Comprendre le profilage de règle et de CPU Snort 3 sur l'interface graphique FMC

Table des matières

Introduction

Ce document décrit la règle Snort 3 et la fonctionnalité de profilage de CPU ajoutée sur FMC 7.6.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

· Connaissance de Snort 3
· Secure Firepower Management Center (FMC)
· Défense contre les menaces Firepower (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Ce document s'applique à toutes les plates-formes Firepower
- Secure Firewall Threat Defense Virtual (FTD) exécutant la version 7.6.0 du logiciel
- Secure Firewall Management Center Virtual (FMC) exécutant la version 7.6.0 du logiciel

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation des fonctionnalités

- La règle et le profilage de CPU existaient déjà dans Snort, mais n'étaient accessibles que via l'interface de ligne de commande FTD. L'objectif de cette fonctionnalité est d'étendre les fonctionnalités de profilage et de simplifier les opérations.
- Activez les problèmes de performances des règles d'intrusion de débogage et modifiez les configurations des règles avant de contacter le TAC pour obtenir de l'aide au dépannage.
- Déterminez quels modules présentent des performances insatisfaisantes lorsque Snort 3 utilise un processeur à haute capacité.
- Créez un moyen convivial de déboguer et d'affiner les politiques d'analyse des intrusions et du réseau pour de meilleures performances.

Profilage

- Le profilage de règle et le profilage de CPU s'exécutent sur le FTD et leurs résultats sont stockés sur le périphérique et extraits par FMC.
- Vous pouvez exécuter plusieurs sessions de profilage simultanément sur différents périphériques.
- Vous pouvez exécuter simultanément le profilage des règles et le profilage de l'UC.
- En cas de haute disponibilité, le profilage ne peut être lancé que sur le périphérique actif au début de la session.
  Pour les configurations en cluster, le profilage peut être exécuté sur chaque noeud du cluster.
- Si un déploiement est déclenché alors qu'une session de profilage est en cours, un avertissement s'affiche pour l'utilisateur.

Si l'utilisateur choisit d'ignorer l'avertissement et le déploiement, cela annule la session de profilage en cours et le résultat du profileur affiche un message à ce sujet.

Une nouvelle session de profilage doit être démarrée sans être interrompue par un déploiement pour obtenir les résultats de profilage réels.

Profileur de règles

- Le profileur de règles Snort 3 collecte des données sur le temps passé à traiter un ensemble de règles d'intrusion Snort 3, ce qui permet de mettre en évidence les problèmes potentiels et d'afficher les règles dont les performances ne sont pas satisfaisantes.

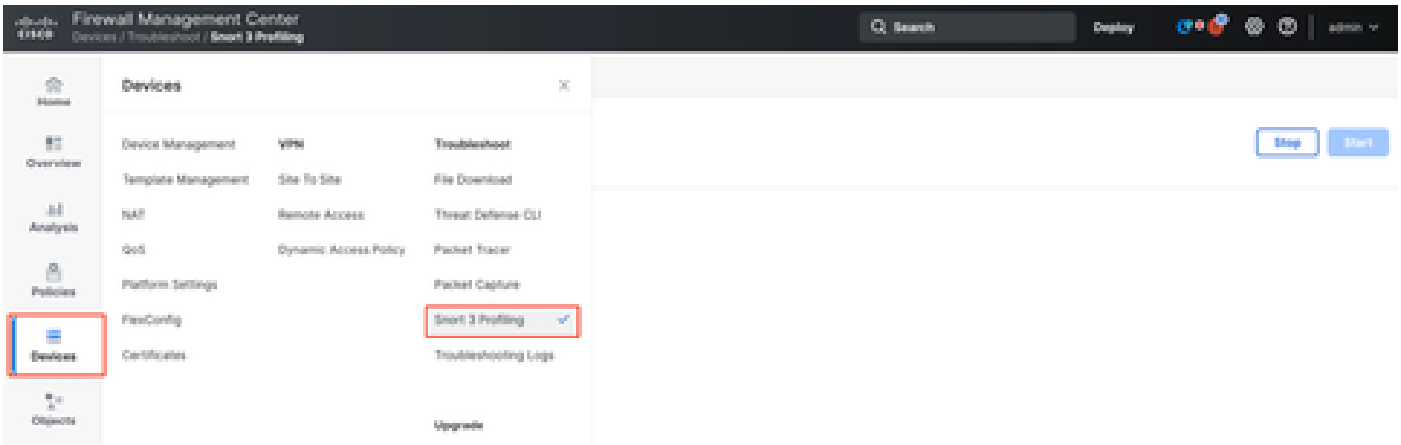
- Le profileur de règles affiche les 100 règles IPS dont la vérification a pris le plus de temps.
- Le déclenchement du profileur de règle ne nécessite ni rechargement ni redémarrage de Snort 3.
- Les résultats du profilage de règle sont enregistrés au format JSON dans le répertoire /ngfw/var/sf/sync/snort_profiling/ et synchronisés sur le FMC.
- Le profileur de règles se trouve dans le Snort 3 et inspecte le trafic avec le mécanisme de détection d'intrusion du Snort 3 ; l'activation du profilage des règles n'a aucun impact notable sur les performances.

