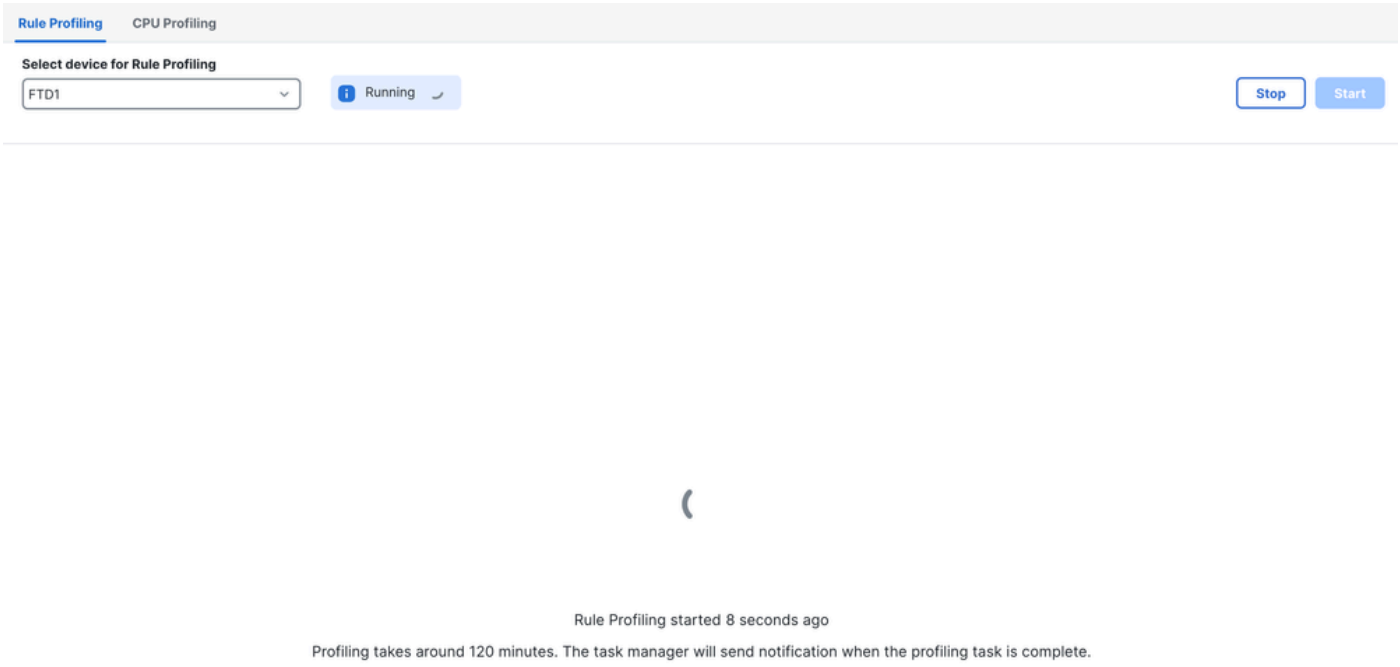
Dispositivos

Iniciar generación de perfiles de reglas

Para iniciar una sesión de generación de perfiles de reglas, haga clic en Iniciar. La sesión se detiene automáticamente después de 120 minutos.

