Snuit 3-regelprofilering en CPU-profilering op FMC GUI begrijpen

Inhoud

Inleiding

In dit document worden de functie snort 3 en CPU-profilering op FMC 7.6 beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

· Kennis van snort 3
· Secure Firepower Management Center (FMC)
· Secure Firepower Threat Defence (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit document is van toepassing op alle FirePOWER-platforms
- Software voor Secure Firewall Threat Defense Virtual (FTD), versie 7.6.0
- Software voor Secure Firewall Management Center Virtual (FMC), versie 7.6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht van functies

- Regel- en CPU-profilering bestond al in Snort, maar was alleen toegankelijk via de FTD CLI. Het doel van deze functie is om profiling mogelijkheden uit te breiden en het eenvoudiger te maken.
- Laat debug van de prestatieskwesties van de inbraakregel toe en pas de regelconfiguraties op hun toe alvorens uit aan TAC voor het oplossen van probleemhulp te bereiken.
- Begrijp welke modules onbevredigende prestaties hebben wanneer Snort 3 hoge CPU verbruikt.
- Creëer een gebruiksvriendelijke manier om inbraakbeleid en netwerkanalysebeleid te debuggen en te verfijnen voor betere prestaties.

Profileren

- Zowel Rule Profiling als CPU Profiling lopen op de FTD en hun resultaten worden op apparaat opgeslagen en door FMC getrokken.
- U kunt meerdere profileringssessies tegelijkertijd op verschillende apparaten uitvoeren.
- U kunt de opties Regelprofilering en CPU-profilering tegelijkertijd uitvoeren.
- In het geval van Hoge Beschikbaarheid, kan het profileren slechts op het apparaat worden gelanceerd dat bij het begin van de zitting actief is.
  Voor geclusterde instellingen kan profilering worden uitgevoerd op elk knooppunt in het cluster.
- Als een plaatsing wordt teweeggebracht terwijl er een het profileren zitting lopend is, wordt een waarschuwing getoond aan de gebruiker.

Als de gebruiker ervoor kiest om de waarschuwing te negeren en te implementeren, annuleert dit de huidige profileringssessie en toont het profielresultaat een bericht hierover.

Een nieuwe profiling sessie moet worden gestart zonder te worden onderbroken door een inzet om de daadwerkelijke profiling resultaten te krijgen.

Regelprofiler

- Snort 3 Regel profiler verzamelt gegevens over de hoeveelheid tijd die besteed is aan het verwerken van een set Snort 3 inbraakregels, waardoor potentiële problemen worden benadrukt, waarbij regels met onbevredigende prestaties worden getoond.
- Regel Profiler toont de 100 IPS regels die de meeste tijd om te controleren vergen.
- Voor het activeren van regelprofiler is geen herladen of opnieuw opstarten via Snort 3 nodig.

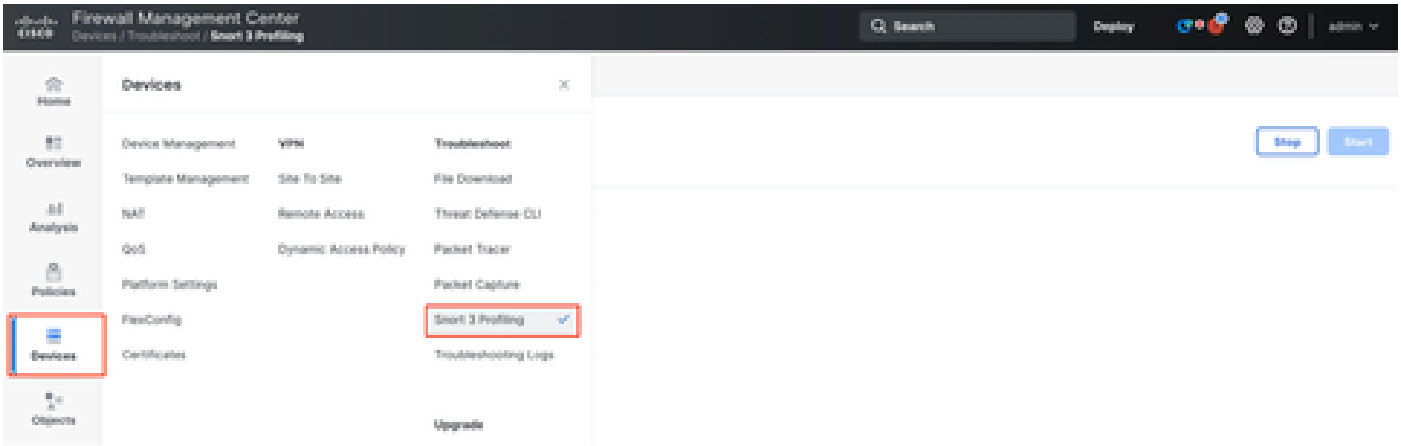
- De resultaten van het opstellen van regels worden opgeslagen in JSON-formaat in /ngfw/var/sf/sync/snort_profiling/-directory en gesynchroniseerd op het VCC.
- Regel profiler ligt binnen Snort 3 en inspecteert verkeer met het snort 3 inbraakdetectiemechanisme; het inschakelen van de Regel profilering heeft geen merkbare invloed op de prestaties.