Profilage des règles d'exploitation

- Le trafic doit traverser le périphérique
- Démarrez le profilage de règle en sélectionnant un périphérique, puis en cliquant sur le bouton Démarrer
  - Le démarrage d'une session de profilage crée une tâche qui peut être surveillée dans Notifications sous Tâches
- La durée par défaut d'une session de profilage des règles est de 120 minutes
  - La session de profilage des règles peut être arrêtée plus tôt, avant la fin, en appuyant sur le bouton Arrêter
- Les résultats peuvent être affichés dans l'interface utilisateur graphique et téléchargés
- L'historique de profilage affiche les résultats des sessions de profilage précédentes. L'utilisateur peut examiner un résultat de profilage spécifique en cliquant sur une carte dans le volet gauche de l'historique de profilage.

Menu Profilage Snort 3

La page Profilage est accessible à partir du menu Périphériques > Profilage Snort 3. La page contient à la fois la règle et le profilage de l'UC, divisés en deux onglets.



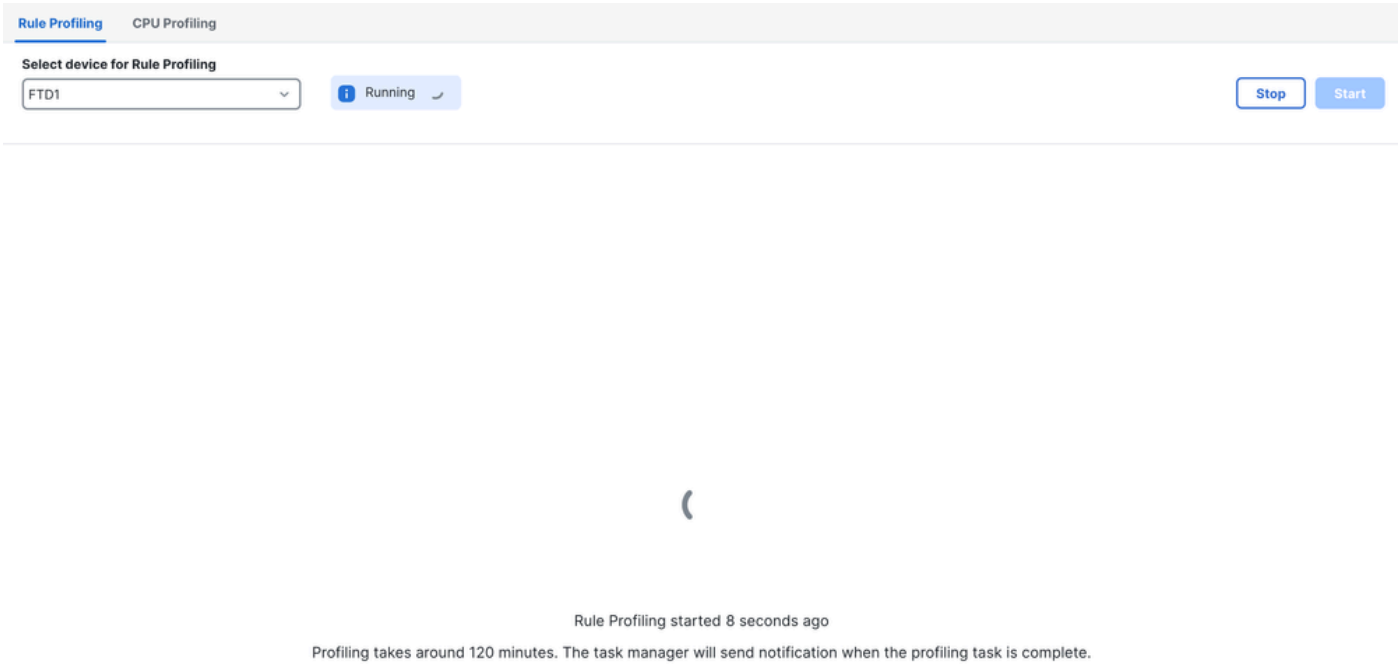
Périphériques

Démarrer le profilage des règles

Pour démarrer une session de profilage de règle, cliquez sur Démarrer. La session est automatiquement arrêtée après 120 minutes.

