فهم ميزة تحديد سمات قواعد الشبكة 3 (SNORT) وتنميط وحدة المعالجة المركزية (CPU) على واجهة المستخدم الرسومية (GUI) التابعة لوحدة التحكم الموحدة (FMC)

المحتويات

المقدمة

يصف هذا المستند ميزة إنشاء ملف تعريف وحدة المعالجة المركزية (CPU) وقاعدة snort 3 التي تمت إضافتها على FMC 7.6.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشورت 3
- مركز إدارة FirePOWER الآمن (FMC)

· الدفاع الآمن ضد تهديد الطاقة النارية (FTD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ينطبق هذا المستند على جميع منصات Firepower
- برنامج الدفاع الظاهري ضد تهديد جدار الحماية الآمن (FTD) الذي يعمل بنظام التشغيل، الإصدار 7.6.0
- Secure Firewall Management Center Virtual (FMC) الذي يشغل الإصدار 7.6.0 من البرنامج

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة على الميزة

- كانت القاعدة وتنميط وحدة المعالجة المركزية موجودين بالفعل في Snort ولكن كان يمكن الوصول إليه فقط من خلال واجهة سطر الأوامر (CLI) الخاصة ب FTD. تتمثل الهدف من هذه الميزة في توسيع إمكانات تحديد السمات وجعلها أكثر مباشرة.
- قم بتمكين مشاكل أداء قاعدة التطفل الخاصة بتصحيح الأخطاء وتعديل تكوينات القاعدة بشكل مستقل قبل الوصول إلى TAC للحصول على تعليمات حول استكشاف الأخطاء وإصلاحها.
- تعرف على الوحدات التي يكون أداؤها غير مرض عندما يستهلك الطراز Snort 3 وحدة معالجة مركزية (CPU) عالية.
- إنشاء طريقة سهلة الاستخدام لتصحيح أخطاء سياسات منع الاختراق وتحليل الشبكة وضبطها من أجل تحسين الأداء.

تنميط

- يتم تشغيل كل من ميزة تحديد سمات القواعد وتنميط وحدة المعالجة المركزية (CPU) على FTD ويتم تخزين نتائجهما على الجهاز ويتم سحبها بواسطة FMC.
- يمكنك تشغيل جلسات عمل ملفات تعريف متعددة في وقت واحد على أجهزة مختلفة.
- يمكنك تشغيل القواعد الخاصة بملفات تعريف البيانات وتنميط وحدة المعالجة المركزية (CPU) في نفس الوقت.
- في حالة التوفر العالي، يمكن بدء تشغيل التنميط فقط على الجهاز النشط في بداية الجلسة.
  بالنسبة للمقاطع المجمعة، يمكن تشغيل التحليل على كل عقدة في نظام المجموعة.
- إذا تم تشغيل النشر أثناء وجود جلسة عمل ملف التعريف قيد التقدم، يتم عرض تحذير للمستخدم.

إذا اختار المستخدم تجاهل التحذير والنشر، يؤدي هذا إلى إلغاء جلسة عمل إنشاء ملف التعريف الحالية ويعرض نتيجة منشئ ملفات التعريف رسالة تتعلق بهذا الأمر.

يجب بدء جلسة عمل جديدة لإنشاء ملف التعريف دون مقاطعة عملية نشر للحصول على نتائج ملف التعريف الفعلية.