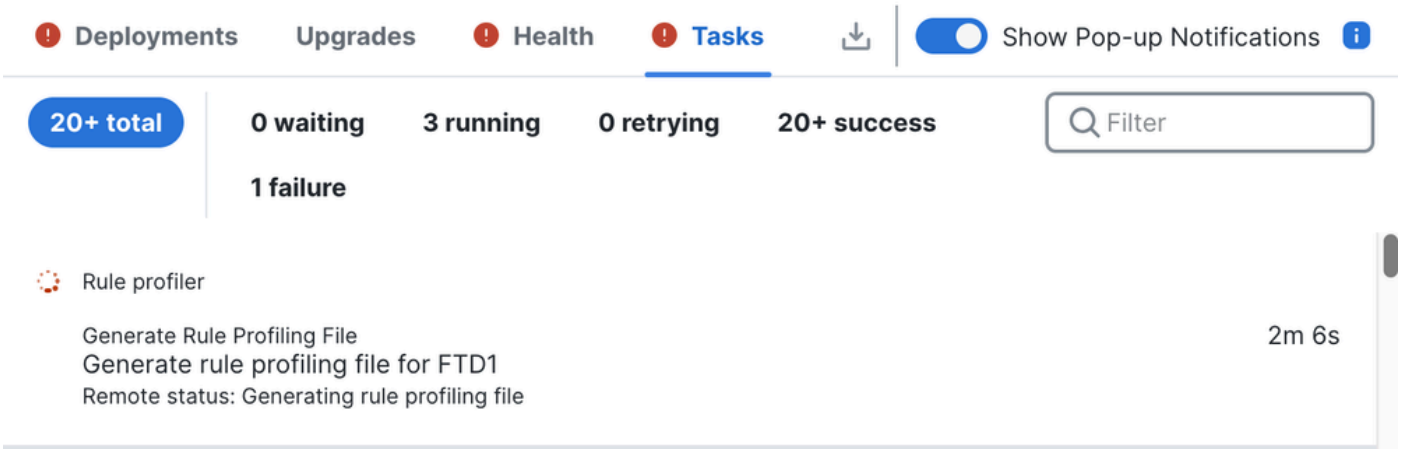
Un usuario no puede configurar la duración de la sesión de creación de perfiles, pero puede detenerla antes de que hayan transcurrido dos horas.