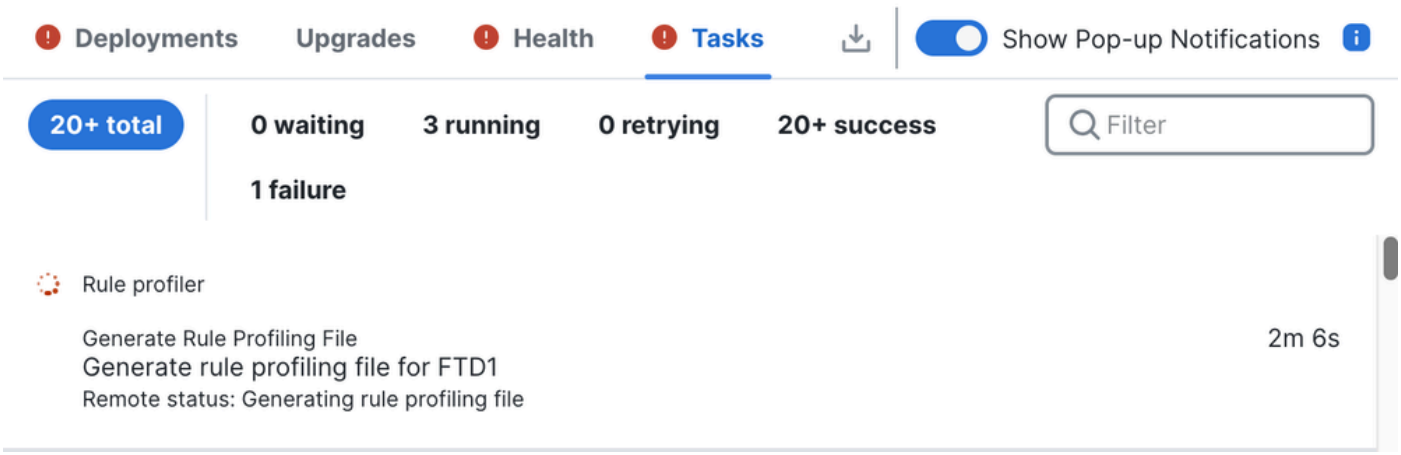
Un utilisateur ne peut pas configurer la durée de la session de profilage, mais il peut l'arrêter avant que les deux heures ne se soient écoulées.

