FMC GUIでのSnort 3ルールプロファイリングとCPUプロファイリングについて

内容

はじめに

このドキュメントでは、FMC 7.6に追加されたSnort 3ルールおよびCPUプロファイリング機能について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Snort 3の知識
- セキュアなFirepower Management Center(FMC)
- セキュアなFirepower Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- このドキュメントは、すべてのFirepowerプラットフォームに適用されます
- ソフトウェアバージョン7.6.0を実行するセキュアファイアウォール脅威対策(FTD)仮想(FTD)
- ソフトウェアバージョン7.6.0を実行するSecure Firewall Management Center Virtual(FMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能の概要

- ルールおよびCPUプロファイリングはSnortにすでに存在していますが、アクセスはFTD CLIからのみでした。この機能の目的は、プロファイリング機能を拡張して、より分かりやすくすることです。
- デバッグ侵入ルールのパフォーマンスの問題を有効にし、独自にルール設定を調整してから、トラブルシューティングのヘルプを求めてTACに連絡してください。
- Snort 3のCPU使用率が高い場合に、どのモジュールのパフォーマンスが低下するかを把握します。
- 侵入ポリシーとネットワーク分析ポリシーをデバッグおよび微調整してパフォーマンスを向上させる使いやすい方法を作成します。

プロファイリング

- ルールプロファイリングとCPUプロファイリングはどちらもFTDで実行され、その結果はデバイスに保存され、FMCによって取得されます。
- 異なるデバイスで複数のプロファイルセッションを同時に実行できます。
- ルールプロファイリングとCPUプロファイリングは同時に実行できます。
- ハイアベイラビリティの場合、プロファイリングは、セッションの開始時にアクティブなデバイスでのみ起動できます。
  クラスタ化されたセットアップでは、クラスタ内の各ノードでプロファイリングを実行できます。
- プロファイルセッションの実行中に展開がトリガーされると、ユーザーに警告が表示されます。

ユーザーが警告を無視して配備を選択した場合、現在のプロファイルセッションが取り消され、プロファイラの結果に関連するメッセージが表示されます。

新しいプロファイルセッションは、実際のプロファイル結果を取得するために、展開によって中断されることなく開始する必要があります。

規則プロファイラ

- Snort 3ルールプロファイラは、Snort 3侵入ルールのセットの処理に費やされた時間に関するデータを収集し、潜在的な問題を強調表示して、パフォーマンスが不十分なルールを示し

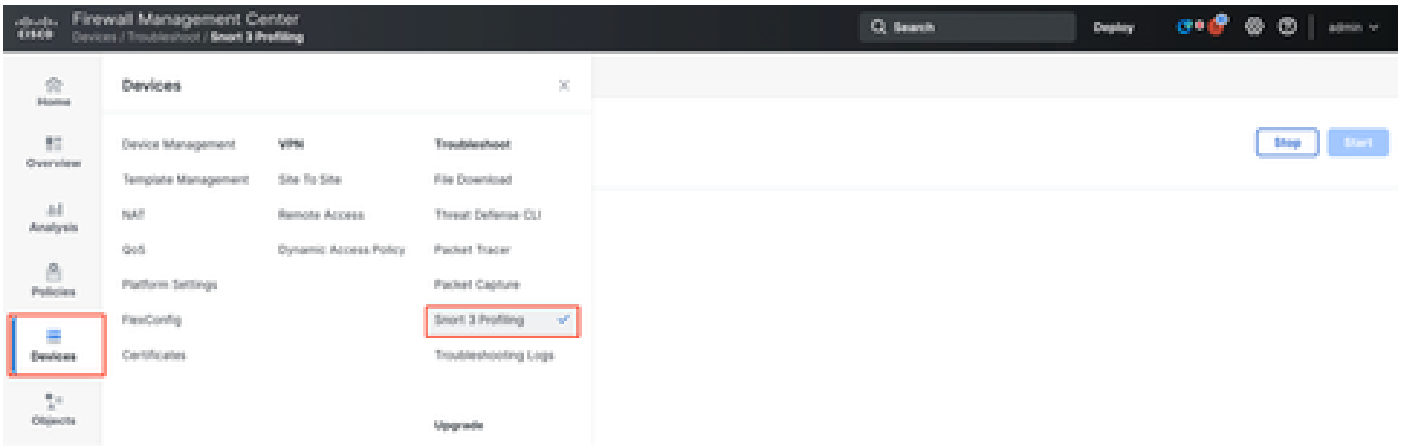
ます。
- ルールプロファイラは、確認に最も時間がかかった100個のIPSルールを表示します。
- Rule Profilerのトリガーには、Snort 3のリロードや再起動は必要ありません。
- ルールプロファイリングの結果はJSON形式で/ngfw/var/sf/sync/snort_profiling/ディレクトリに保存され、FMCで同期されます。
- ルールプロファイラはSnort 3内に配置され、Snort 3侵入検知メカニズムを使用してトラフィックを検査します。ルールプロファイリングを有効にしても、パフォーマンスに目立った影響はありません。

