Verständnis der Snort 3-Regelprofilierung und der CPU-Profilierung auf der FMC-GUI

Inhalt

Einleitung

In diesem Dokument werden die Snort 3-Regel und die Funktion zur CPU-Profilerstellung in FMC 7.6 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von Snort 3
- Secure FirePOWER Management Center (FMC)
- Sicherer FirePOWER Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieses Dokument gilt für alle FirePOWER-Plattformen
- Secure Firewall Threat Defense Virtual (FTD) mit Software-Version 7.6.0
- Secure Firewall Management Center Virtual (FMC) mit Softwareversion 7.6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Funktionsüberblick

- Regel- und CPU-Profilerstellung gab es bereits in Snort, der Zugriff erfolgte jedoch nur über die FTD-CLI. Ziel dieser Funktion ist es, die Profilerstellungsfunktionen zu erweitern und sie einfacher zu gestalten.
- Aktivieren Sie die Leistungsprobleme der Debugging-Intrusionsregeln, und passen Sie die Regelkonfigurationen eigenständig an, bevor Sie sich an das TAC wenden, um Hilfe bei der Fehlerbehebung zu erhalten.
- Verstehen Sie, welche Module eine unzureichende Leistung aufweisen, wenn Snort 3 eine hohe CPU-Auslastung verbraucht.
- Erstellen Sie eine benutzerfreundliche Methode zum Debuggen und Feinabstimmen von Richtlinien für Eindringversuche und Netzwerkanalysen, um eine bessere Leistung zu erzielen.

Profilierung

- Sowohl die Regelprofilierung als auch die CPU-Profilierung werden auf dem FTD ausgeführt, und die Ergebnisse werden auf dem Gerät gespeichert und vom FMC abgerufen.
- Sie können mehrere Profilerstellungssitzungen gleichzeitig auf verschiedenen Geräten ausführen.
- Sie können die Regelprofilierung und die CPU-Profilierung gleichzeitig ausführen.
- Bei hoher Verfügbarkeit kann die Profilerstellung nur auf dem Gerät gestartet werden, das zu Beginn der Sitzung aktiv ist.
  Für Cluster-Konfigurationen kann die Profilerstellung auf jedem Knoten im Cluster ausgeführt werden.
- Wenn eine Bereitstellung ausgelöst wird, während eine Profilerstellungssitzung ausgeführt wird, wird dem Benutzer eine Warnung angezeigt.

Wenn der Benutzer die Warnung ignoriert und bereitstellt, wird die aktuelle Profilerstellungssitzung abgebrochen, und das Profilerergebnis zeigt eine entsprechende Meldung an.

Eine neue Profilerstellungssitzung muss gestartet werden, ohne durch eine Bereitstellung unterbrochen zu werden, um die tatsächlichen Profilerstellungsergebnisse zu erhalten.

Regelprofiler

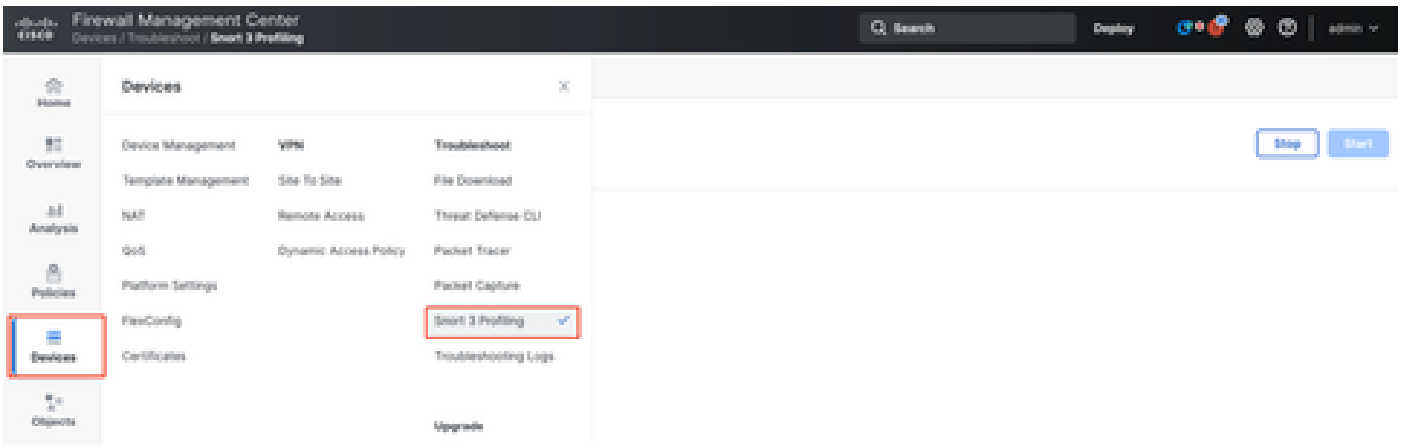
- Snort 3 Rule Profiler sammelt Daten über die Zeit, die für die Verarbeitung einer Reihe von Snort 3 Intrusion-Regeln aufgewendet wurde. Dadurch werden potenzielle Probleme hervorgehoben und Regeln mit unzureichender Leistung angezeigt.
- Rule Profiler zeigt die 100 IPS-Regeln an, deren Überprüfung am längsten gedauert hat.
- Das Auslösen von Rule Profiler erfordert kein Neuladen oder Neustarten von Snort 3.
- Ergebnisse der Regelprofilierung werden im JSON-Format im Verzeichnis /ngfw/var/sf/sync/snort_profiling/ gespeichert und auf dem FMC synchronisiert.
- Regelprofiler wird in Snort 3 platziert und überprüft den Datenverkehr mithilfe des Intrusion Detection-Mechanismus von Snort 3. Die Aktivierung der Regelprofilierung hat keine spürbaren Auswirkungen auf die Leistung.