منشئ ملفات تعريف القاعدة

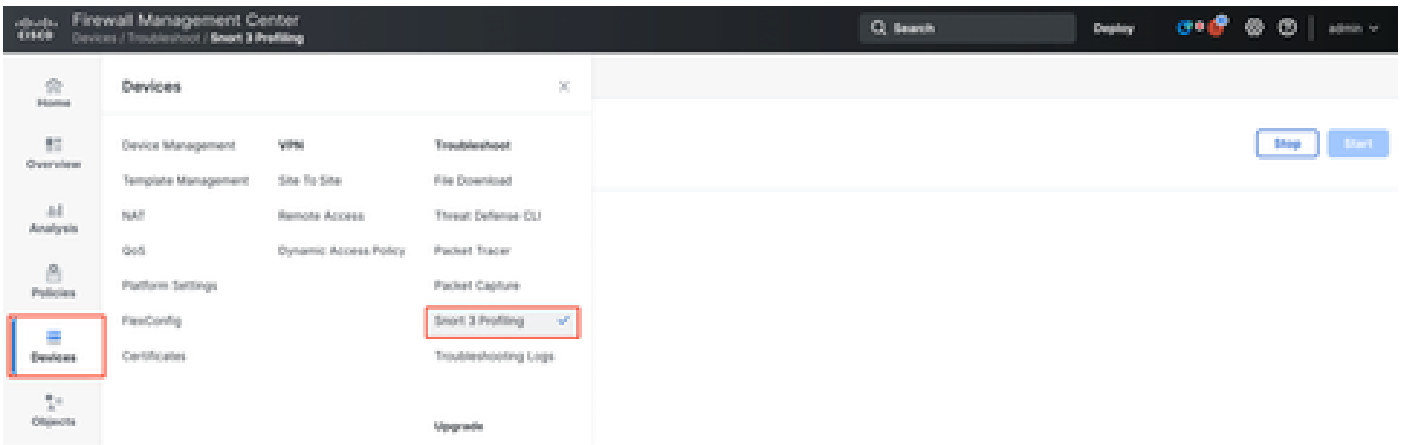
- يقوم منشئ ملفات تعريف قواعد SNORT 3 بتجميع بيانات عن مقدار الوقت المستغرق في معالجة مجموعة من قواعد إقتحام SNORT 3، مما يسلط الضوء على المشكلات المحتملة، ويعرض القواعد التي لها أداء غير مرض.
- يقوم منشئ ملفات تعريف القواعد بعرض قواعد IPS التي تستغرق معظم الوقت للتحقق منها.
- لا يتطلب تشغيل منشئ ملفات تعريف القاعدة إعادة تحميل Snort 3 أو إعادة تشغيله.
- يتم حفظ نتائج تصنيف القواعد بتنسيق JSON في الدليل /ngfw/var/sf/sync/snort_profiling/ ومزامنتها على FMC.
- توجد وحدة تعريف القواعد داخل وحدة التحكم SNORT 3 وتفحص حركة المرور باستخدام آلية اكتشاف التسلل SNORT 3؛ لا يؤثر تمكين تنميط القواعد بشكل ملحوظ على الأداء.

تشغيل تنميط القواعد

- يجب أن تتدفق حركة المرور عبر الجهاز
- بدء عملية تحديد سمات القاعدة عن طريق انتقاء جهاز، ثم النقر فوق الزر "ابدأ"
  - يؤدي بدء جلسة عمل إنشاء ملف التعريف إلى إنشاء مهمة يمكن مراقبتها في الإعلامات ضمن المهام
- المدة الافتراضية لجلسة عمل تحديد القاعدة هي 120 دقيقة
  - يمكن إيقاف جلسة تعريف القاعدة قبل اكتمالها بالضغط على زر الإيقاف
- يمكن عرض النتائج في واجهة المستخدم الرسومية (GUI) وتنزيلها
- يعرض "محفوظات ملف التعريف" نتائج جلسات عمل ملف التعريف السابقة. يمكن للمستخدم فحص نتيجة ملف تعريف محددة بالنقر فوق بطاقة من اللوحة الجانبية اليسرى الخاصة ب "محفوظات ملف التعريف".

قائمة ملف التعريف ل SNORT 3

يمكن الوصول إلى صفحة إنشاء ملفات التعريف من قائمة الأجهزة > ملف تعريف snort 3. تحتوي الصفحة على كل من تنميط القاعدة ووحدة المعالجة المركزية (CPU)، المقسمة إلى علامتي تبويب.