Perfiles de reglas



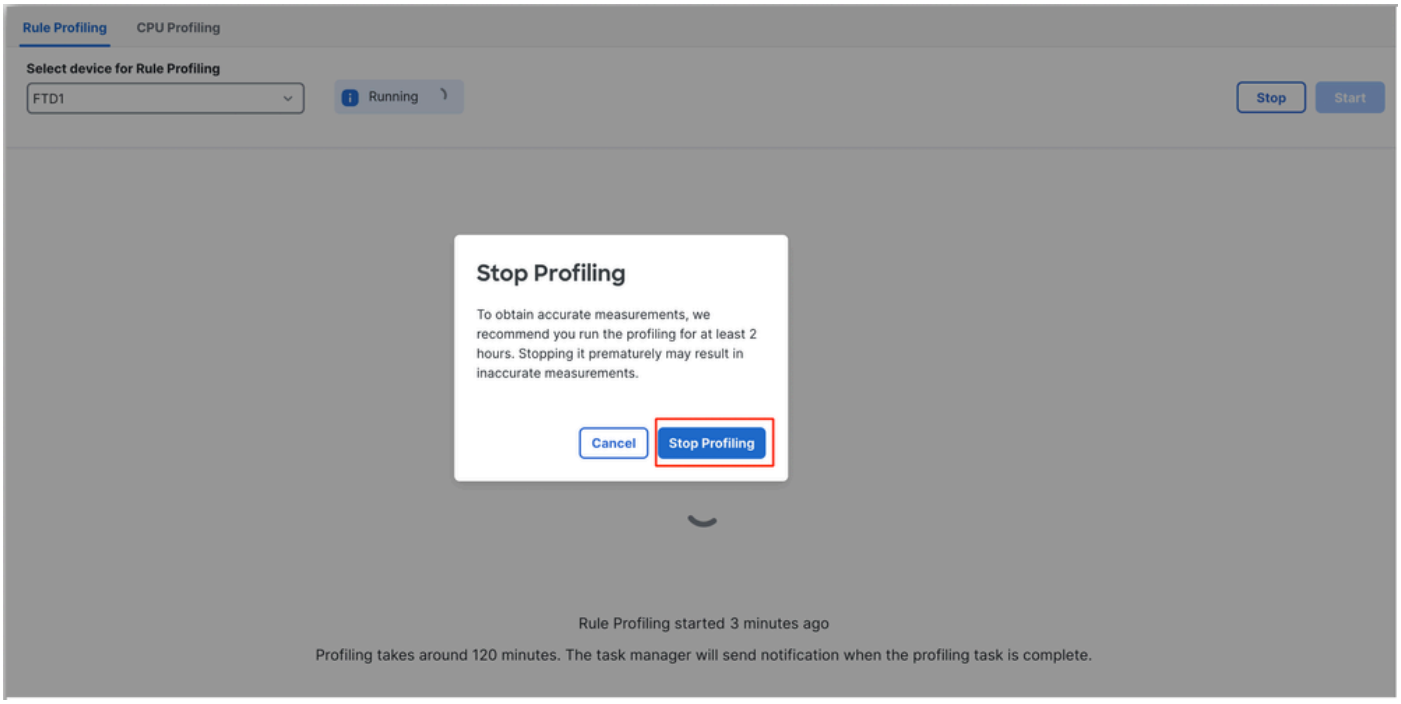
Ejecutándose

Una vez iniciada la sesión de generación de perfiles de reglas, se crea una tarea. Esto se puede verificar en Notifications > Tasks.



Tareas

Para detener una sesión de generación de perfiles de regla en curso, en caso de que tenga que interrumpirla antes de la detención automática, haga clic en Detener y confirmar.



Detener creación de perfiles

Después de seleccionar un dispositivo, el último resultado de generación de perfiles se muestra automáticamente en la sección Resultados de generación de perfiles de reglas.

La tabla contiene estadísticas de las reglas que tardaron más tiempo en procesar ordenadas en orden descendente por el tiempo total (en microsegundos (s) que tardaron.consumidas.

Resultados

Resultados del analizador de reglas

La salida del analizador de reglas para una regla IPS incluye estos campos:

- % de tiempo de Snort: tiempo empleado en procesar la regla, en relación con el tiempo de funcionamiento de Snort 3
- Comprobaciones: número de veces que se ha ejecutado la regla IPS
- Coincidencias: número de veces que la regla IPS coincide completamente
- Alertas: número de veces que la regla IPS ha activado una alerta IPS
- Tiempo (s): tiempo en microsegundos que Snort dedicó a comprobar la regla IPS.
- Promedio de comprobación: tiempo promedio que Snort dedicó a una comprobación de la regla
- Prom./coincidencia: tiempo promedio que Snort dedicó a una comprobación y que resultó en una coincidencia
- Prom./No coincidente: tiempo promedio que Snort dedicó a una comprobación que no dio como resultado una coincidencia
- Tiempos de espera: la regla de número de veces que se excedió el umbral de administración de reglas configurado en la configuración de rendimiento basado en latencia de la política de CA
- Suspendidos: número de veces que se ha suspendido la regla debido a algunas infracciones de umbral consecutivas

Descargue los resultados

- El usuario puede descargar el resultado de la definición de perfiles ("instantánea") haciendo clic en el botón "Descargar instantánea". El archivo descargado está en formato .csv y contiene todos los campos de la página de resultados de generación de perfiles.
- Extraer del archivo .csv de instantánea:

```
Device,Start Time,End Time,GID:SID,Rule Description,% of Snort Time,Rev,Checks,Matches,Alerts,Time ( µs
```

Vista de archivo .csv de instantánea:

Rule_Profiling_172.16.0.102_2024-03-13 11_08_41

Device	Start Time	End Time	GID:SID	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (µs)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	2000:1000001	TEST 1	0.00014	1	4	4	1	284	71	71	0	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:28585	FILE-PDF Adobe Acrobat Reader CTF font head table size overflow attempt	0.00006	8	4	0	0	113	28	0	28	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00003	13	4	0	0	64	16	0	16	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:55993	PROTOCOL-ICMP Microsoft Windows IPv6 DNSSL option record denial of service attempt	0.00002	1	4	0	0	32	8	0	8	0	0