Erstellen von Regelprofilen

- Datenverkehr muss durch das Gerät fließen
- Starten Sie die Regelprofilierung, indem Sie ein Gerät auswählen und dann auf die Schaltfläche Start klicken.
    - Durch Starten einer Profilerstellungssitzung wird eine Aufgabe erstellt, die in Benachrichtigungen unter Aufgaben überwacht werden kann.
- Die Standarddauer einer Regelprofilsitzung beträgt 120 Minuten.
    - Die Regelprofilsitzung kann früher, vor Abschluss, beendet werden, indem Sie auf die Schaltfläche Stopp drücken.
- Die Ergebnisse können in der Benutzeroberfläche angezeigt und heruntergeladen werden.
- Der Profilverlauf zeigt die Ergebnisse der vorherigen Profilerstellungssitzungen an. Der Benutzer kann ein bestimmtes Profilierungsergebnis überprüfen, indem er auf eine Karte im linken Bereich des Profiling History klickt.

Menü "Snort 3 Profiling"

Die Profiling-Seite kann über das Menü Devices > Snort 3 Profiling aufgerufen werden. Die Seite enthält sowohl die Regel- als auch die CPU-Profilerstellung, die in zwei Registerkarten unterteilt sind.

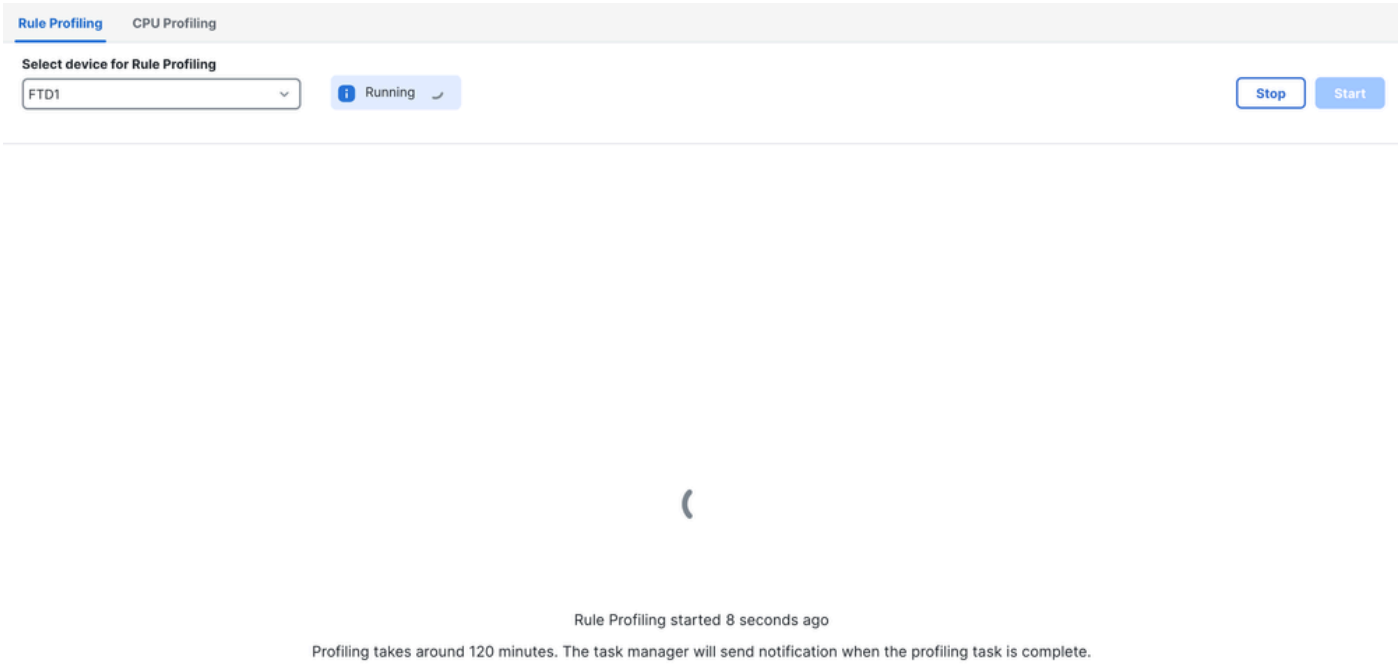


Regelprofilierung starten

Klicken Sie auf Start, um eine Sitzung zur Erstellung von Regelprofilen zu starten. Die Sitzung wird nach 120 Minuten automatisch beendet.

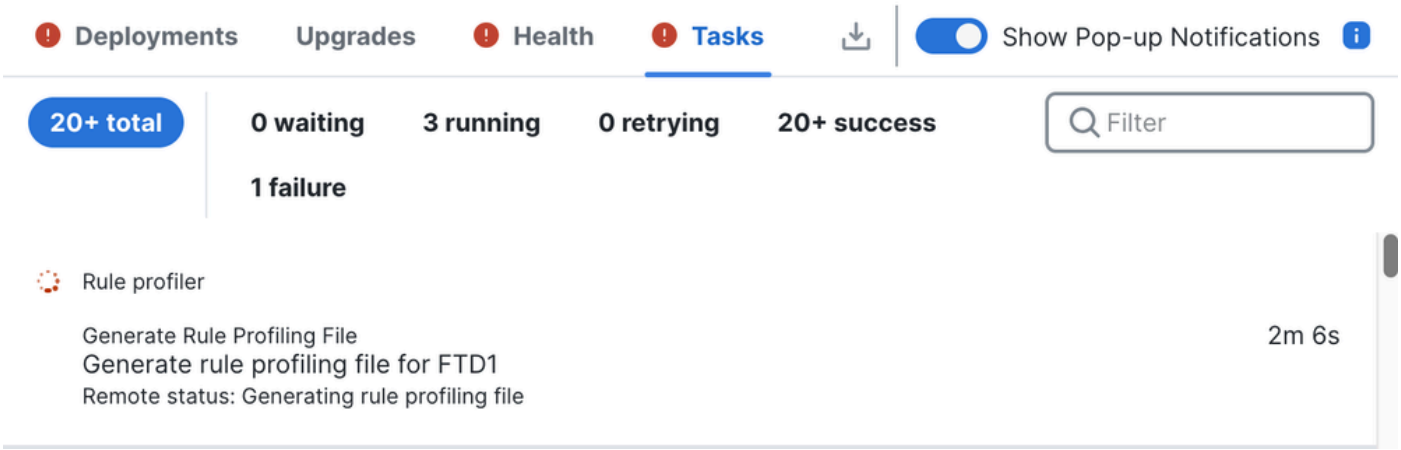
Ein Benutzer kann die Dauer der Profilerstellungssitzung nicht konfigurieren, sie jedoch beenden, bevor die zwei Stunden verstrichen sind.