Profilering van werkregels

- Het verkeer moet door het apparaat stromen
- Start Regel Profiling door een apparaat te kiezen en klik vervolgens op de knop Start
  - Wanneer u een profileringssessie start, wordt een taak gemaakt die kan worden bewaakt in meldingen onder Taken
- De standaardduur van een sessie voor regelprofilering is 120 minuten
  - De sessie voor regelprofilering kan eerder voor de voltooiing worden gestopt door op de knop Stop te drukken
- De resultaten kunnen in de GUI worden bekeken en worden gedownload
- De Profiling Geschiedenis toont de vorige het profileren sessieresultaten. De gebruiker kan een specifiek profileringsresultaat inspecteren door op een kaart van het Linkerpaneel van de Geschiedenis van het Profileren te klikken.

Sneltoets 3 Profielmenu

De pagina Profileren is toegankelijk via het menu Apparaten > Snelheid 3 Profileren. De pagina bevat zowel Rule- als CPU-profilering, verdeeld in twee tabbladen.



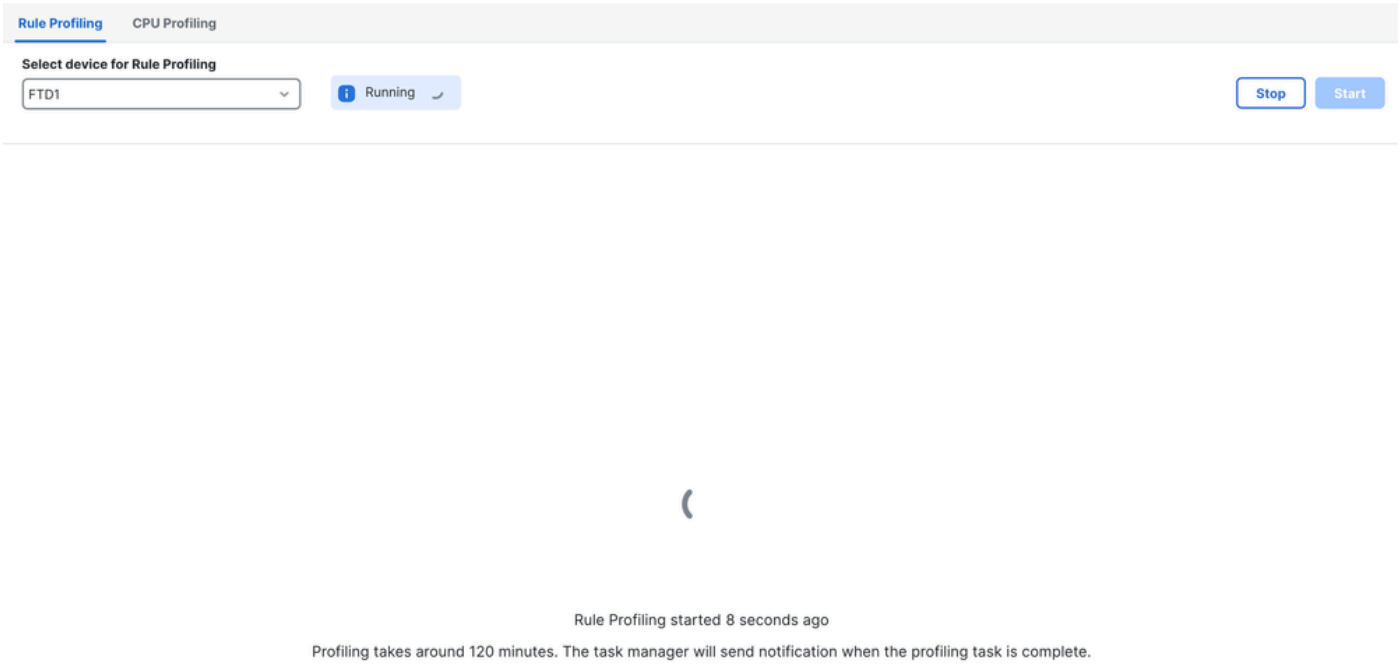
Apparaten

Regel-profilering starten

Klik op Start om een sessie met regelprofilering te starten. De sessie wordt automatisch na 120 minuten stopgezet.