Instantánea

Perfiles de CPU

Descripción general de CPU Profiler Snort 3

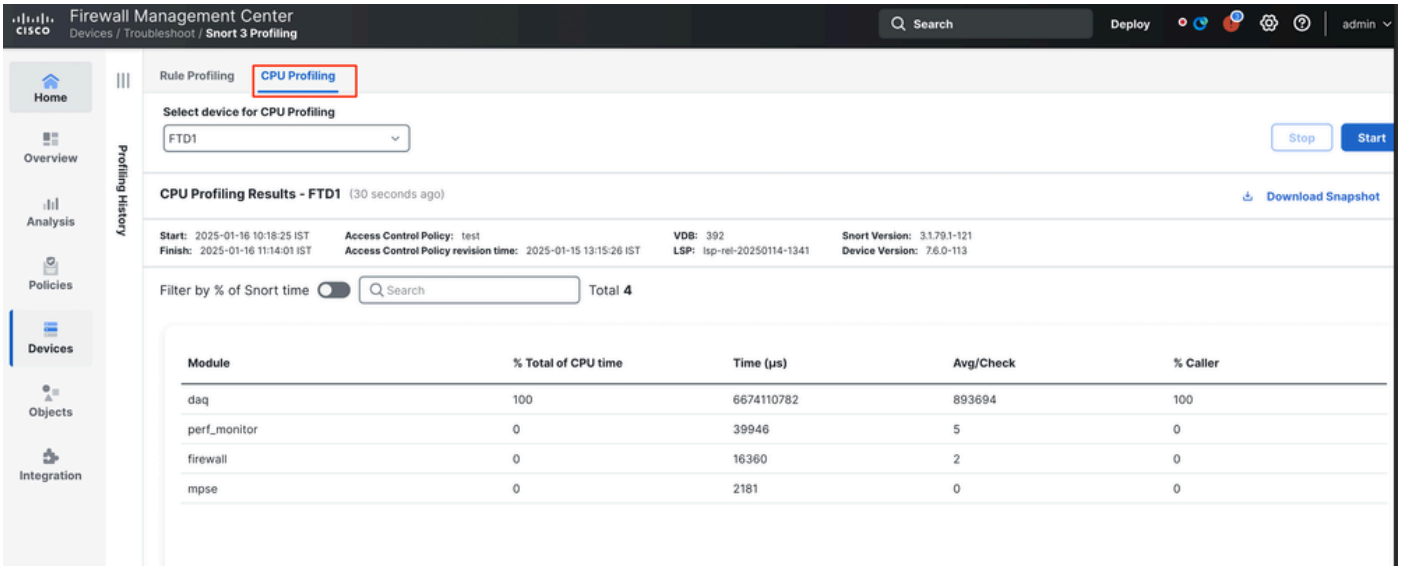
- El analizador de CPU perfila el tiempo de CPU que tardan los módulos/inspectores de Snort 3 en procesar los paquetes en un intervalo de tiempo determinado. Ofrece información sobre la cantidad de CPU que consume cada módulo, con respecto a la CPU total consumida por el proceso Snort 3.
- El uso de CPU Profiler no requiere volver a cargar la configuración ni reiniciar Snort 3, lo que evita el tiempo de inactividad.
- El resultado de CPU Profiler muestra el tiempo de procesamiento empleado por todos los módulos durante la última sesión de generación de perfiles.
- Los resultados de los perfiles de CPU se guardan en formato JSON en el directorio /ngfw/var/sf/sync/cpu_profiling/ y se sincronizan en el directorio FMC /var/sf/peers/<UUID de dispositivo>/sync/cpu_profiling.

- Se ha añadido una nueva página de perfiles de Snort 3 en la interfaz de usuario de FMC
- Se puede acceder a esta página desde la pestaña Devices > Snort 3 Profiling > CPU Profiling
- Utilice Descargar Instantánea en la ficha Perfiles de CPU para descargar una instantánea de los resultados de los perfiles en formato CSV.