Regelprofilierung



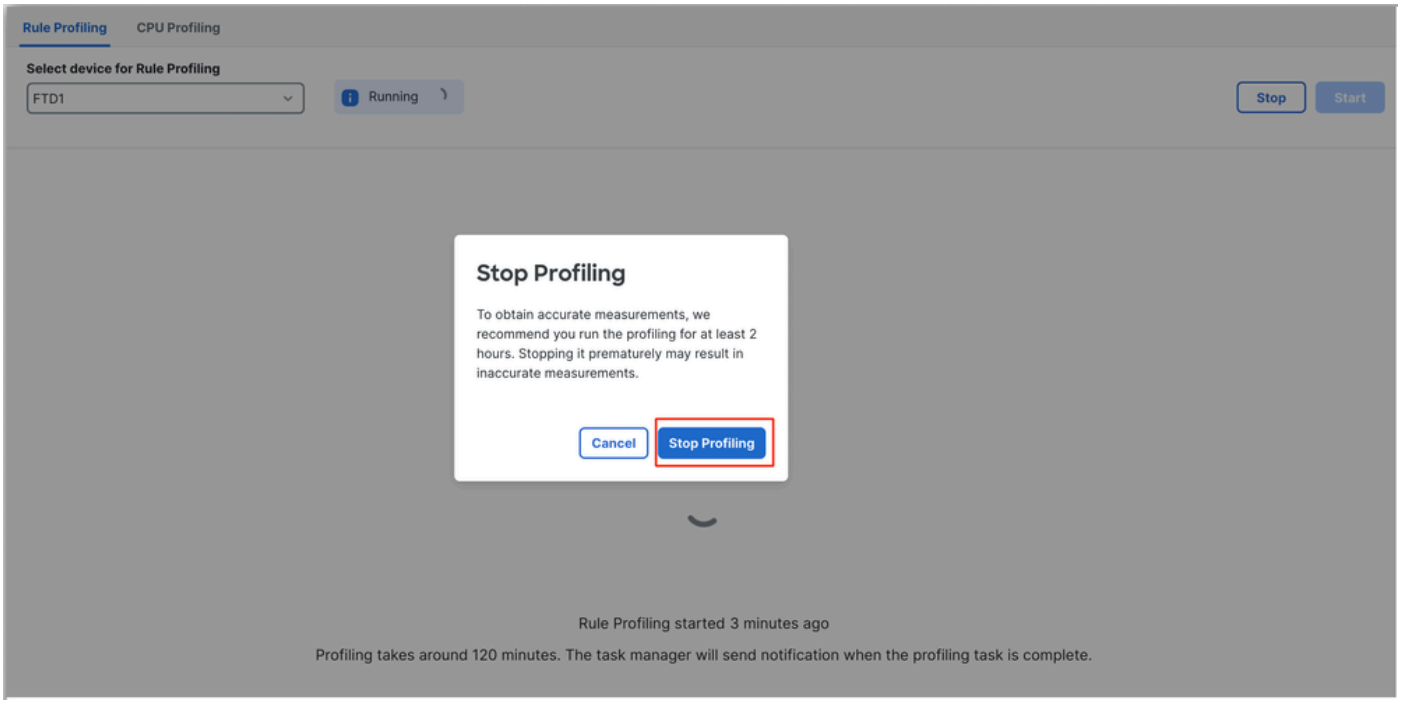
Ausgeführt

Nachdem die Regelprofilierungssitzung gestartet wurde, wird eine Aufgabe erstellt. Dies kann unter Benachrichtigungen > Aufgaben überprüft werden.



Aufgaben

Um eine laufende Regelprofilerstellungssitzung zu beenden, klicken Sie auf Beenden und bestätigen, falls Sie sie vor dem automatischen Beenden unterbrechen müssen.



Profilerstellung beenden

Nachdem Sie ein Gerät ausgewählt haben, wird das aktuelle Profilerstellungsergebnis automatisch im Abschnitt Ergebnisse der Regelprofilierung angezeigt.

Die Tabelle enthält Statistiken für Regeln, die am meisten Zeit für die Verarbeitung benötigten, sortiert in absteigender Reihenfolge nach der Gesamtzeit (in Mikrosekunden (µs)), die sie verbraucht haben.

Ergebnisse der Regelprofilerstellung

Die Regelprofilerausgabe für eine IPS-Regel umfasst folgende Felder:

- % der Snort-Zeit - Die für die Verarbeitung der Regel aufgewendete Zeit im Verhältnis zur Zeit des Snort 3-Vorgangs.
- Prüfungen - Anzahl der Ausführungsvorgänge der IPS-Regel
- Übereinstimmungen - Anzahl der Übereinstimmungen der IPS-Regel
- Warnungen - Anzahl der Auslöser einer IPS-Warnung durch die IPS-Regel
- Zeit (µ s) - Zeit in Mikrosekunden Snort verbrachte mit der Überprüfung der IPS-Regel
- Durchschn./Scheck - Durchschnittliche Zeit, die Snort mit einer Überprüfung der Regel verbracht hat
- Durchschn./Übereinstimmung - Durchschnittliche Zeit, die Snort für einen Scheck aufgewendet hat, der zu einem Spiel geführt hat
- Durchschn./Nicht-Übereinstimmung - Durchschnittliche Zeit, die Snort für einen Scheck aufgewendet hat, der nicht zu einer Übereinstimmung geführt hat
- Timeouts - Anzahl der Überschreitungen der Regelbehandlung durch die Regel - Schwellenwert, der in den latenzbasierten Leistungseinstellungen der Wechselstromrichtlinie konfiguriert wurde
- Unterbrechungen - Anzahl der Unterbrechungen der Regel aufgrund aufeinander folgender Schwellenwertverletzungen