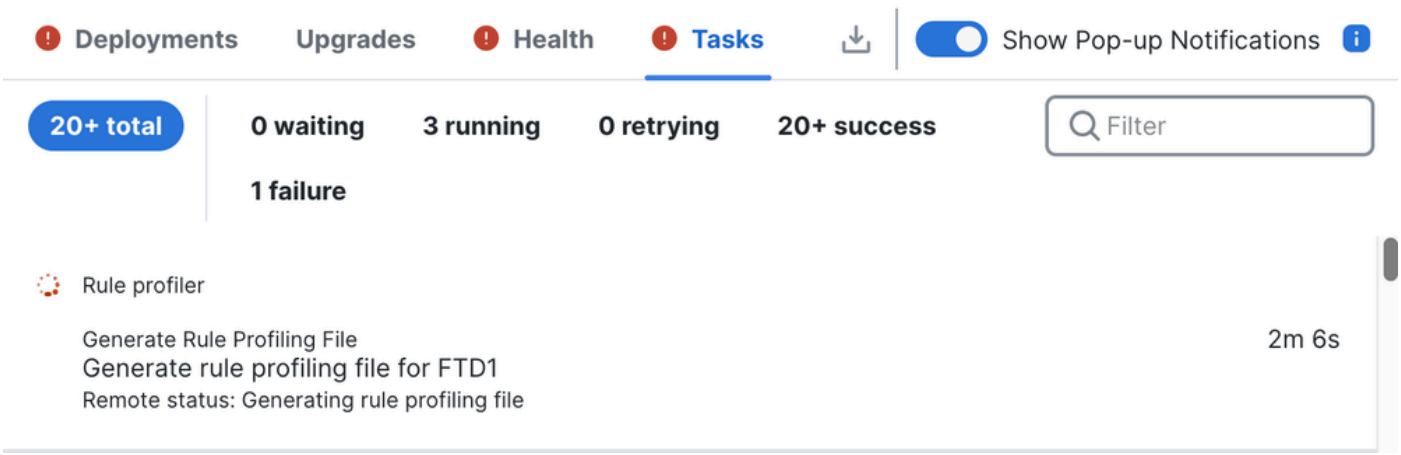
Een gebruiker kan de lengte van de profileringssessie niet configureren maar kan deze stoppen voordat de twee uur zijn verstreken.