Profilage des règles



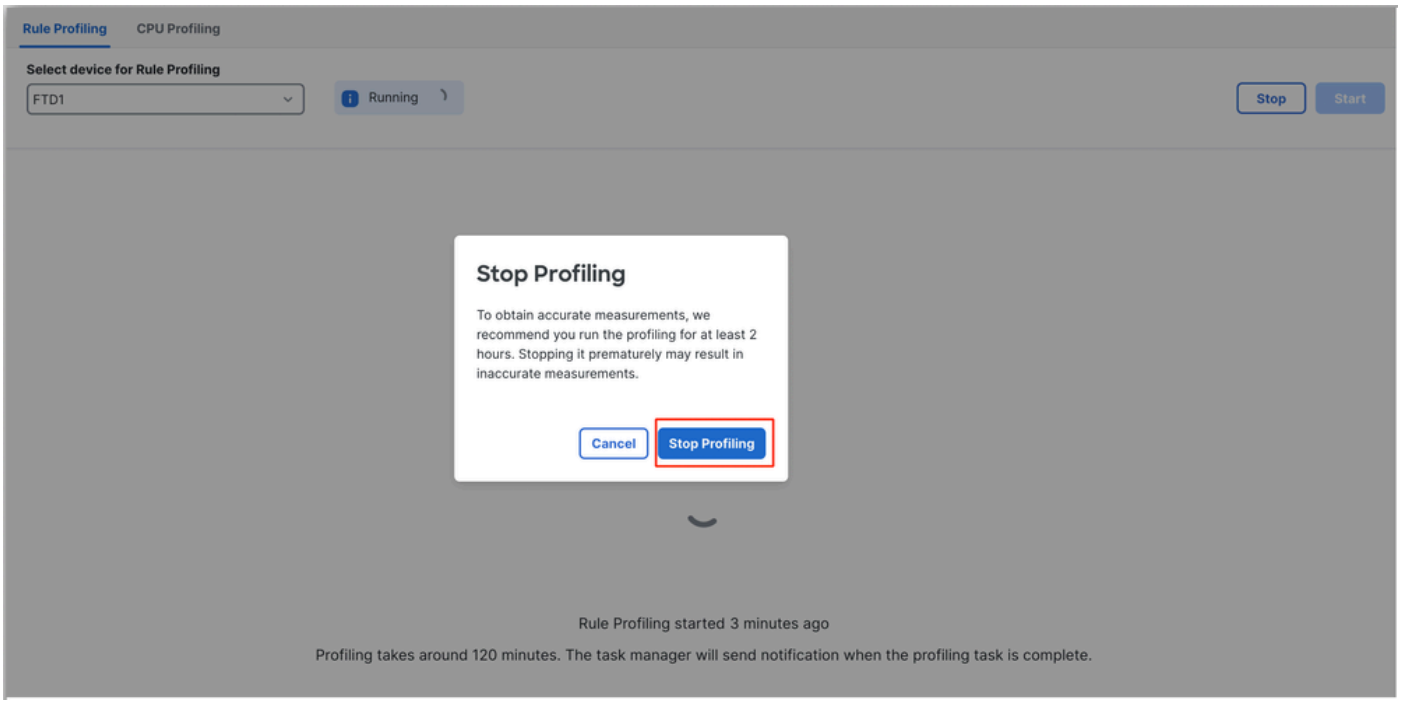
Marche

Une fois la session de profilage de règle démarrée, une tâche est créée. Vous pouvez l'intégrer dans Notifications > Tâches.



Tâche

Pour arrêter une session de profilage de règle en cours, au cas où vous auriez besoin de l'interrompre avant l'arrêt automatique, cliquez sur Stop et confirmez.



Arrêter le profilage

Une fois que vous avez sélectionné un périphérique, le dernier résultat de profilage s'affiche automatiquement dans la section Rule Profiling Results.

La table contient des statistiques sur les règles dont le traitement a pris le plus de temps, triées par ordre décroissant en fonction de la durée totale (en microsecondes (s)) qu'elles ont prise.consommée.

Résultats

Résultats du profileur de règles

Le résultat du profileur de règle pour une règle IPS comprend les champs suivants :

- % du temps de Snort - Temps passé à traiter la règle, par rapport à la durée de l'opération Snort 3
- Contrôles : nombre d'exécutions de la règle IPS
- Correspondances - Nombre de fois où la règle IPS correspond entièrement
- Alertes : nombre de fois où la règle IPS a déclenché une alerte IPS
- Durée (s) - Durée en microsecondes que Snort a passé à vérifier la règle IPS
- Moyenne/vérification - Temps moyen passé par Snort sur une vérification de la règle
- Moy./Correspondance - Temps moyen passé par Snort sur une vérification qui a abouti à

une correspondance
- Moy./Non concordance - Temps moyen passé par Snort sur une vérification qui n'a pas donné lieu à une correspondance
- Délais d'expiration - Nombre de fois où la règle a dépassé le seuil de gestion des règles configuré dans les paramètres de performance basés sur la latence de la stratégie AC
- Suspends : nombre de suspensions de la règle dues à des violations de seuil consécutives

Télécharger les résultats

- L'utilisateur peut télécharger le résultat du profilage (« cliché ») en cliquant sur le bouton « Télécharger le cliché ». Le fichier téléchargé est au format .csv et contient tous les champs de la page de résultats du profilage.
- Extrait du fichier .csv de l'instantané :

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

Vue du fichier .csv du snapshot :

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

Instantané

Profilage de la CPU

Présentation de Snort 3 CPU Profiler

- Le profileur de CPU établit le profil du temps CPU nécessaire aux modules/inspecteurs de Snort 3 pour traiter les paquets dans un intervalle de temps donné. Il donne un aperçu de la quantité de CPU consommée par chaque module, par rapport à la quantité totale de CPU consommée par le processus Snort 3.
- L'utilisation de CPU Profiler ne nécessite pas le rechargement de la configuration ou le redémarrage de Snort 3, évitant ainsi les temps d'arrêt.
- Le résultat de CPU Profiler affiche le temps de traitement pris par tous les modules lors de la dernière session de profilage.
- Les résultats du profilage du processeur sont enregistrés au format JSON dans le répertoire /ngfw/var/sf/sync/cpu_profiling/ et synchronisés dans le répertoire FMC /var/sf/peers/<device UID>/sync/cpu_profiling.