Operate Ruleのプロファイリング

- トラフィックはデバイスを通過する必要がある
- デバイスを選択し、[開始]ボタンをクリックして、ルールのプロファイリングを開始します
  - プロファイルセッションを開始すると、「タスク」の「通知」で監視できるタスクが作成されます
- ルールプロファイルセッションのデフォルトの時間は120分です
  - ルールプロファイルセッションは、[停止]ボタンを押すことで、完了前に停止できます
- 結果はGUIで表示してダウンロードできます
- 「プロファイル履歴」には、以前のプロファイルセッションの結果が表示されます。ユーザーは、プロファイル履歴の左側のパネルからカードをクリックして、特定のプロファイル結果を検査できます。

Snort 3のプロファイルメニュー

プロファイルページには、Devices > Snort 3 Profilingメニューからアクセスできます。このページには、ルールプロファイリングとCPUプロファイリングの両方が2つのタブに分かれて表示されます。



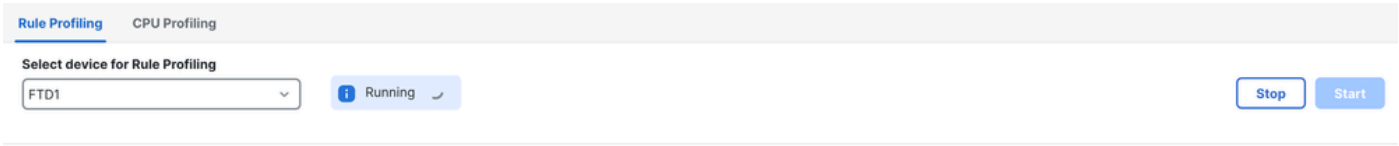
デバイス

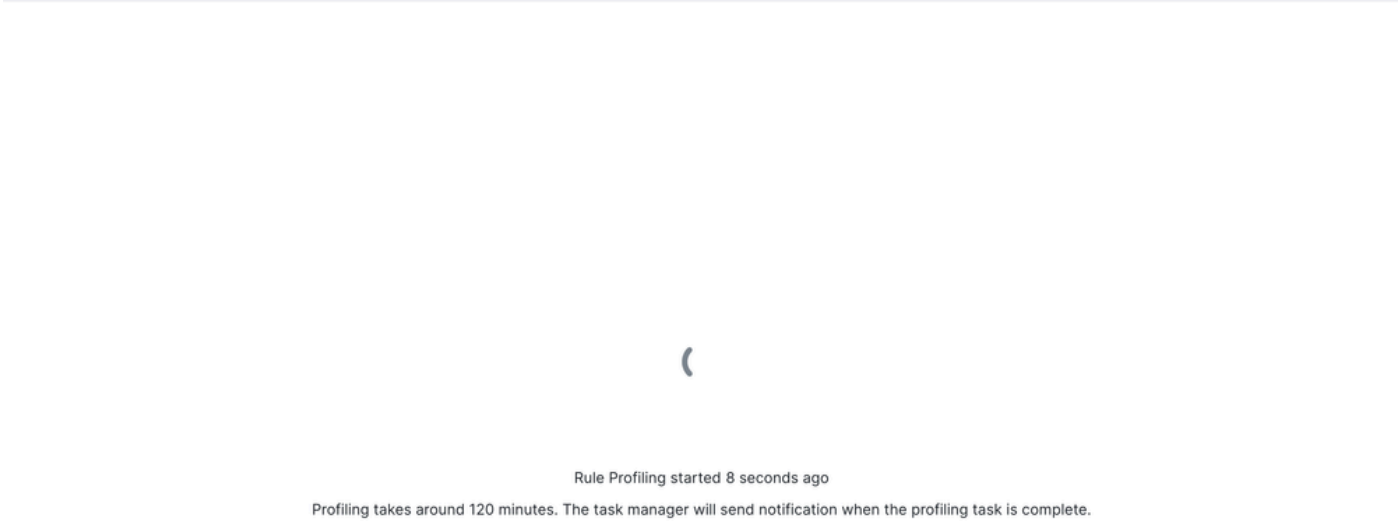
ルールのプロファイルの開始