Ergebnisse herunterladen

- Der Benutzer kann das Profiling-Ergebnis ("Snapshot") durch Klicken auf die Schaltfläche "Snapshot herunterladen" herunterladen. Die heruntergeladene Datei hat das CSV-Format und enthält alle Felder auf der Ergebnisseite der Profilerstellung.
- Aus der Snapshot-CSV-Datei extrahieren:

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

Snapshot-CSV-Dateiansicht:

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 OTF 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

CPU-Profilierung

Übersicht: Snort 3 CPU Profiler

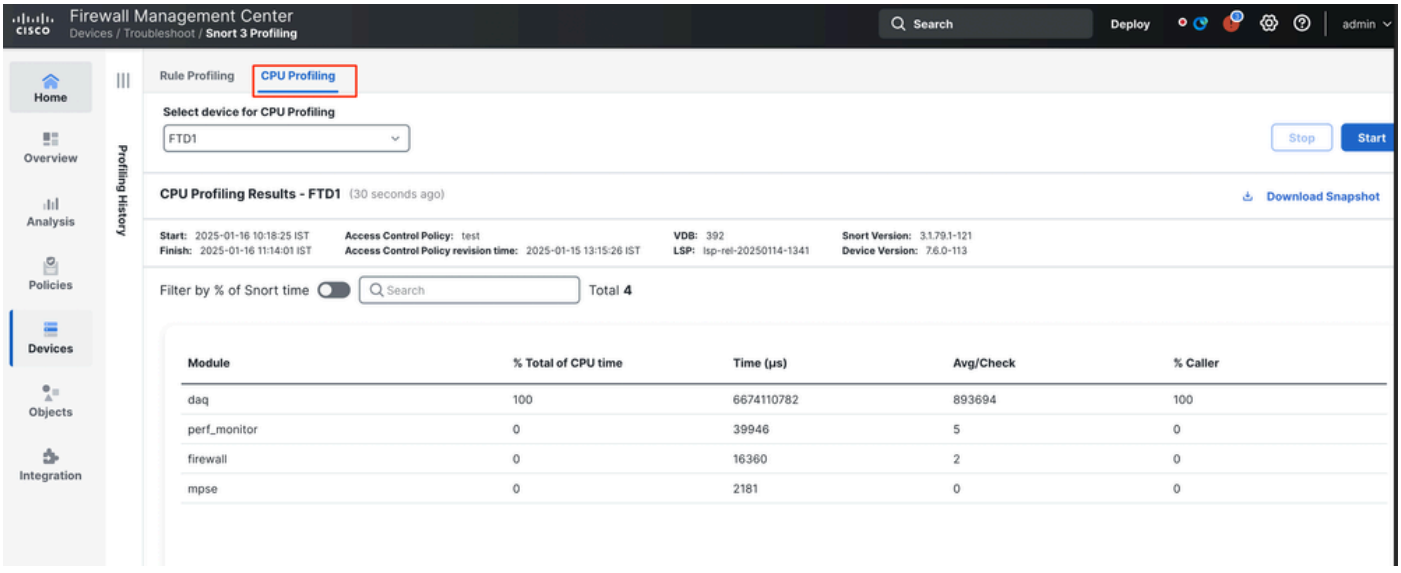
- Der CPU-Profiler ermittelt die CPU-Zeit, die Module/Inspektoren von Snort 3 benötigt haben, um Pakete in einem bestimmten Zeitintervall zu verarbeiten. Es gibt einen Einblick, wie viel CPU jedes Modul verbraucht, im Vergleich zur gesamten CPU, die vom Snort 3-Prozess verbraucht wird.
- Die Verwendung von CPU Profiler erfordert kein Neuladen der Konfiguration oder Neustarten von Snort 3, wodurch Ausfallzeiten vermieden werden.
- Das Ergebnis der CPU-Profilerstellung zeigt die Verarbeitungszeit an, die von allen Modulen während der letzten Profilerstellung benötigt wurde.
- Die Ergebnisse der CPU-Profilerstellung werden im JSON-Format im Verzeichnis "/ngfw/var/sf/sync/cpu_profiling/" gespeichert und im Verzeichnis "FMC /var/sf/peers/<UUID des Geräts>/sync/cpu_profiling" synchronisiert.

- Eine neue Snort 3-Profiling-Seite wurde der FMC-Benutzeroberfläche hinzugefügt.
- Diese Seite kann über die Registerkarte Devices > Snort 3 Profiling (Geräte > Snort 3 Profiling) aufgerufen werden.
- Verwenden Sie Snapshot herunterladen auf der Registerkarte "CPU Profiling", um einen Snapshot der Profilierungsergebnisse im CSV-Format herunterzuladen.