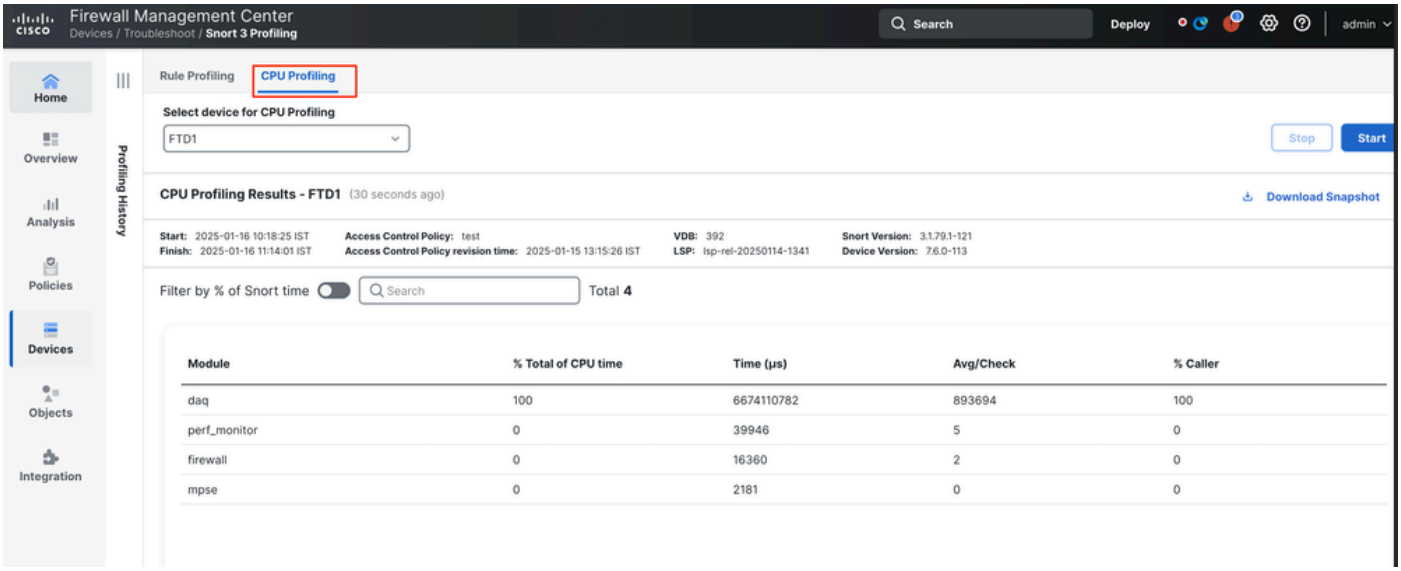
- Une nouvelle page de profilage Snort 3 a été ajoutée dans l'interface utilisateur FMC
- Cette page est accessible à partir du menu Devices > Snort 3 Profiling > onglet CPU Profiling

- Utilisez Download Snapshot sur l'onglet CPU profiling pour télécharger un instantané des résultats de profilage au format CSV.

Onglet Profil du processeur

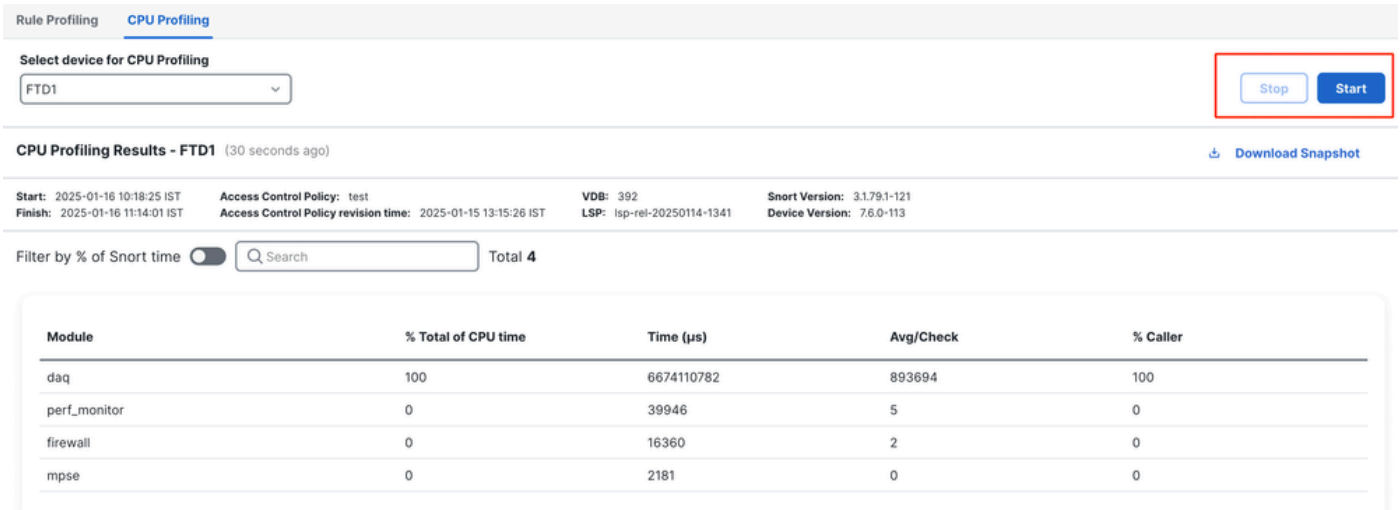
La page CPU Profiling est accessible à partir du menu Devices > Snort 3 Profiling > onglet CPU Profiling.