ルールプロファイルセッションを開始するには、Startをクリックします。セッションは120分後に自動的に停止します。

ユーザーはプロファイリング・セッションの長さを構成できませんが、2時間が経過する前に終了できます。

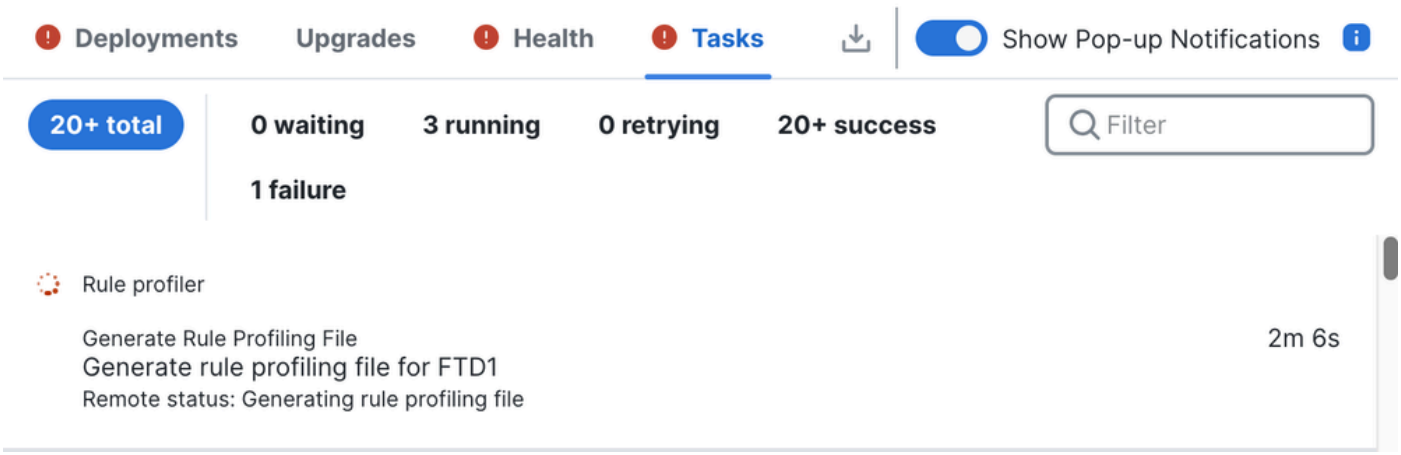
ルールのプロファイリング





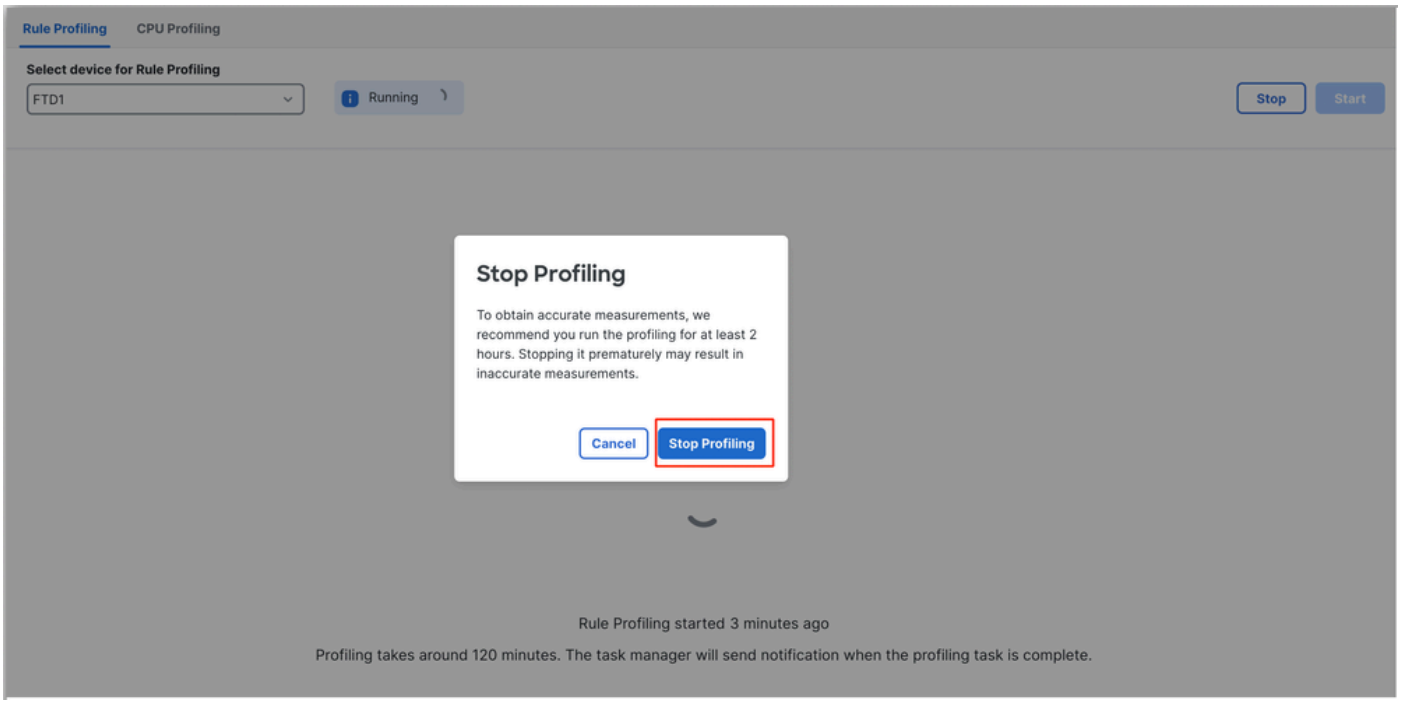
実行中

ルール・プロファイリング・セッションが開始されると、タスクが作成されます。これは、Notifications > Tasksで確認できます。



タスク

進行中のルールプロファイルセッションを停止するには、自動停止の前に中断する必要がある場合は、Stopをクリックして確認します。



プロファイルの停止

デバイスを選択すると、最新のプロファイリング結果が「Rule Profiling Results」セクションに自動的に表示されます。

このテーブルには、処理時間が最も長かったルールの統計が、合計時間(マイクロ秒(µs)単位で降順にソートされて格納されます。

成果

規則プロファイラの結果

IPSルールのルールプロファイラの出力には、次のフィールドが含まれます。

- % of Snort time:Snort 3の動作時間に対する、ルールの処理に要した時間
- Checks:IPSルールの実行回数
- Matches:IPSルールが完全に一致した回数
- Alerts:IPSルールによってIPSアラートがトリガーされた回数
- 時間(µs):SnortがIPSルールのチェックに費やした時間（マイクロ秒）
- Avg/Check:Snortがルールの1つのチェックに費やした平均時間
- Avg/Match：一致が発生した1回のチェックにSnortが費やした平均時間
- Avg/Non-Match：一致が得られなかった1回のチェックにSnortが費やした平均時間
- Timeouts：ルールがルール処理を超えた回数 – ACポリシーの遅延ベースパフォーマンス設

定でしきい値が設定されています。
- Suspends：連続したしきい値違反のためにルールが中断された回数

結果のダウンロード

- 「Download Snapshot（スナップショットのダウンロード）」ボタンをクリックすると、プロファイリング結果（「スナップショット」）をダウンロードできます。ダウンロードされたファイルは.csv形式で、プロファイル結果ページのすべてのフィールドが含まれています。
- スナップショットの.csvファイルから抽出します。