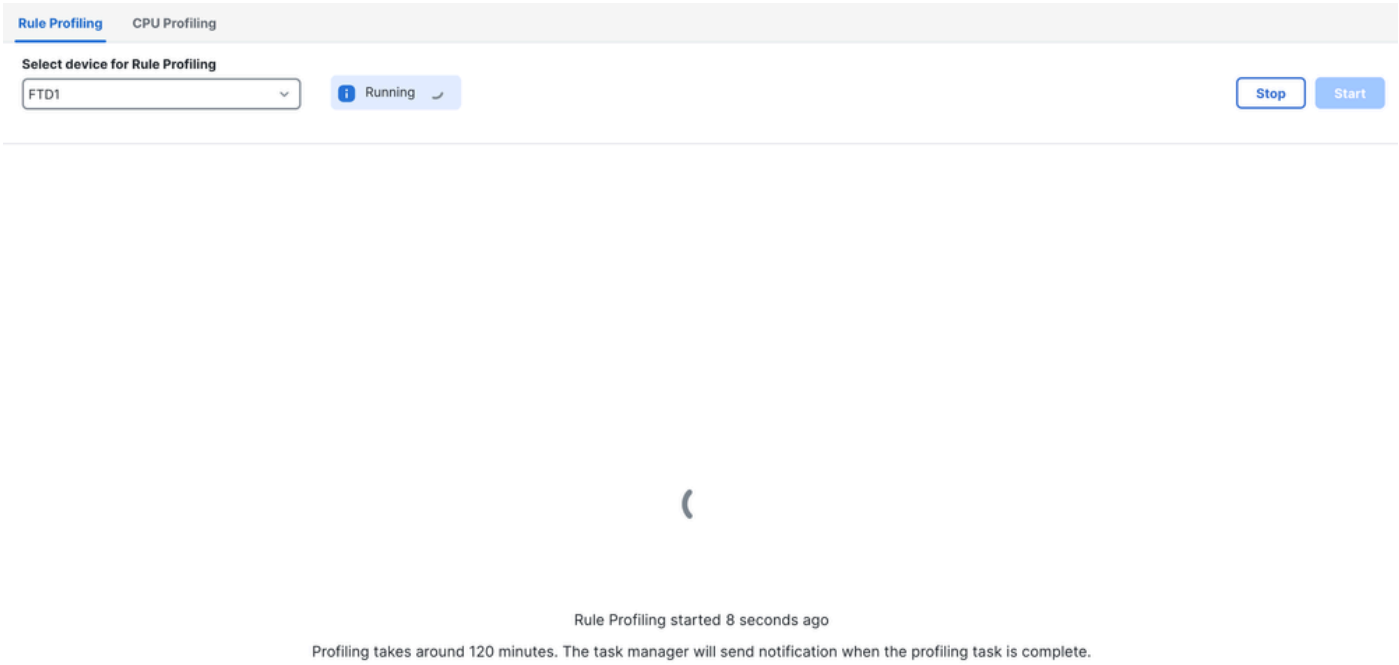
الأجهزة

بدء تحديد سمات القاعدة

لبدء جلسة عمل تحديد قاعدة، انقر فوق بدء. يتم إيقاف جلسة العمل تلقائيا بعد 120 دقيقة.

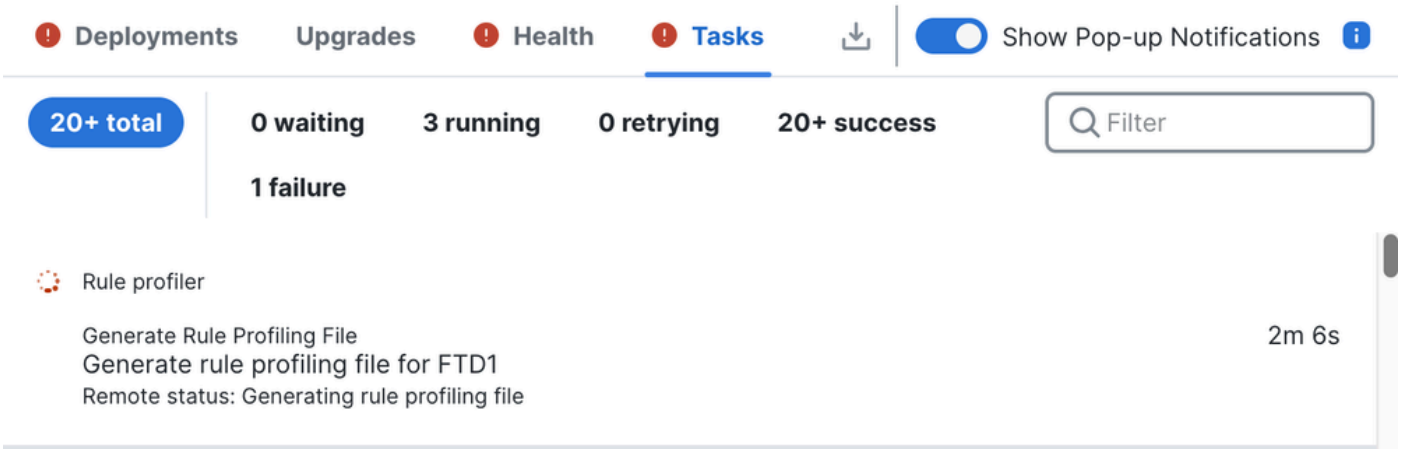
يتعذر على المستخدم تكوين طول جلسة عمل إنشاء ملف التعريف ولكن يمكن إيقافها قبل انقضاء الساعتين.