Ficha Perfiles de CPU

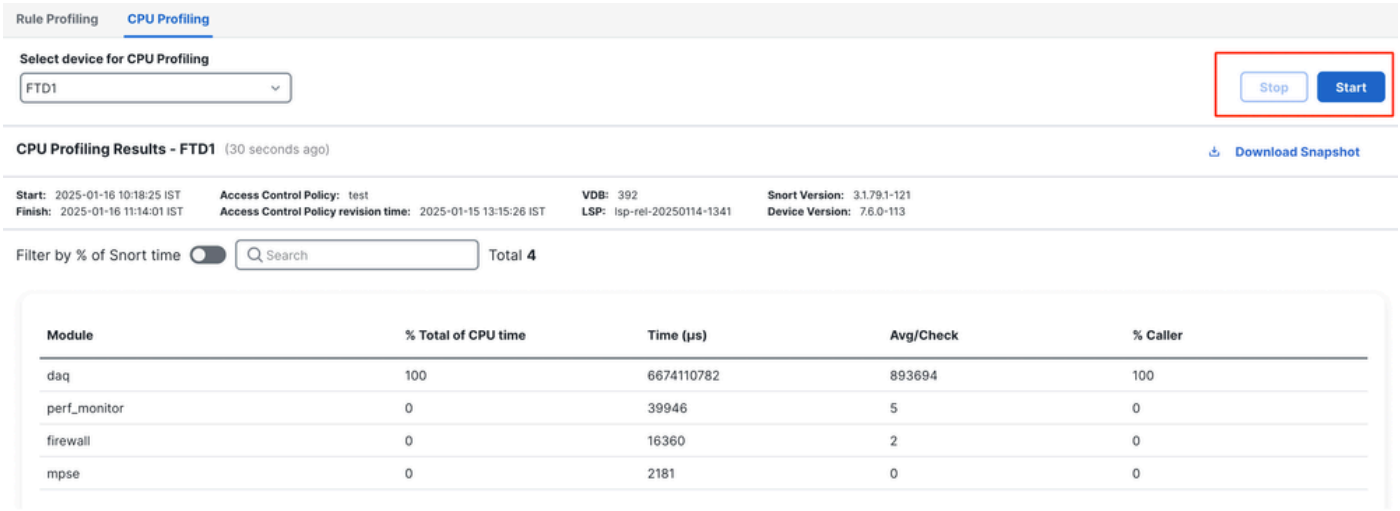
Se accede a la página Perfiles de CPU desde la pestaña Dispositivos > Perfiles de Snort 3 > Perfiles de CPU.

Contiene un selector de dispositivo, los botones Start/Stop, el botón Download Snapshot, una sección de resultados de perfiles y una sección Profiling History en el lado izquierdo que se expande al hacer clic en él.



Perfiles De Cpu

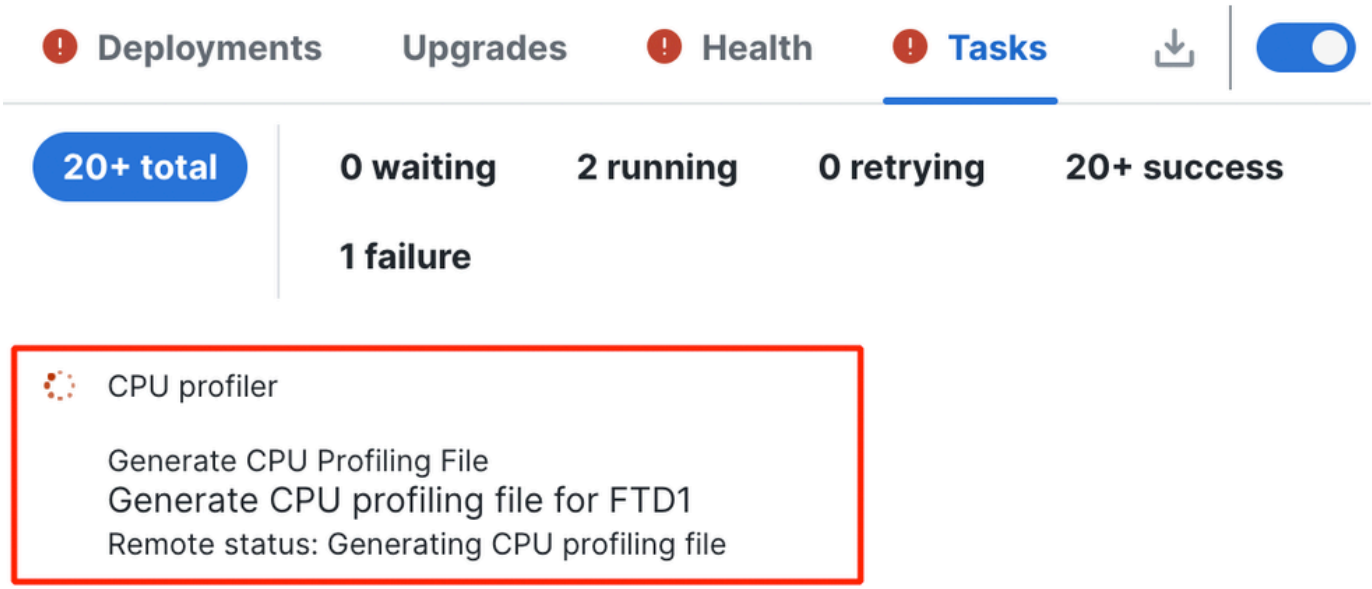
Para iniciar una sesión de generación de perfiles de CPU, haga clic en Start. Esta página se muestra al iniciar la sesión.