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

スナップショット.csvファイルビュー：

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

スナップショット

CPU プロファイリング

Snort 3 CPUプロファイラの概要

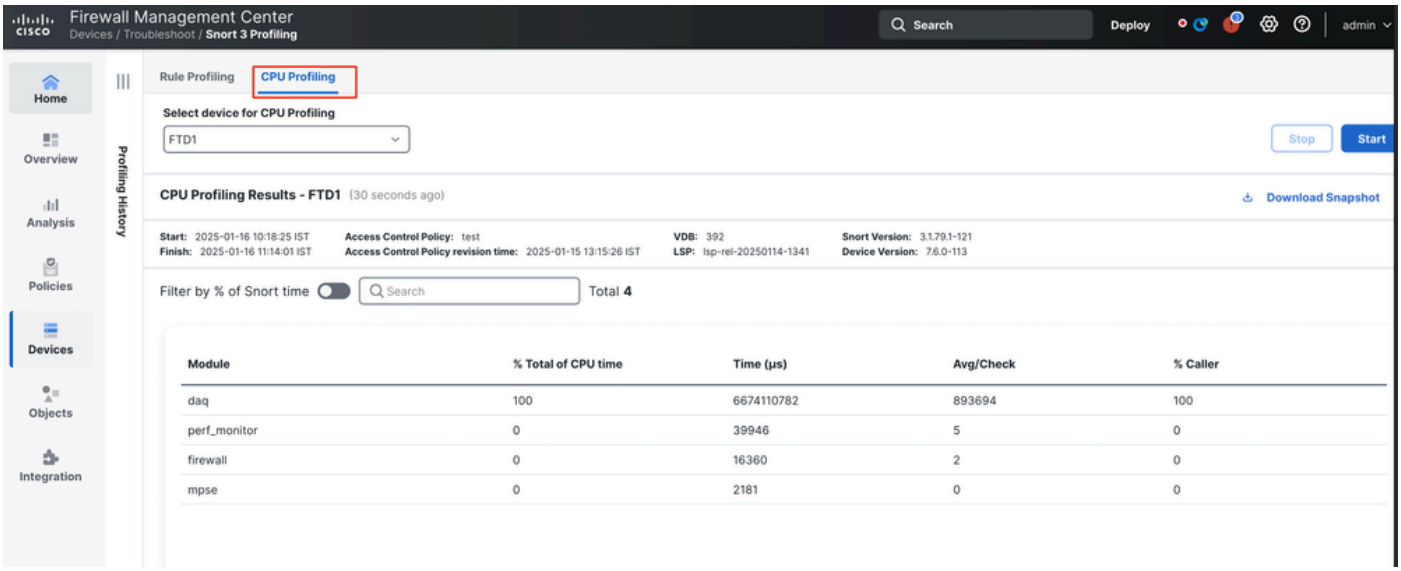
- CPUプロファイラは、特定の時間間隔でパケットを処理するためにSnort 3のモジュール/インスペクタにかかるCPU時間をプロファイリングします。Snort 3プロセスによって消費される合計CPU量に関する観点から、各モジュールが消費しているCPUの量に関する洞察が得られます。
- CPU Profilerを使用すると、設定をリロードしたりSnort 3を再起動したりする必要がないため、ダウンタイムを回避できます。
- CPUプロファイラの結果には、最後のプロファイリングセッション中にすべてのモジュールによって実行された処理時間が表示されます。
- CPUプロファイリングの結果は、/ngfw/var/sf/sync/cpu_profiling/ディレクトリにJSON形式で保存され、FMC /var/sf/peers/<device UUID>/sync/cpu_profilingディレクトリで同期されます。

- 新しいSnort 3プロファイリングページがFMC UIに追加されました
- このページには、Devices > Snort 3 Profilingメニュー> CPU Profilingタブからアクセスできます
- CPUプロファイルタブのDownload Snapshotを使用して、プロファイル結果のスナップショットをCSV形式でダウンロードします。

CPU Profilingタブ

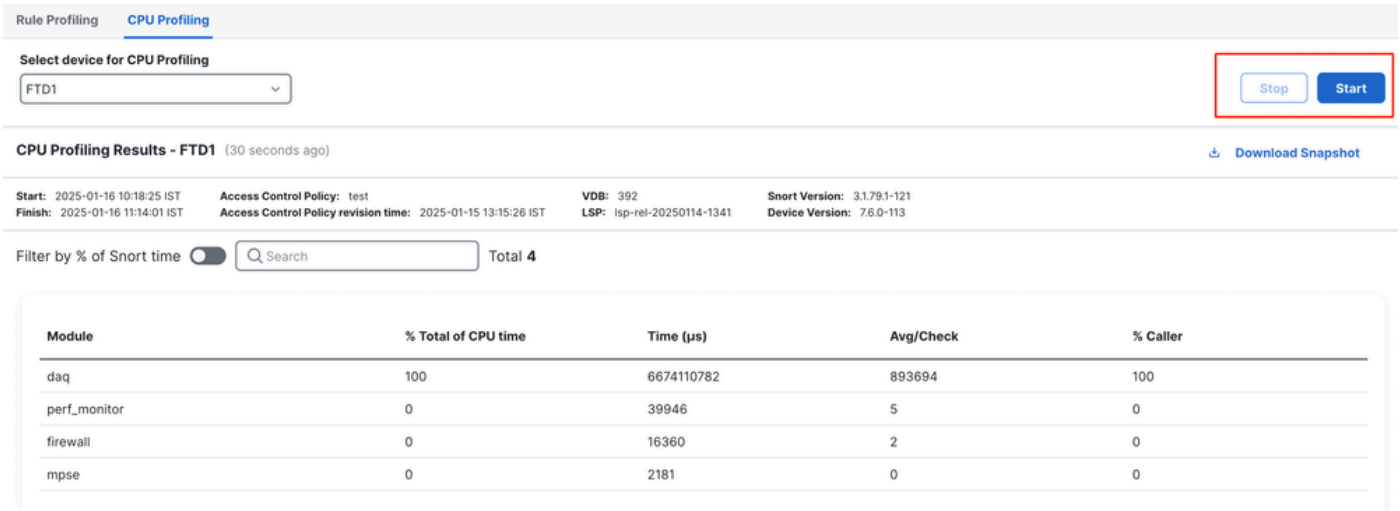
CPU Profilingページには、Devices > Snort 3 Profiling メニュー> CPU Profilingタブからアクセスできます。