Regelprofilering



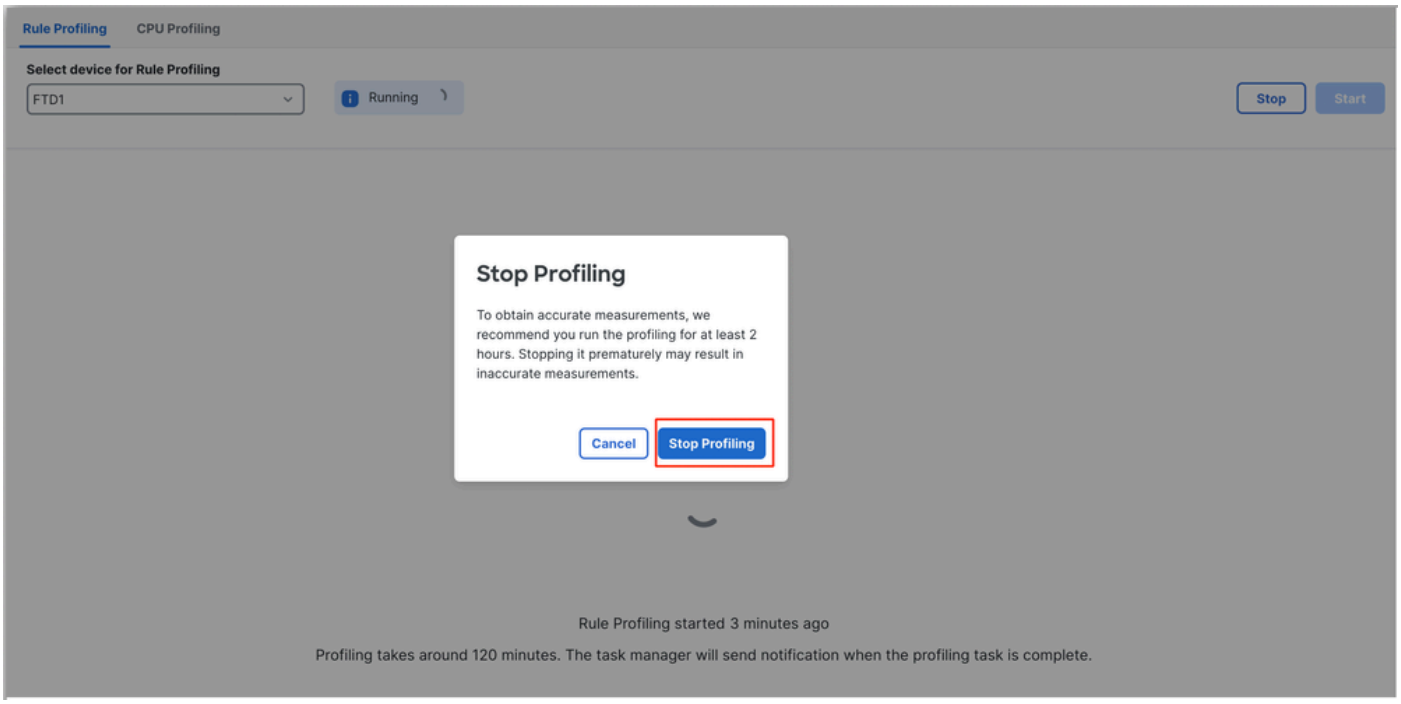
Lopen

Nadat de regel-profileringssessie is gestart, wordt een taak gemaakt. Dit kan worden gecontroleerd in Meldingen > Taken.



Taken

Om een regel profileren sessie die bezig is te stoppen, voor het geval dat u moet onderbreken voor de automatische stop, klik op Stop en bevestig.



Stop-profilering

Nadat u een apparaat hebt geselecteerd, wordt het laatste resultaat van de profilering automatisch weergegeven in het gedeelte Resultaten van regelprofilering.

De tabel bevat statistieken voor regels die de meeste tijd nodig hebben gehad om te verwerken, gesorteerd in aflopende volgorde op basis van de totale tijd (in microseconden) die ze hebben ingenomen.

Resultaten

Resultaten van regelprofiler

De output van het profiel van de regel voor een IPS regel omvat deze gebieden:

- % van Snort-tijd - tijd die aan de verwerking van de regel is besteed, in verhouding tot de tijd van snort 3-bewerking
- Controles - Aantal keren dat de IPS-regel is uitgevoerd
- Overeenkomsten - Aantal keren dat de IPS-regel volledig is aangepast
- Waarschuwingen - Aantal keren dat een IPS-waarschuwing is geactiveerd door de IPS-regel
- Tijd (µs) - Tijd in microseconden die aan het controleren van de IPS-regel wordt besteed
- Gemiddelde/controle - Gemiddelde tijd Snort besteed aan één controle van de regel
- Gem/overeenkomst - Gemiddelde tijd Snort besteed aan één controle die resulteerde in een match
- Gem./niet-overeenkomst - Gemiddelde tijd besteed aan één controle die niet resulteerde in een overeenkomst

- Time-outs - Regel aantal keren overschreden de regelafhandeling - Drempel geconfigureerd in de op Latency-gebaseerde prestatie-instellingen van het AC-beleid
- Opschortingen - Aantal keren dat de regel is opgeschort vanwege een aantal opeenvolgende overschrijdingen van drempelwaarden

Resultaten downloaden

- De gebruiker kan het profileringsresultaat ("snapshot") downloaden door op de knop "Snapshot downloaden" te klikken. Het gedownloade bestand heeft de indeling .csv en bevat alle velden van de pagina met profielresultaten.
- Uit het .csv-bestand snapshot halen:

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

Snapshot .csv bestandsweergave:

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

momentopname

CPU-profilering

Snort 3 CPU profieloverzicht

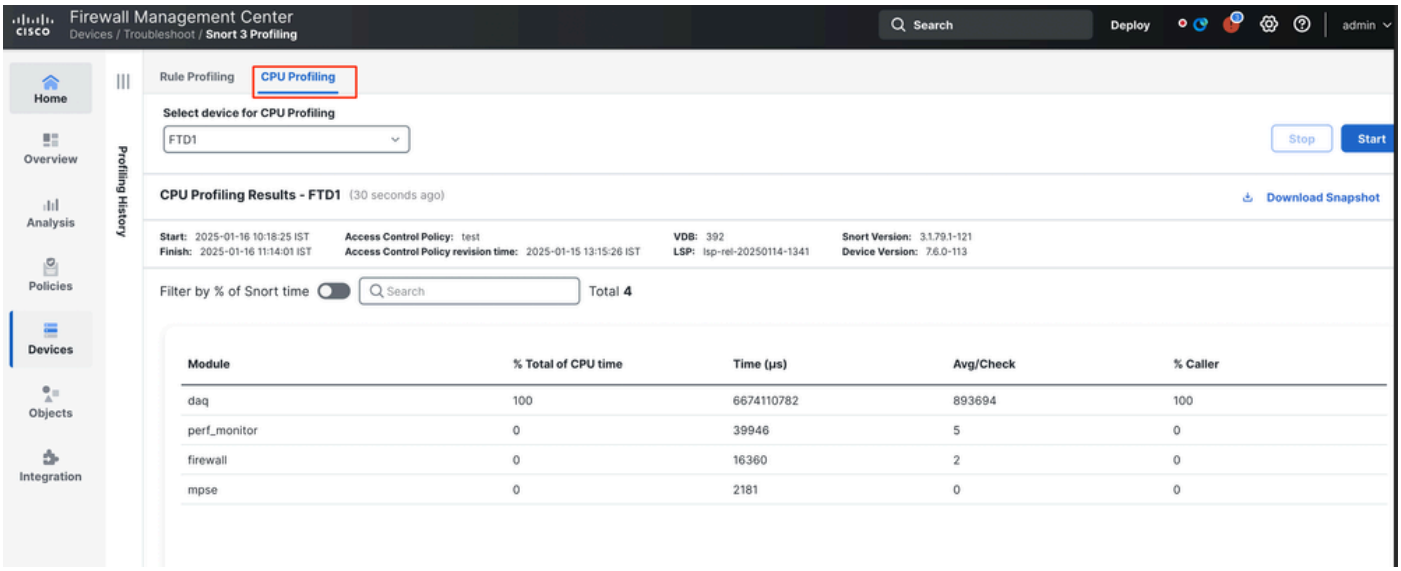
- CPU profiler profielen de CPU-tijd die modules/inspecteurs van Snuit 3 nemen om pakketten in een gegeven tijdsinterval te verwerken. Het geeft inzicht in hoeveel CPU elke module verbruikt, vergeleken met de totale CPU die verbruikt wordt door Snort 3-proces.
- Voor het gebruik van CPU-profiler hoeft de configuratie niet opnieuw te worden geladen of het opnieuw starten van Sneltoets 3, waardoor downtime wordt voorkomen.
- Het resultaat van de CPU-profiler toont de verwerkingstijd die alle modules tijdens de laatste profileringssessie hebben genomen.
- De resultaten van de CPU-profilering worden opgeslagen in JSON-indeling onder de directory /ngfw/var/sf/sync/cpu_profiling/ en gesynchroniseerd in de directory FMC /var/sf/peers/<device UUID>/sync/cpu_profiling.

- Een nieuwe Snort 3 profiling pagina werd toegevoegd in FMC UI
- Deze pagina is toegankelijk via het menu Apparaten > Snelheid 3 Profileren > tabblad CPU-profielen
- Gebruik Download Snapshot op het tabblad CPU-profilering om een snapshot te downloaden van de profielresultaten in CSV-indeling.

Tabblad CPU-profielen

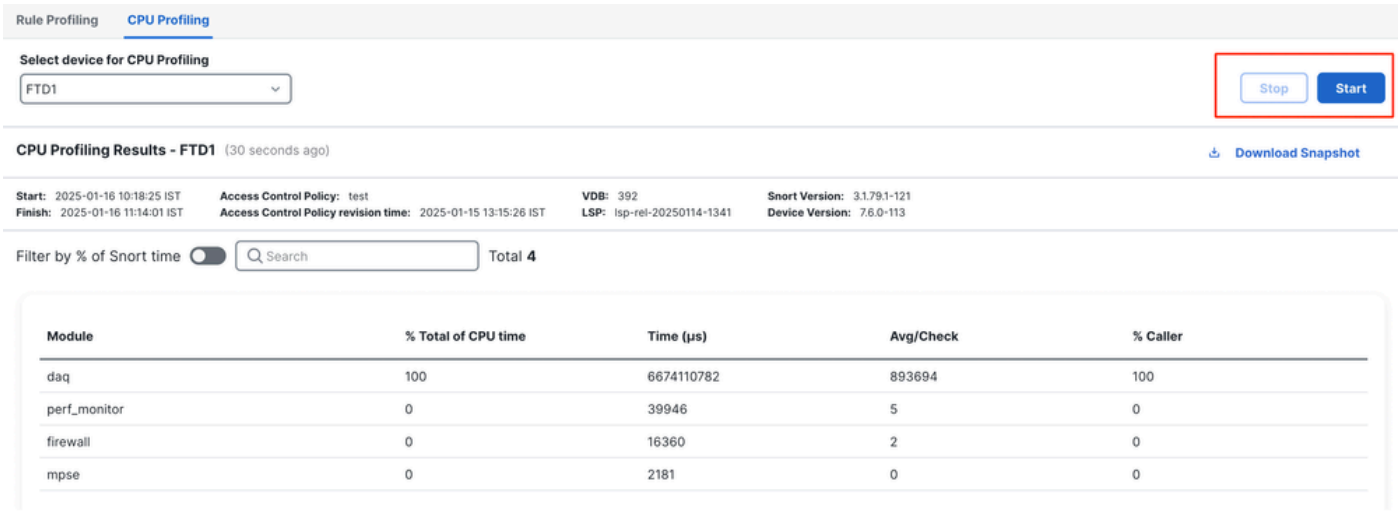
De pagina CPU-profilering is toegankelijk via het tabblad Apparaten > Snelheid 3 menu > CPU-profilering.