تنميط القاعدة



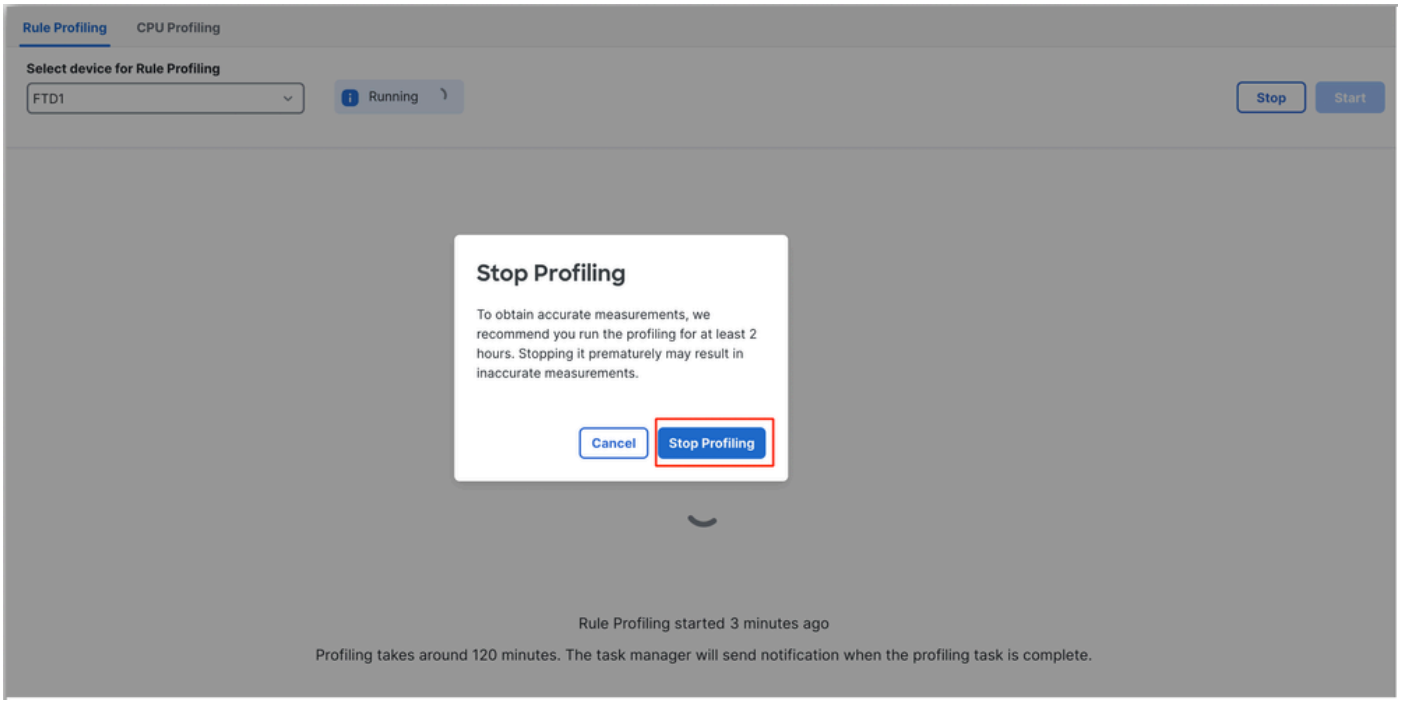
ركض

بعد بدء جلسة عمل إنشاء ملف تعريف القاعدة، يتم إنشاء مهمة. يمكن إيداع هذا في الإعلامات > المهام.



المهام

لإيقاف جلسة عمل تحديد قاعدة قيد التقدم، في حالة الحاجة إلى مقاطعتها قبل التوقف التلقائي، انقر فوق إيقاف والتأكيد.



إيقاف التحليل

بعد تحديد جهاز، يتم عرض أحدث نتيجة ملف التعريف تلقائيا في قسم نتائج تحديد قاعدة البيانات.

يحتوي الجدول على إحصائيات للقواعد التي استغرقت معظم الوقت لمعالجة مفروزة بالترتيب التنازلي حسب إجمالي الوقت (بالميكروثانية (µs) التي إستغرقتها.استهلكت.

النتائج

نتائج منشئ ملفات تعريف القاعدة

يتضمن إخراج منشئ ملفات تعريف القاعدة لقاعدة IPS الحقول التالية:

- ٪ من وقت الشخير - الوقت المستغرق في معالجة القاعدة، نسبة إلى وقت عملية Snort 3
- عمليات التحقق - عدد مرات تنفيذ قاعدة IPS
- التطابقات - عدد مرات تطابق قاعدة IPS بالكامل
- التنبيهات - عدد المرات التي قامت فيها قاعدة IPS بتشغيل تنبيه IPS
- الوقت (µ) - الوقت بالميكروثانية التي قضاها الشخير في التحقق من قاعدة IPS
- متوسط الوقت المستغرق في فحص واحد للقاعدة
- AVG/Match - متوسط الوقت المستغرق في حساب واحد والذي ينتج عنه تطابق
- AVG/Non-Match - متوسط الوقت المستغرق في حساب واحد والذي لم ينتج عنه تطابق
- حالات انتهاء المهلة - عدد المرات التي تجاوزت فيها القاعدة معالجة القاعدة - الحد المكون في إعدادات الأداء المستندة إلى زمن الوصول لنهج AC
- معلق - عدد المرات التي تم فيها تعليق القاعدة بسبب بعض الانتهاكات المتتالية للحد الأدنى