Registerkarte "CPU-Profilerstellung"

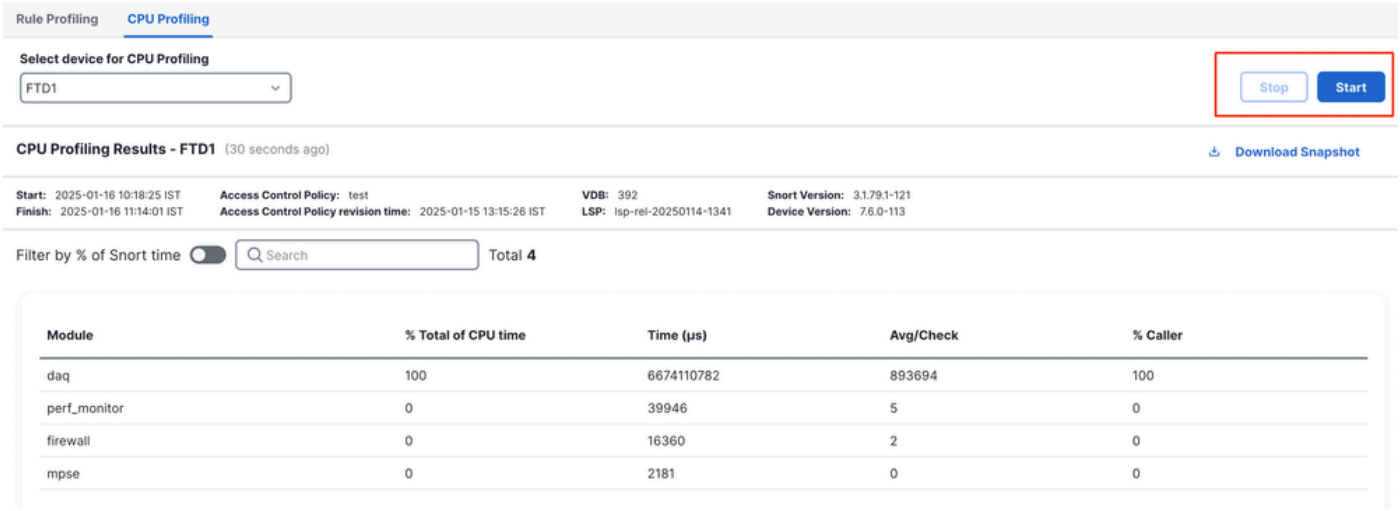
Die Seite "CPU Profiling" wird über die Registerkarte "Devices" (Geräte) > "Snort 3 Profiling" (Profilerstellung in Snort 3) > "CPU Profiling" aufgerufen.

Es enthält eine Geräteauswahl, Start-/Stopp-Schaltflächen, die Schaltfläche Snapshot herunterladen, einen Abschnitt mit den Profilergebnissen und einen Abschnitt mit dem Profilverlauf auf der linken Seite, der beim Klicken darauf erweitert wird.



CPU-Profilierung

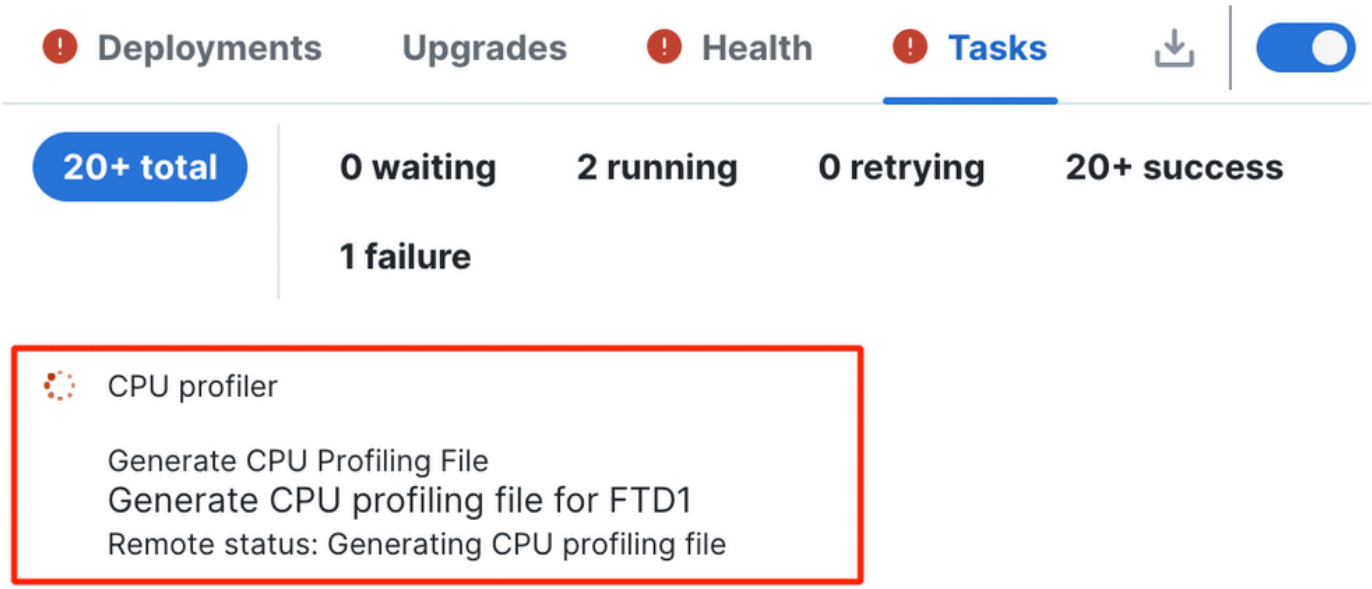
Um eine CPU-Profilerstellungssitzung zu starten, klicken Sie auf Start. Diese Seite wird angezeigt, wenn die Sitzung gestartet wird.