Het bevat een apparaat selector, Start/Stop knoppen, Download Snapshot knop, een profiling resultaten sectie, en een Profiling History sectie aan de linkerkant die wordt uitgebreid wanneer u erop klikt.

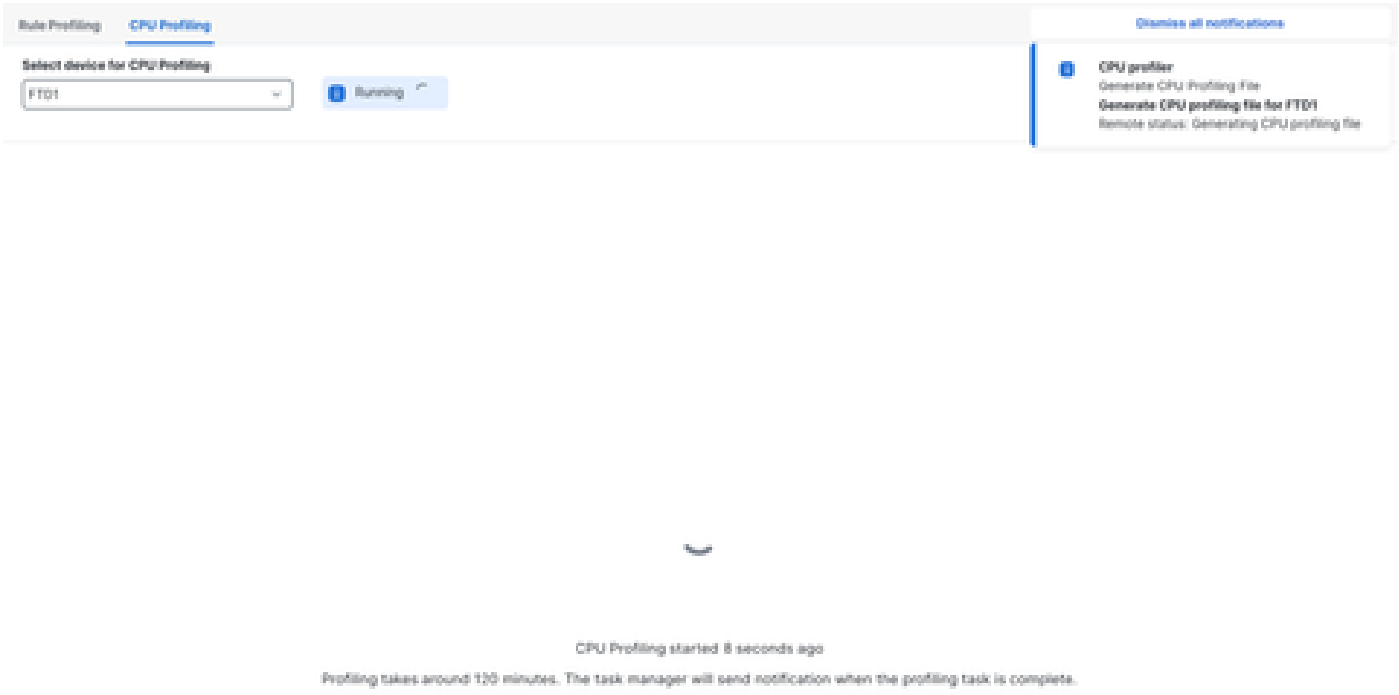


CPU-profilering

Klik op Start om een CPU-profielsessie te starten. Deze pagina wordt getoond wanneer de sessie is gestart.