Inicio

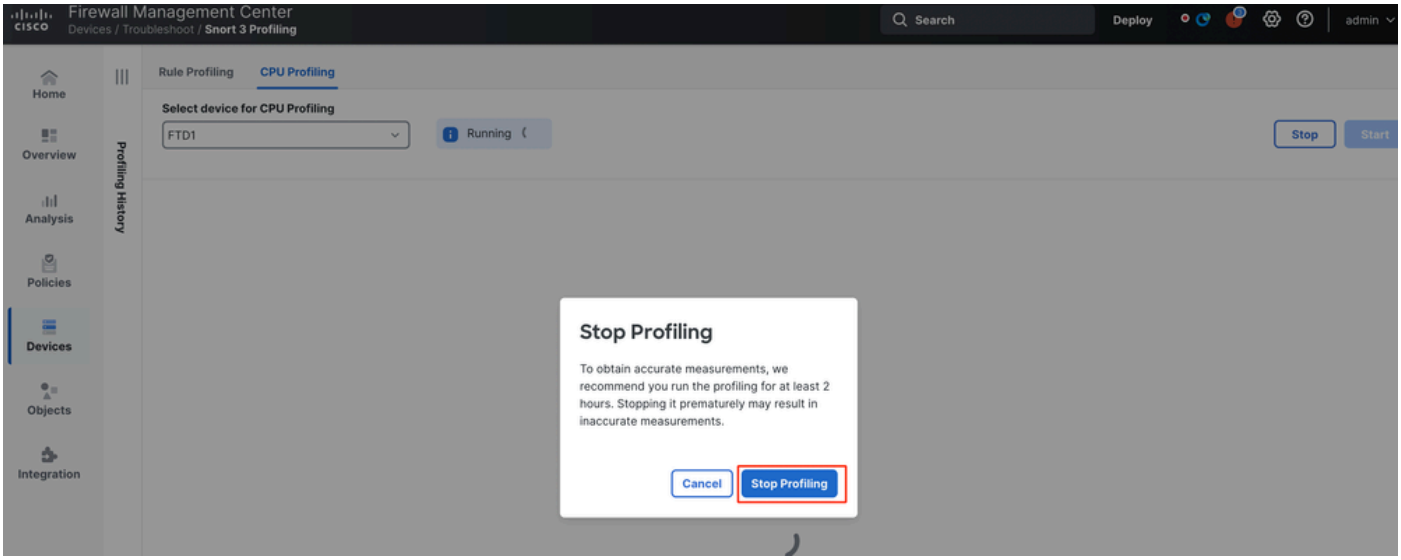
Ejecutándose

Una vez iniciada la sesión de generación de perfiles de CPU, se crea una tarea. Esto se puede verificar en Notifications > Tasks.