Start

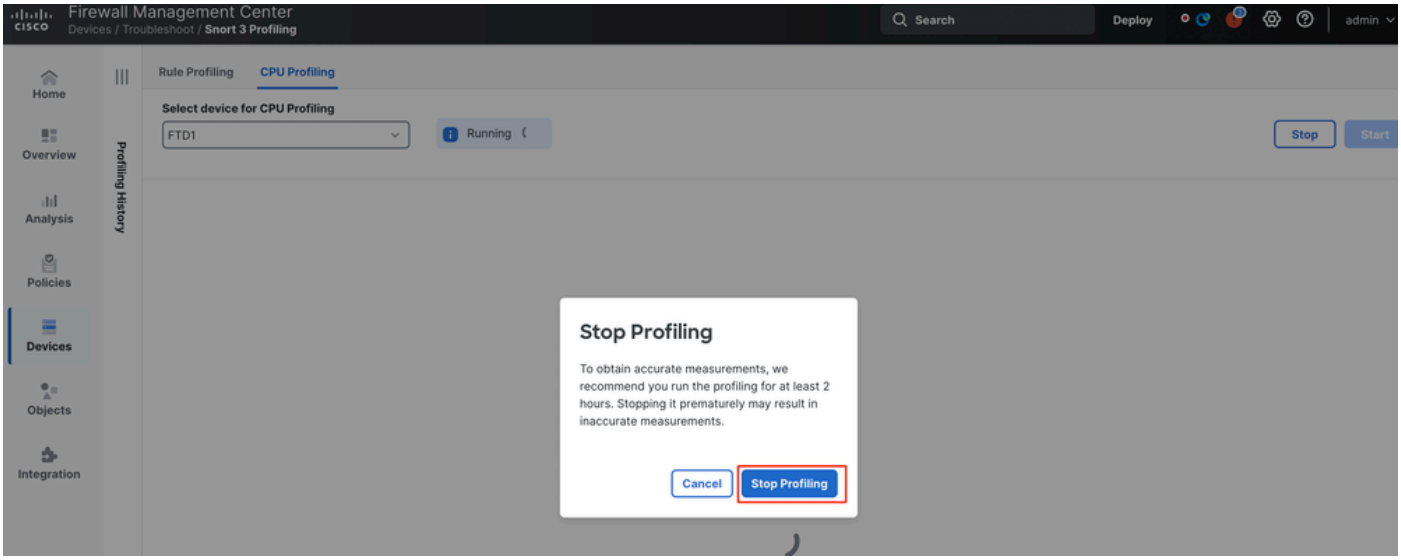
Ausgeführt

Nachdem die CPU-Profilerstellungssitzung gestartet wurde, wird eine Aufgabe erstellt. Dies kann unter Benachrichtigungen > Aufgaben überprüft werden.