Il contient un sélecteur de périphérique, des boutons Start/Stop, le bouton Download Snapshot, une section de résultats de profilage et une section d'historique de profilage sur le côté gauche qui est développé en cliquant dessus.

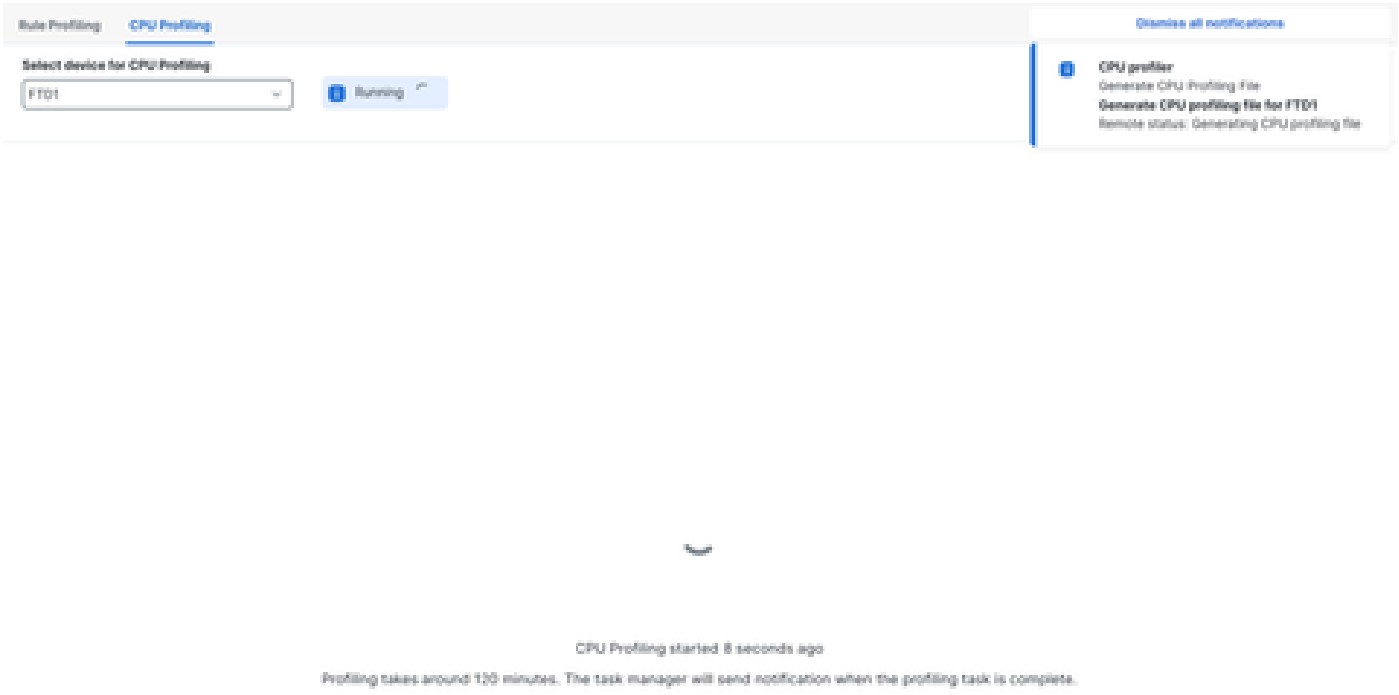


Profilage de la CPU

Pour démarrer une session de profilage du processeur, cliquez sur Démarrer. Cette page s'affiche au démarrage de la session.