デバイスセレクタ、「Start/Stop」ボタン、「Download Snapshot」ボタン、プロファイリング結果セクション、およびクリックすると展開される「Profiling History」セクションが左側に表示されます。

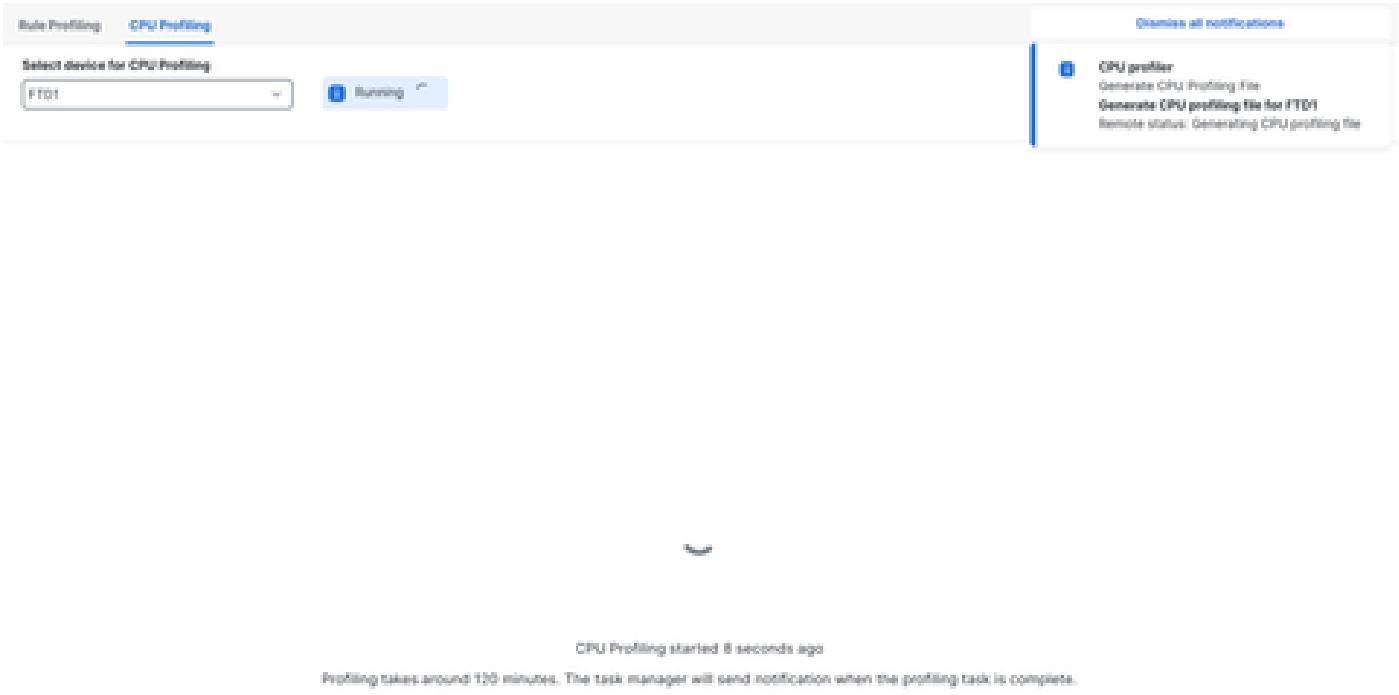


CPU プロファイリング

CPUプロファイルセッションを開始するには、Startをクリックします。このページは、セッションの開始時に表示されます。

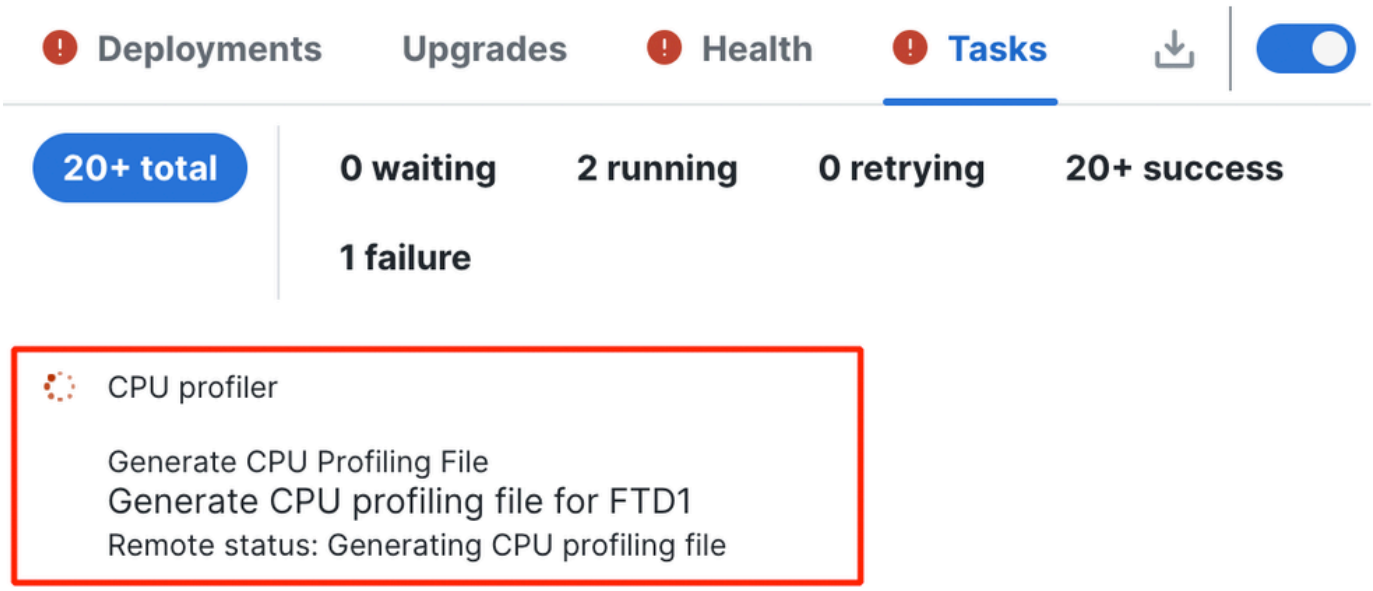


開始



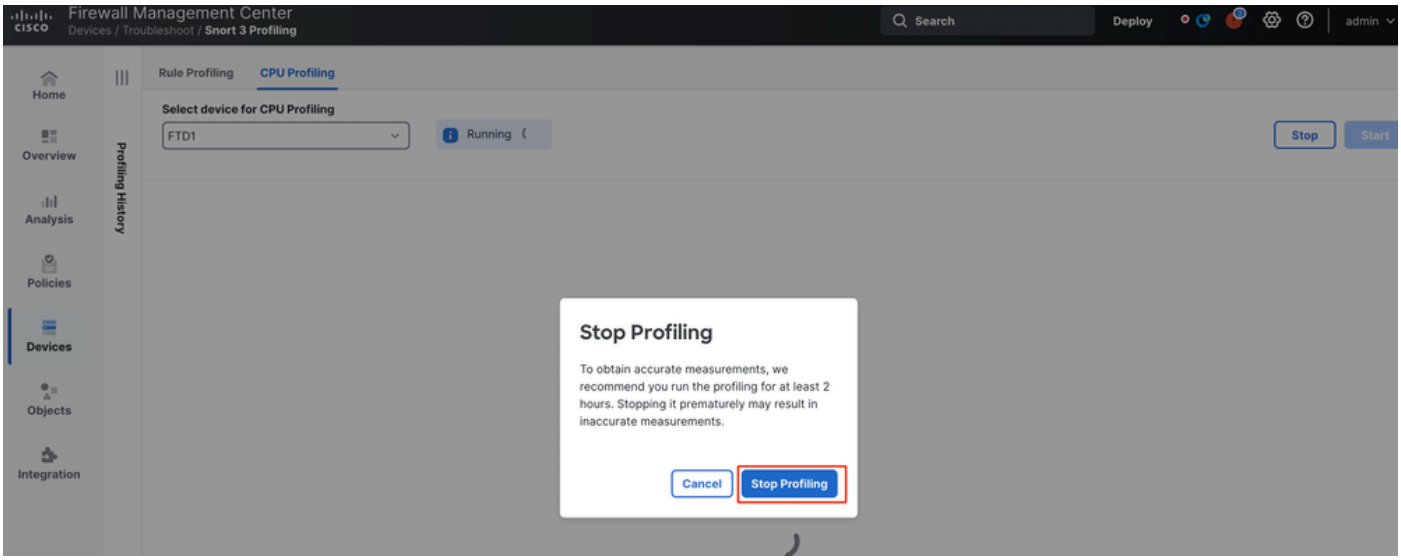
実行中

CPUプロファイルセッションが開始されると、タスクが作成されます。これは、Notifications > Tasksの順に選択して確認できます。



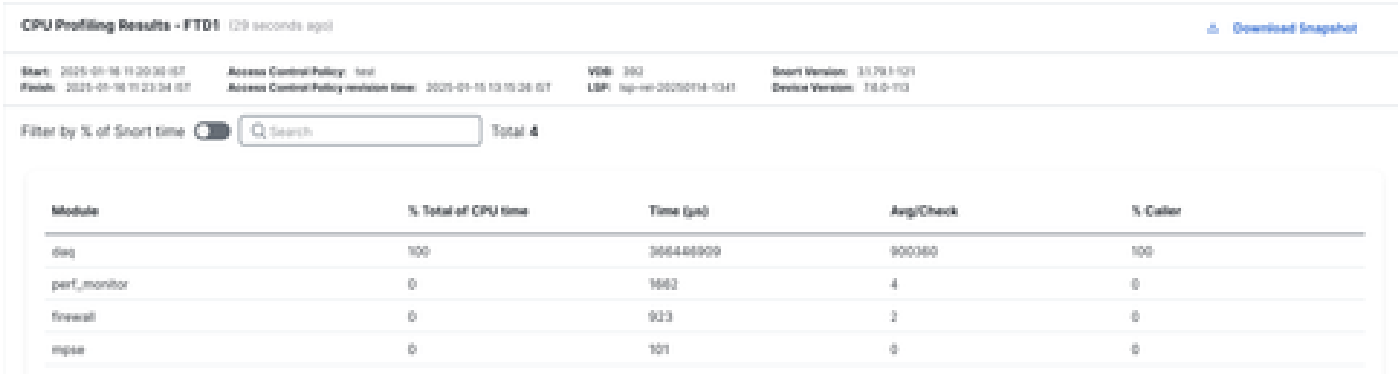
タスク

- 進行中のCPUプロファイルセッションを停止するには、Stopをクリックします。