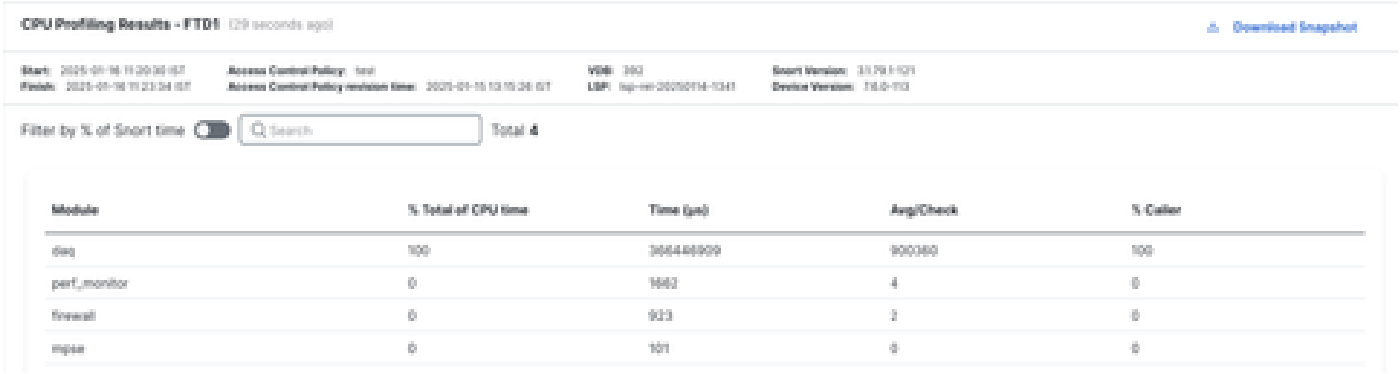
Aufgaben

- Um eine laufende CPU-Profilerstellungssitzung zu beenden, klicken Sie auf Beenden.
- Ein Bestätigungsdialogfeld wird angezeigt. auf Profilerstellung beenden klicken.



Ausführung beenden

Das neueste Profilergebnis wird im Abschnitt "Ergebnisse der CPU-Profilerstellung" angezeigt.



Ergebnisse

Ergebnisse der CPU-Profiler

- Spalte "Modul" bezeichnet den Namen des Moduls/Inspektors.
- Spalte "% Gesamt der CPU-Zeit" gibt den Prozentsatz der Zeit an, die das Modul im Verhältnis zur Gesamtzeit von Snort 3 für die Verarbeitung des Datenverkehrs benötigt. Wenn dieser Wert wesentlich größer ist als der anderer Module, dann trägt das Modul mehr zu einer unbefriedigenden Leistung von Snort 3 bei.
- "Zeit (µ s)" bezeichnet die Gesamtzeit in Mikrosekunden, die von jedem Modul benötigt wird.
- "Durchschn./Prüfen" steht für die durchschnittliche Zeit, die das Modul für jeden Aufruf des Moduls benötigt.
- "% Caller" bezeichnet die Zeit, die das Untermodul (falls konfiguriert) in Bezug auf das Hauptmodul benötigt. Es wird hauptsächlich zum Debuggen von Entwicklern verwendet.

Ergebnis des CPU-Profilers - Snapshot herunterladen

- Der Benutzer kann den Profilerstellungsergebnis-Snapshot herunterladen, indem er auf Snapshot herunterladen klickt. Die heruntergeladene Datei hat das CSV-Format und enthält alle Felder auf der Ergebnisseite der Profilerstellung, wie in diesem Beispiel gezeigt.
- Aus der Snapshot-CSV-Datei extrahieren:

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

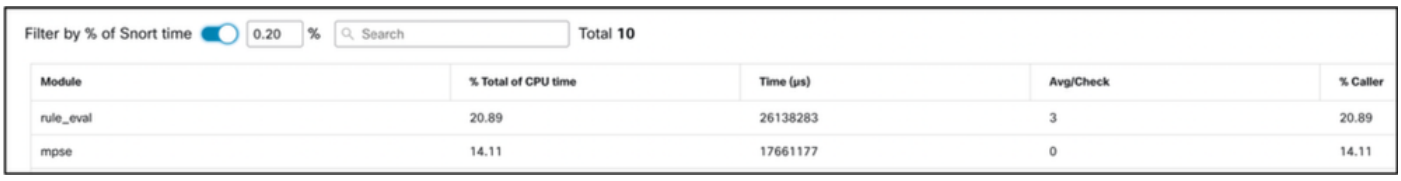
Snapshot

Ergebnisfilterung der CPU-Profilerstellung

Profilergebnisse können gefiltert werden mit:

- "Filtern nach % der Snort-Zeit": Ermöglicht das Herausfiltern von Modulen, deren Ausführung mehr als n % der Profilerstellungszeit in Anspruch nahm.
- Suchen: Ermöglicht die Textsuche in einem beliebigen Feld in der Ergebnistabelle.

Jede Spalte mit Ausnahme von "Modul" kann durch Klicken auf die Überschrift sortiert werden.



Ergebnisse

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.