تنزيل النتائج

- يمكن للمستخدم تنزيل نتيجة ملف التعريف ("لقطة") بالنقر فوق الزر "تنزيل لقطة". الملف الذي تم تنزيله بتنسيق csv. ويحتوي على كافة الحقول من صفحة نتائج التحليل.
- إستخراج من ملف .csv الخاص باللقطة:

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

طريقة عرض ملف .csv للقطة:

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

لقطة

تنميط المعالج

نظرة عامة على منشئ ملفات تعريف وحدة المعالجة المركزية (CPU) ل Snort 3

- يقوم منشئ ملفات تعريف وحدة المعالجة المركزية (CPU) بتوصيف وقت وحدة المعالجة المركزية (CPU) الذي تستغرقه الوحدات النمطية/المفتشون في برنامج Snort 3 لمعالجة الحزم في فترة زمنية معينة. وهو يعطي فكرة عن مقدار إستهلاك وحدة المعالجة المركزية (CPU) في كل وحدة، فيما يتعلق بإجمالي وحدة المعالجة

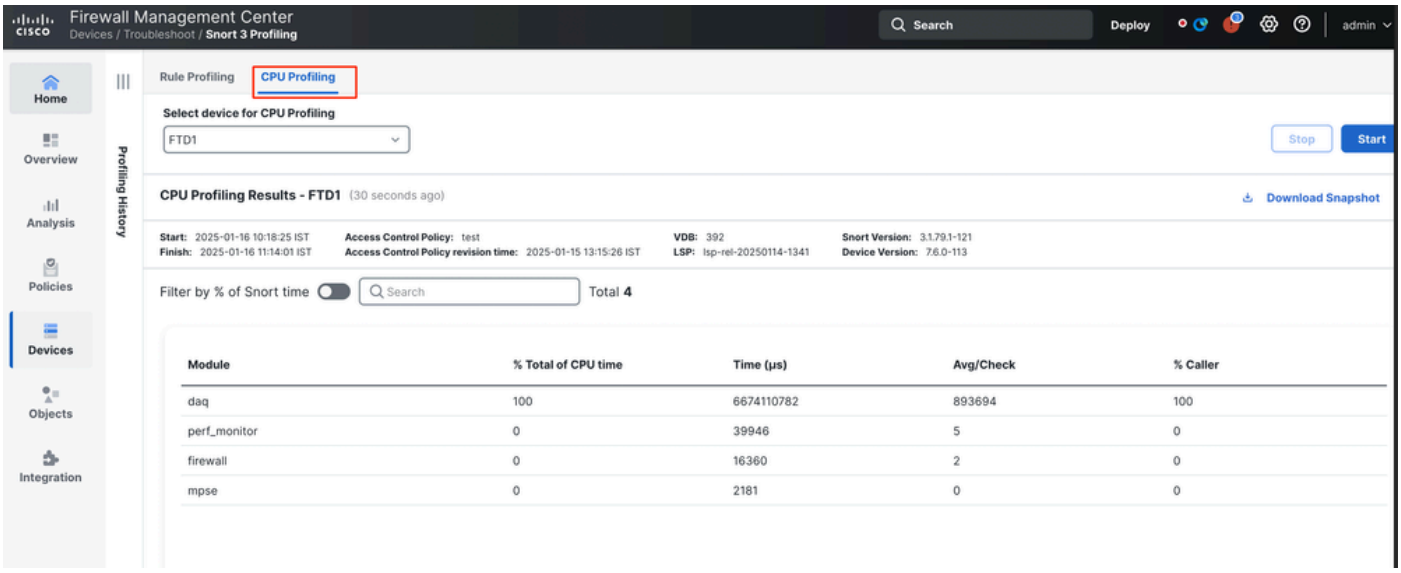
المركزية (CPU) التي تستهلكها عملية Snort 3.
- لا يتطلب إستخدام منشئ ملفات تعريف وحدة المعالجة المركزية إعادة تحميل التكوين أو إعادة تشغيل Snort 3، وبالتالي تجنب وقت التوقف عن العمل.
- تعرض نتيجة منشئ ملفات تعريف وحدة المعالجة المركزية وقت المعالجة الذي تستغرقه جميع الوحدات النمطية أثناء جلسة عمل ملف التعريف الأخيرة.
- يتم حفظ نتائج تصنيف وحدة المعالجة المركزية (CPU) بتنسيق JSON تحت الدليل /ngfw/var/sf/sync/cpu_profiling/ ومزامنتها على دليل FMC /var/sf/peers/<device uid>/sync/cpu_profiling.

- تمت إضافة صفحة ملف تعريف Snort 3 جديدة في واجهة مستخدم FMC
- يمكن الوصول إلى هذه الصفحة من الأجهزة > قائمة إنشاء ملفات تعريف SNORT 3 > علامة التبويب تعريف وحدة المعالجة المركزية (CPU)
- أستخدم لقطة التنزيل على علامة التبويب "إنشاء ملفات تعريف وحدة المعالجة المركزية (CPU)" لتنزيل لقطة لنتائج إنشاء ملفات التعريف بتنسيق CSV.