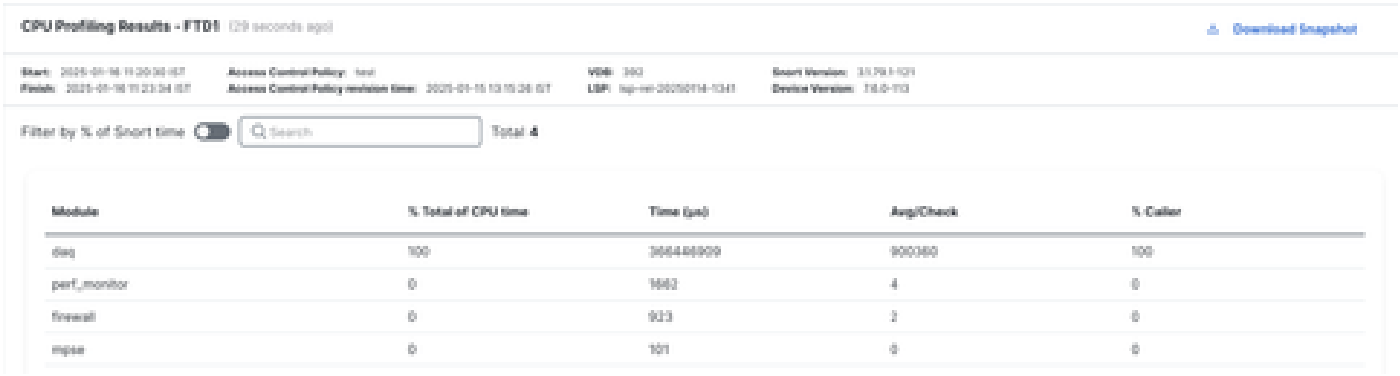
Tareas

- Para detener una sesión de generación de perfiles de CPU en curso, haga clic en Detener.
- Aparecerá un cuadro de diálogo de confirmación. haga clic en Stop Profiling.



Detener ejecución

El último resultado de generación de perfiles se muestra en la sección Resultados de generación de perfiles de CPU.



Resultados

Explicación de los resultados del analizador de CPU

- La columna "Módulo" indica el nombre del módulo/inspector.
- La columna "% del tiempo total de la CPU" indica el porcentaje de tiempo empleado por el módulo con respecto al tiempo total empleado por Snort 3 en el procesamiento del tráfico. Si este valor es considerablemente mayor que el de otros módulos, entonces el módulo está contribuyendo más al rendimiento insatisfactorio de Snort 3.
- "Tiempo ()" representa el tiempo total en microsegundos que tarda cada módulo.
- "Prom./comprobación" representa el tiempo medio que tarda el módulo en cada vez que se invoca el módulo.
- "% Caller" indica el tiempo que tarda un submódulo (si está configurado) con respecto al módulo principal. Se utiliza principalmente con fines de depuración para desarrolladores.

Resultado del analizador de CPU - Descargar instantánea

- El usuario puede descargar la instantánea de los resultados de la generación de perfiles haciendo clic en Descargar instantánea. El archivo descargado está en formato .csv y contiene todos los campos de la página de resultados de generación de perfiles, como se muestra en este ejemplo.
- Extraer del archivo .csv de instantánea:

CPU_Profiling_FTD1_2025-01-16 00_55_45

Device	Start Time	End Time	Module	% Total of CPU time	Time (µs)	Avg/Check	%/Caller
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	daq	100	366446909	900360	100
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	perf_monitor	0	1662	4	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	firewall	0	923	2	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	mpse	0	101	0	0

Instantánea

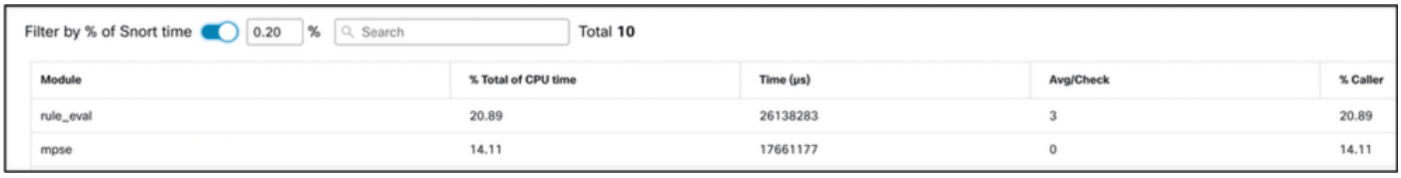
Filtrado de resultados de perfiles de CPU

Los resultados de la definición de perfiles se pueden filtrar mediante:

- "Filtrar por % de tiempo de Snort": permite filtrar los módulos cuya ejecución tardó más del

n% del tiempo de creación de perfiles.
- Buscar: permite realizar una búsqueda de texto en cualquier campo de la tabla de resultados.

Cualquier columna excepto "Módulo" se puede ordenar haciendo clic en su encabezado.



Resultados

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).