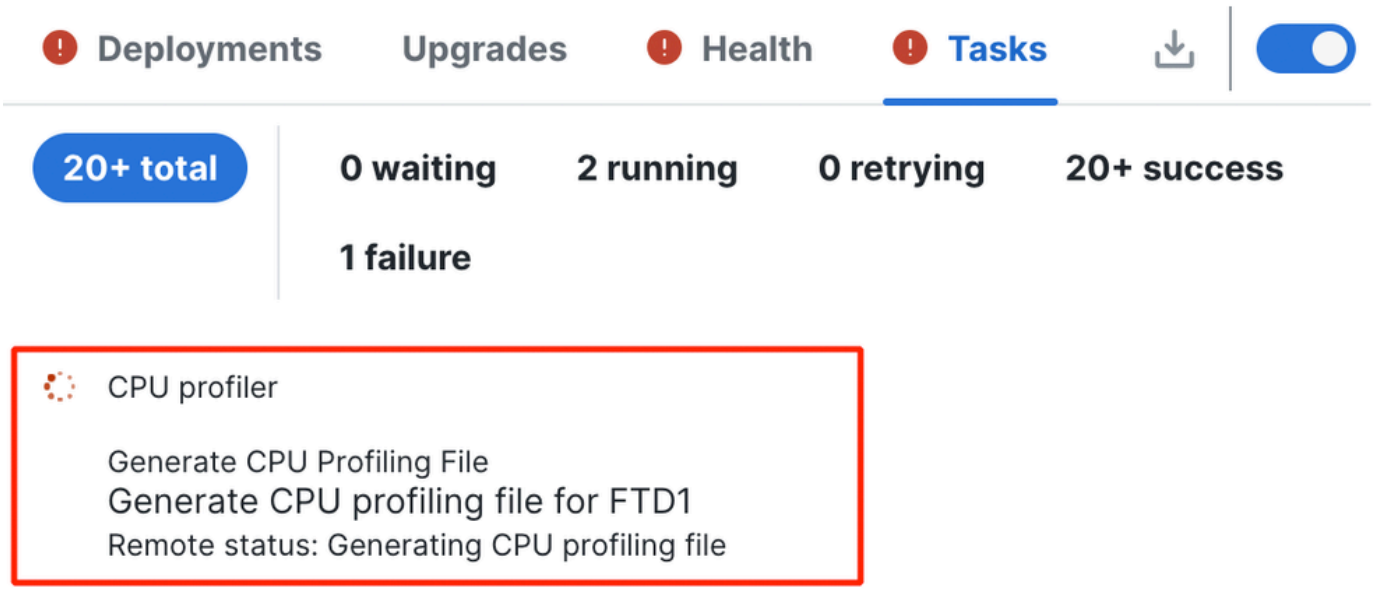


Starten



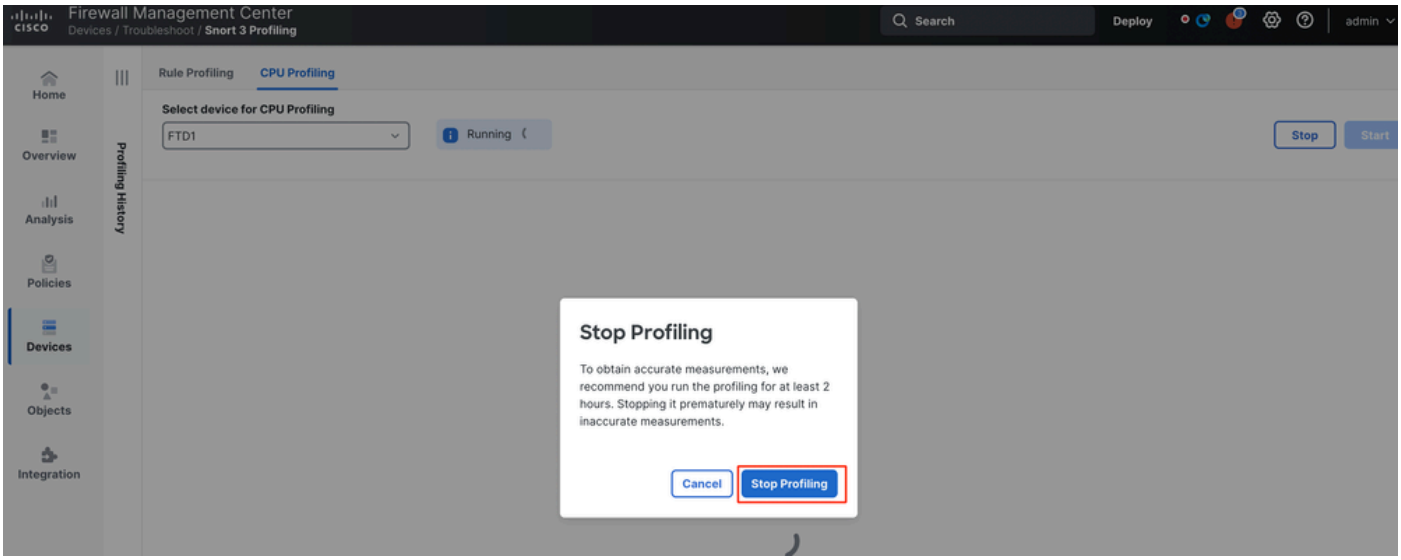
Lopen

Nadat de CPU-profileringssessie is gestart, wordt een taak gemaakt. Dit kan worden gecontroleerd in meldingen > taken.