علامة التبويب إنشاء ملفات تعريف وحدة المعالجة المركزية

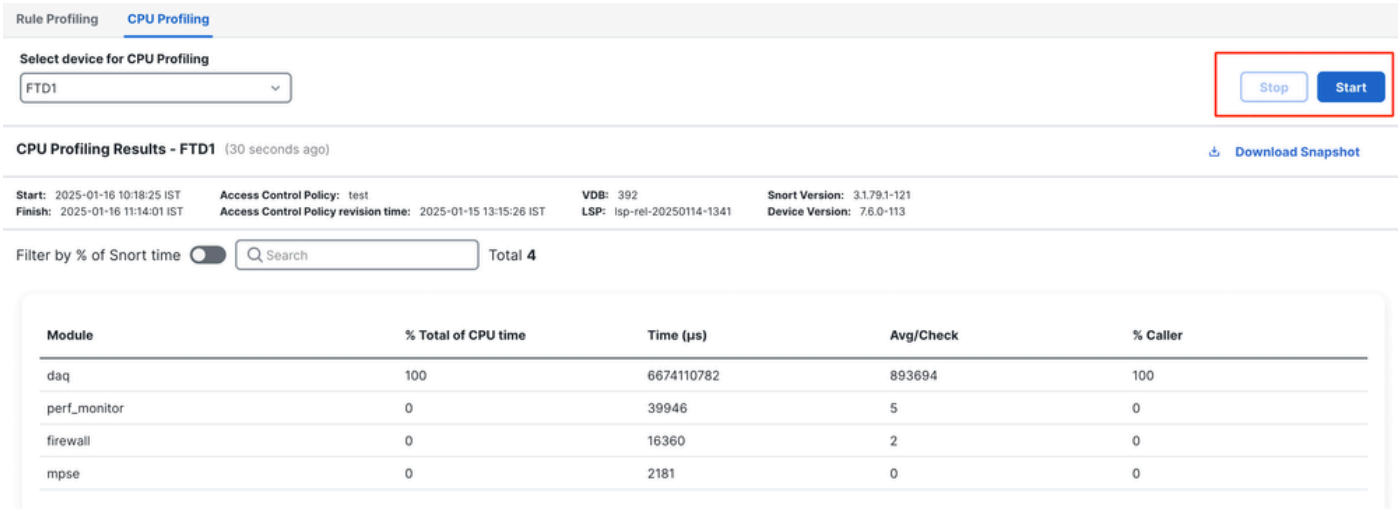
يتم الوصول إلى صفحة ملف تعريف وحدة المعالجة المركزية (CPU) من الأجهزة > قائمة ملف تعريف SNORT 3 >علامة التبويب تعريف وحدة المعالجة المركزية (CPU).

وهو يحتوي على أداة تحديد الجهاز وأزرار بدء/إيقاف وزر لقطة التنزيل وقسم نتائج التحديد وقسم محفوظات إنشاء ملفات التعريف على الجانب الأيسر الذي يتم توسيعه عند النقر عليه.



تنميط المعالج

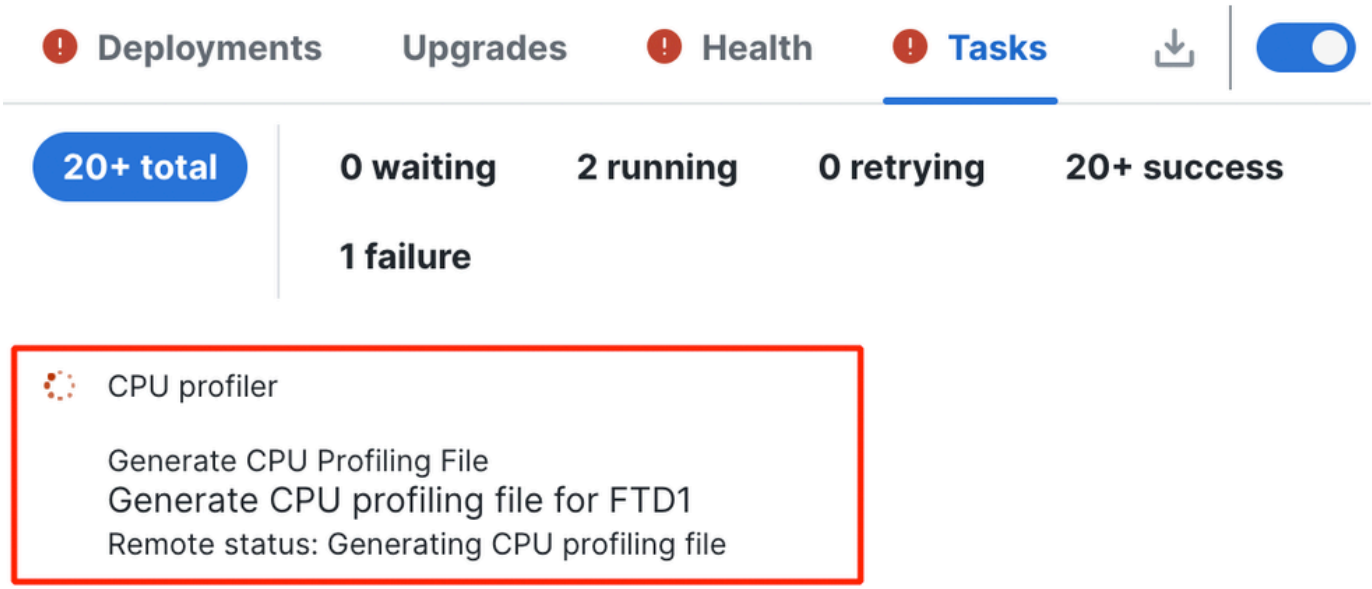
لبدء جلسة عمل ملف تعريف وحدة المعالجة المركزية (CPU)، انقر فوق بدء. يتم عرض هذه الصفحة عند بدء جلسة العمل.