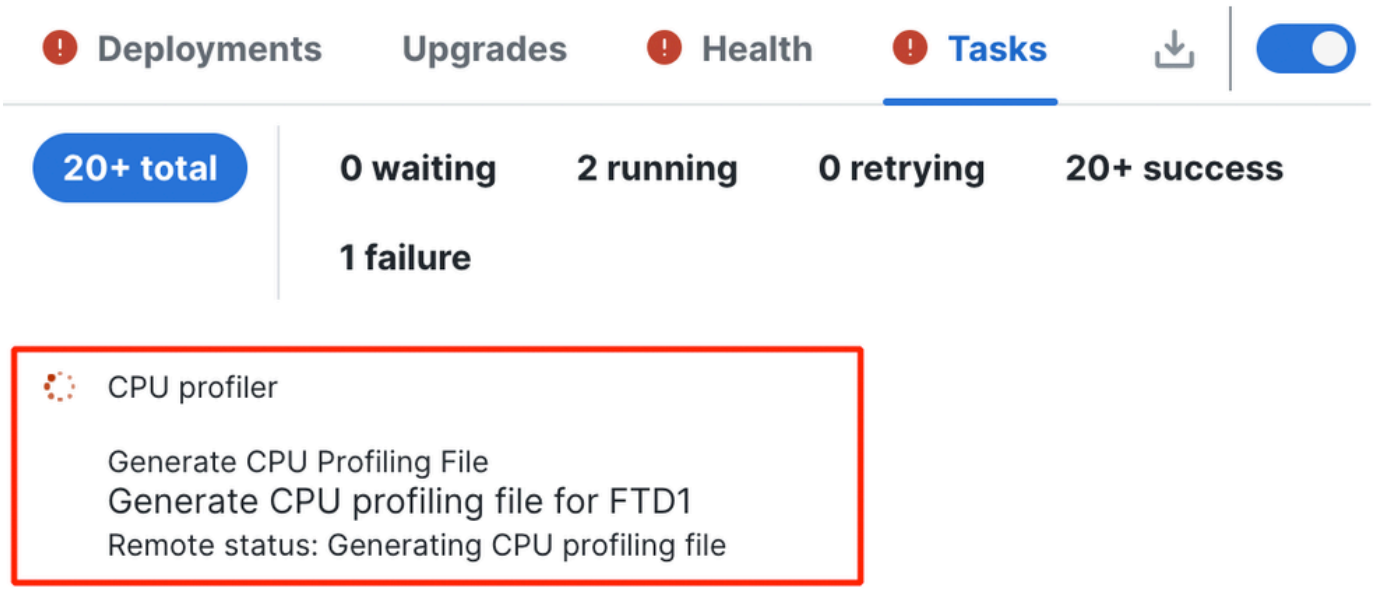


Début



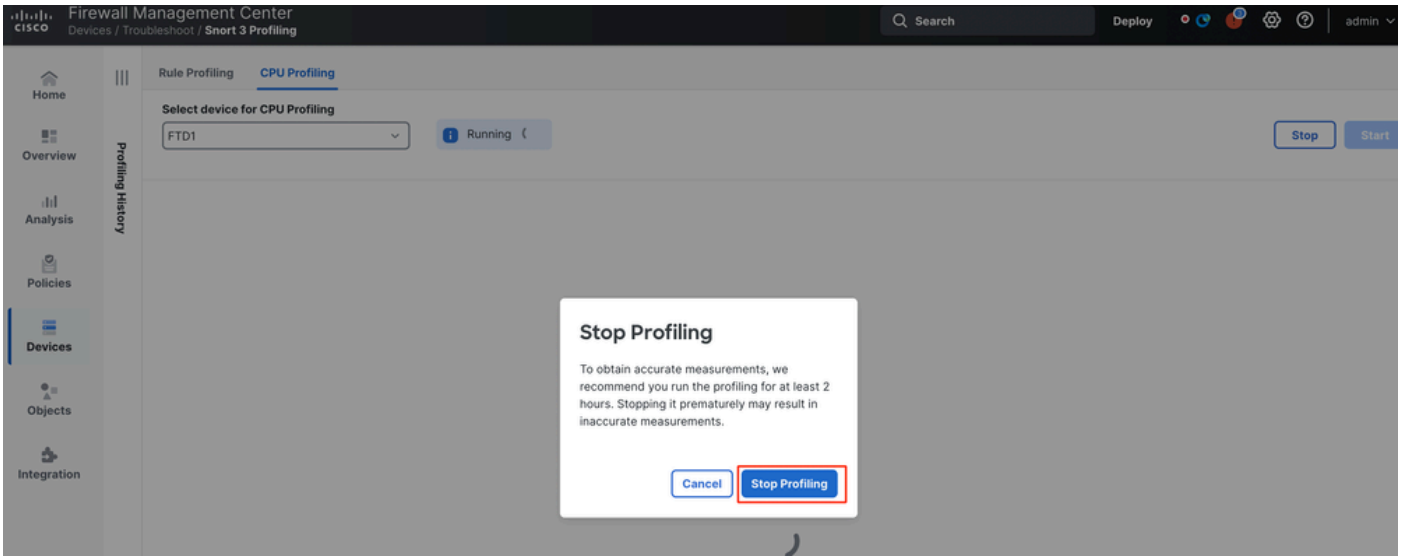
Marche

Une fois la session de profilage du processeur démarrée, une tâche est créée. Vous pouvez l'intégrer dans Notifications > Tâches.