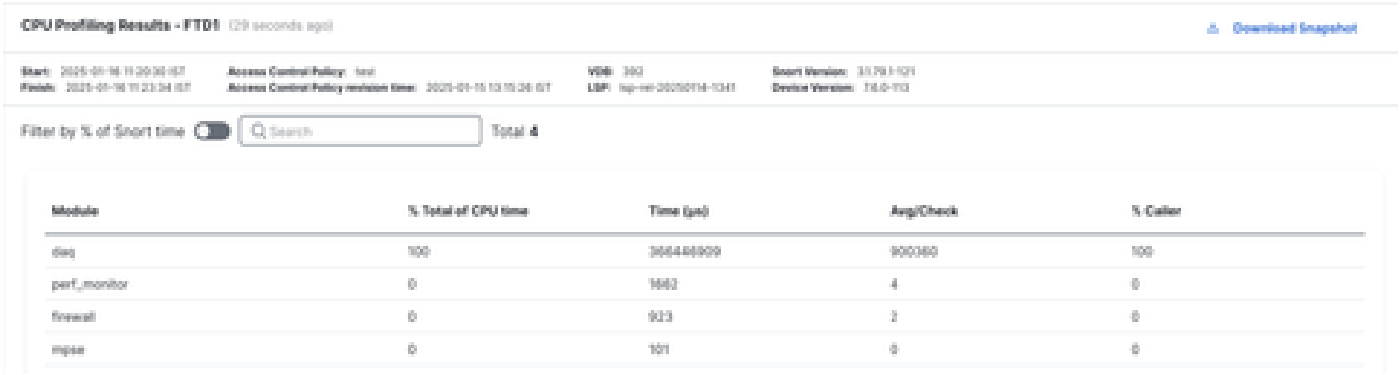
Taken

- Klik op Stoppen om een CPU-profileringssessie te stoppen die wordt uitgevoerd.
- Er verschijnt een bevestigingsvenster. klik op Profileren stoppen.



Stoppen met draaien

Het laatste profileringsresultaat wordt weergegeven in het gedeelte CPU-profielresultaten.



Resultaten

Uitleg van CPU-profielresultaten

- "Module" kolom geeft de naam van de module/inspecteur aan.
- "% totaal CPU tijd" kolom geeft het percentage aan van de tijd die een module nodig heeft ten opzichte van de totale tijd die Snort 3 nodig heeft in het verwerkingsverkeer. Als deze waarde aanzienlijk groter is dan die van andere modules, dan draagt module meer bij aan de onbevredigende prestaties van Snort 3.
- "Tijd (µ s)" staat voor de totale tijd in microseconden die door elke module wordt genomen.
- "Gem./controle" staat voor de gemiddelde tijd die de module neemt voor elke keer dat de module wordt opgeroepen.
- "% Caller" geeft de tijd aan die een submodule (indien geconfigureerd) nodig heeft voor de hoofdmodule. Het wordt voornamelijk gebruikt voor ontwikkelaar debugging doeleinden.

CPU profielresultaat - momentopname downloaden

- De gebruiker kan de momentopname van het profileringsresultaat downloaden door op Download Snapshot te klikken. Het gedownloade bestand heeft de indeling .csv en bevat alle velden van de pagina met profielresultaten zoals in dit voorbeeld.

- Uit het .csv-bestand snapshot halen:

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

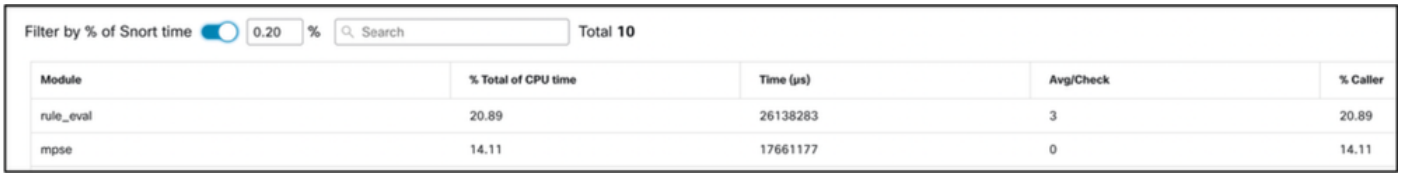
momentopname

Filtering van CPU-profielen

Profilatieresultaten kunnen worden gefilterd met:

- "Filter met % van de korte tijd" - kunt u modules uitfilteren waarvan de uitvoering meer dan n% van de profilingtijd heeft gekost.
- Zoeken - hiermee kunt u een tekstzoekopdracht uitvoeren door elk veld dat in de resultatentabel aanwezig is.

Elke kolom behalve "Module" kan gesorteerd worden door op de kop te klikken.



Resultaten

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.