بدء

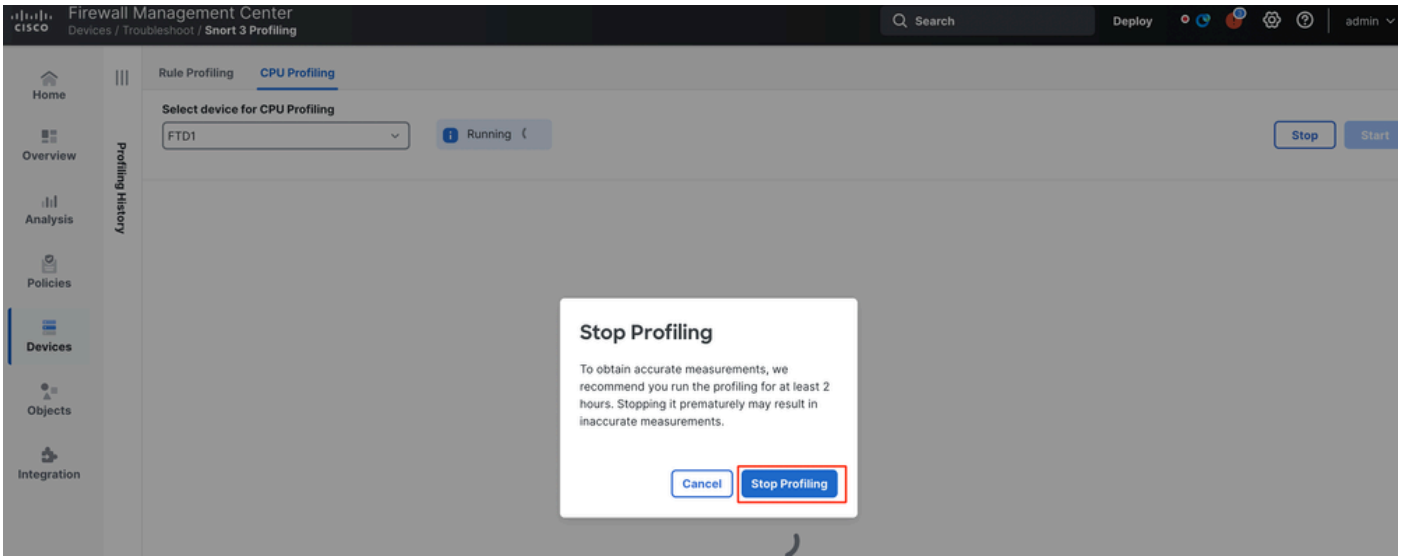
ركض

بعد بدء جلسة عمل ملف تعريف وحدة المعالجة المركزية، يتم إنشاء مهمة. يمكن إيداع هذه الإجراء في الإعدامات > المهام.