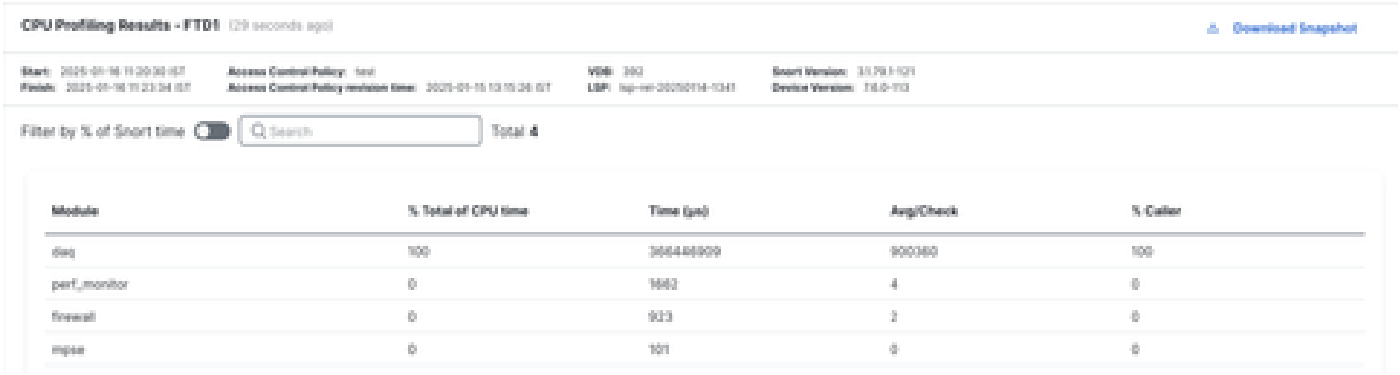
Tâche

- Pour arrêter une session de profilage du processeur en cours, cliquez sur Arrêter.
- Une boîte de dialogue de confirmation apparaît. cliquez sur Arrêter le profilage.



Arrêter l'exécution

Le dernier résultat du profilage est affiché dans la section Résultats du profilage du processeur.



Résultats

Résultats du profileur de CPU expliqués

- La colonne "Module" indique le nom du module/inspecteur.
- La colonne « % du temps total de l'UC » indique le pourcentage de temps pris par le module par rapport au temps total pris par Snort 3 dans le traitement du trafic. Si cette valeur est considérablement plus grande que celle des autres modules, alors le module contribue davantage aux performances insatisfaisantes de Snort 3.
- "Temps (s)" représente le temps total en microsecondes pris par chaque module.
- "Avg/Check" représente le temps moyen pris par le module pour chaque appel du module.
- "% Caller" indique le temps pris par le sous-module (s'il est configuré) par rapport au module principal. Il est principalement utilisé à des fins de débogage par les développeurs.

Résultat de CPU Profiler - Télécharger le snapshot

- L'utilisateur peut télécharger le cliché du résultat du profilage en cliquant sur Télécharger le cliché. Le fichier téléchargé est au format .csv et contient tous les champs de la page de résultats du profilage, comme illustré dans cet exemple.
- Extrait du fichier .csv de l'instantané :

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

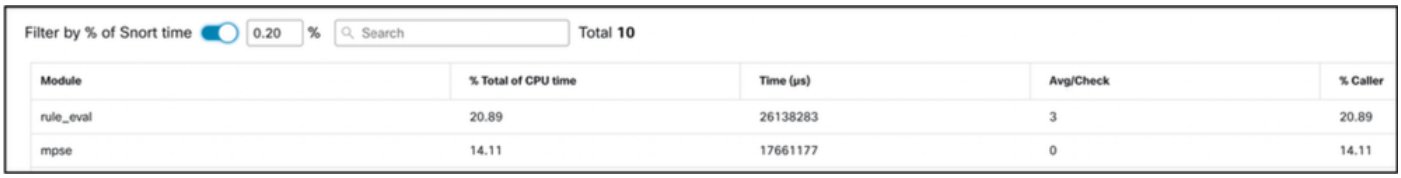
Instantané

Filtrage des résultats de profilage CPU

Les résultats de profilage peuvent être filtrés à l'aide de :

- « Filtrer par % du temps d'analyse » - vous permet de filtrer les modules dont l'exécution a pris plus de n % du temps de profilage.
- Rechercher : vous permet d'effectuer une recherche textuelle dans n'importe quel champ présent dans la table de résultats.

Toute colonne, à l'exception de « Module », peut être triée en cliquant sur son en-tête.



Résultats

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.