- 確認のダイアログが表示されます。Stop Profilingをクリックします。



実行の停止

最新のプロファイリング結果が「CPU Profiling Results」セクションに表示されます。



成果

CPUプロファイラの結果の説明

- 「Module」列は、モジュール/インスペクタの名前を示します。
- 「% Total of CPU Time」列は、トラフィックの処理でSnort 3にかかった全体時間に対する、モジュールにかかった時間の割合を示します。この値が他のモジュールよりも大幅に大きい場合、そのモジュールはSnort 3のパフォーマンスの低下の一因となります。
- 「Time (µs)」は、各モジュールにかかった合計時間をマイクロ秒単位で表します。
- 「Avg/Check」は、モジュールが呼び出されるたびにモジュールにかかる平均時間を表します。
- 「% Caller」は、メインモジュールに対してサブモジュールが要した時間（設定されている場合）を示します。主に開発者のデバッグ目的で使用されます。

CPUプロファイラの結果 – スナップショットのダウンロード

- プロファイリング結果のスナップショットをダウンロードするには、Download Snapshotをクリックします。ダウンロードされたファイルは.csv形式で、この例に示すように、プロファイル結果ページのすべてのフィールドが含まれています。
- スナップショットの.csvファイルから抽出します。

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

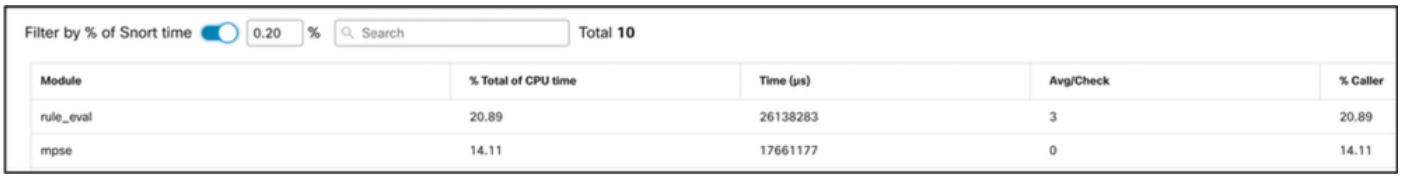
スナップショット

CPUプロファイリング結果のフィルタリング

プロファイル結果は、次の方法でフィルタ処理できます。

- 「Snort時間の%」によるフィルタリング：実行にプロファイリング時間のn %を超えたモジュールをフィルタリングして除外できます。
- 検索：結果テーブルに存在する任意のフィールドでテキスト検索を実行できます。

「モジュール」以外の列は、そのヘッダーをクリックして並べ替えることができます。



成果

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。