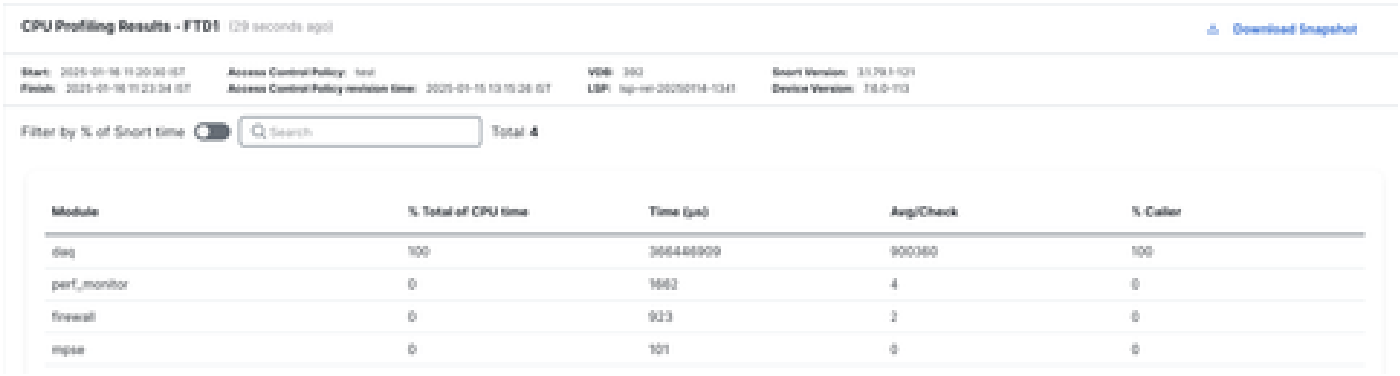
المهام

- لإيقاف جلسة عمل ملف تعريف وحدة المعالجة المركزية (CPU) قيد التقدم، انقر فوق إيقاف.
- يظهر مربع حوار التأكيد. طقطقة يوقف التوصيف.



إيقاف التشغيل

يتم عرض أحدث نتيجة ملف التعريف في قسم نتائج ملف تعريف وحدة المعالجة المركزية (CPU).



النتائج

شرح نتائج منشئ ملفات تعريف وحدة المعالجة المركزية

- يشير عمود "الوحدة النمطية" إلى اسم الوحدة النمطية/المفتش.
- يشير العمود "٪ إجمالي وقت وحدة المعالجة المركزية" إلى نسبة الوقت المستغرق بواسطة الوحدة فيما يتعلق بالوقت الإجمالي المستغرق من قبل Snort 3 في معالجة حركة المرور. إذا كانت هذه القيمة أكبر بكثير من تلك الخاصة بالوحدات الأخرى، فإن الوحدة النمطية تساهم أكثر في الأداء غير المرضي لـ Snort 3.
- يمثل "الوقت (µ)" إجمالي الوقت بالثواني الدقيقة الذي تستغرقه كل وحدة نمطية.
- يمثل "avg/Check" متوسط الوقت المستغرق بواسطة الوحدة النمطية لكل مرة يتم فيها إستدعاء الوحدة النمطية.
- يشير "٪ المتصل" إلى الوقت المستغرق بواسطة الوحدة النمطية الفرعية (في حالة تكوينها) فيما يتعلق بالوحدة النمطية الرئيسية. ويتم إستخدامها بشكل رئيسي لأغراض تصحيح أخطاء المطورين.

نتيجة منشئ ملفات تعريف وحدة المعالجة المركزية - تنزيل لقطة

- يمكن للمستخدم تنزيل لقطة نتيجة ملف التعريف بالنقر فوق تنزيل لقطة. الملف الذي تم تنزيله بتنسيق csv. ويحتوي على كافة الحقول من صفحة نتائج التحليل كما هو موضح في هذا المثال.
- إستخراج من ملف .csv الخاص باللقطة:

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

لقطة

تصفية نتائج تنميط وحدة المعالجة المركزية

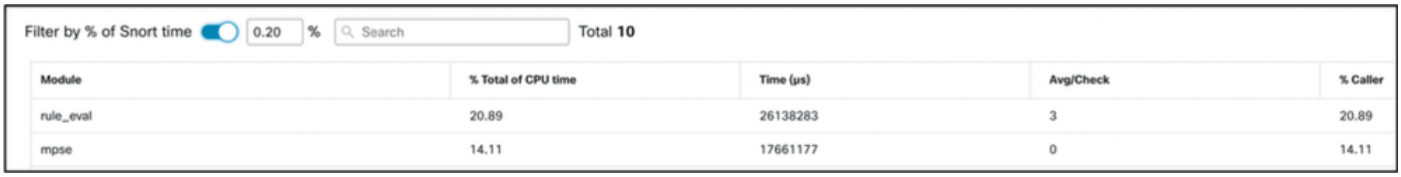
يمكن تصفية نتائج التحليل باستخدام:

- "التصفية حسب ٪ من وقت الشخير" - يسمح لك بتصفية الوحدات النمطية التي

استغرق تنفيذها أكثر من n٪ من وقت التحليل.

- بحث - يسمح لك بإجراء بحث نصي من خلال أي حقل موجود في جدول النتائج.

يمكن فرز أي عمود باستثناء "وحدة نمطية" بالنقر فوق رأسه.



النتائج

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).