تحديد إصدار الشبكة النشط الذي يتم تشغيله على برنامج الدفاع ضد تهديد FirePOWER (FTD)

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لتأكيد إصدار البرنامج النشط الذي يتم تشغيله باستخدام برنامج FTD من Cisco عندما تتم إدارته بواسطة Cisco FDM أو Cisco FMC أو CDO.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة FireSIGHT (FMC) من Cisco
- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- مدير جهاز FirePOWER (FDM) من Cisco
- Cisco Defense Orchestrator (CDO)

المكونات المستخدمة

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

- برنامج الدفاع ضد تهديد FirePOWER الإصدار 6.7.0 و 7.0.0 من Cisco
- مركز إدارة Cisco Firepower الإصدار 6.7.0 و 7.0.0
- Cisco Defense Orchestrator

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.

معلومات أساسية

قام نظام منع الاقتحام SNORT®إطلاق برنامج Snort 3 رسمياً، وهو عبارة عن ترقية شاملة تتميز بتحسينات ومميزات جديدة تعمل على تحسين الأداء والمعالجة السريعة وقابلية التوطير المحسنة لشبكتك، بالإضافة إلى مجموعة من الإضافات التي تزيد عن 200+ حتى يمكنك إنشاء إعداد مخصص لشبكتك.

وتشمل مزايا الشوط 3، ولكنها لا تقتصر على، ما يلي:

- أداء محسن
- تحسين فحص SMBv2
- إمكانات اكتشاف البرامج النصية الجديدة
- فحص HTTP/2
- مجموعات القواعد المخصصة
- بناء الجملة الذي يجعل قواعد التطفل المخصصة أكثر سهولة للكتابة.
- أسباب قد تؤدي إلى إسقاط نتائج مضمنة في أحداث التسلل.
- الـ تتم إعادة تشغيل أي عمليات تغييري عند نشر التغييرات إلى قاعدة بيانات المورد (VDB) وسياسات قائمة مكونات الخدمة (SSL) وأجهزة الكشف عن التطبيقات المخصصة ومصادر هوية البوابة المقيدة واكتشاف هوية خادم TLS.
- قابلية صيانة محسنة، بسبب إرسال بيانات تتبع بيانات خاصة بـ 3 أجهزة إستشعار عن بعد إلى شبكة نجاح Cisco وسجلات أستكشاف الأخطاء وإصلاحها بشكل أفضل.

تم تقديم الدعم لـ Snort 3.0 لـ 6.7.0 Cisco Firepower Threat Defense (FTD)، فقط عند إدارة FTD مع خلال مدير أجهزة FirePOWER (FDM) من Cisco.

ملاحظة: بالنسبة لعمليات النشر الجديدة في برنامج الإرسال فائق السرعة (FTD) الإصدار 6.7.0 التي تم إدارتها بواسطة FDM، يعد برنامج Snort 3.0 محرك الفحص الافتراضي. إذا قمت بترقية FTD إلى 6.7 من إصدار أقدم، فإن Snort 2.0 يبقى محرك التفتيش النشط، لكن يمكنك التبديل إلى Snort 3.0.

ملاحظة: بالنسبة لهذا الإصدار، الـ يدعم برنامج Snort 3.0 الموجهات الظاهرية أو قواعد التحكم في الوصول المستندة إلى الوقت أو فك تشفير إتصالات TLS 1.1 أو الاتصالات الأقل. قم بتمكين snort 3.0 فقط إذا لم تكن بحاجة إلى هذه المميزات.

بعد ذلك، قدم Firepower الإصدار 7.0 دعم SNORT 3.0 لأجهزة الدفاع عن تهديد FirePOWER التي تتم إدارتها من قبل كل من الطرازين؛ برنامج FDM من Cisco ومركز إدارة FirePOWER (FMC) من Cisco.

ملاحظة: بالنسبة لعمليات النشر الجديدة في برنامج الإرسال فائق السرعة (FTD) الإصدار 7.0، يعد الطراز Snort 3 الآن محرك الفحص الافتراضي. تستمر عمليات النشر التي تمت ترقيتها في إستخدام Snort 2، ولكن يمكنك التبديل في أي وقت.

تحذير: يمكنك التبديل بحرية بين الشوريتين 2.0 و 3.0، حتى يمكنك الرجوع إلى التغيير إذا لزم الأمر. تتم مقاطعة حركة المرور عند تبديل الإصدارات.

تحذير: قبل التبديل إلى Snort 3، يوصى بشدة بقراءة دليل تكوين FirePOWER Management Center snort 3 وفهمه. عليك أن تولي اهتمام خاص لقيود الميزات وإرشادات الترحيل. على الرغم من أن الترقية إلى Snort 3 مصممة لتقليل التأثير إلى الحد الأدنى، إلا أن الميزات لا تتوافق بالتعيين بدقة. يمكن أن تساعدك الخطة والتحضير قبل الترقية على التأكد من معالجة حركة المرور كما هو متوقع.

تحديد إصدار Active Snort الذي يتم تشغيله على FTD

واجهة سطر الأوامر (CLI) لـ FTD

لتحديد إصدار snort النشط الذي يتم تشغيله على FTD، قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) في FTD وقم بتشغيل الأمر show snort3 status:

مثال 1: عندما لا يوجد إخراج معروض، يقوم FTD بتشغيل Snort 2.

```
<#root>

>

show snort3 status

>
```

مثال 2: عندما يظهر الإخراج، الذي يتم تشغيله حاليا في الإصدار 2، يقوم FTD بتشغيل الإصدار 2.

```
<#root>

>

show snort3 status

Currently running Snort 2
```

المثال 3: عند عرض الإخراج، الذي يتم تشغيله حاليا في الإصدار 3، يقوم برنامج الإرسال فائق السرعة (FTD) بتشغيل الإصدار 3.

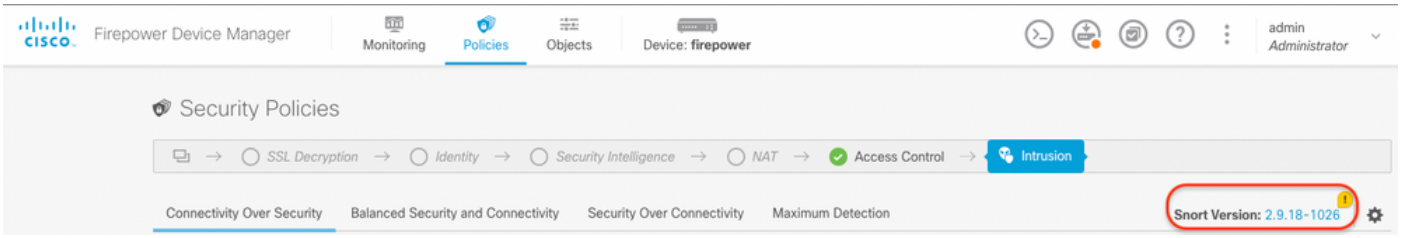
```
<#root>

>

show snort3 status


Currently running Snort 3
```

تتم إدارة FTD بواسطة Cisco FDM

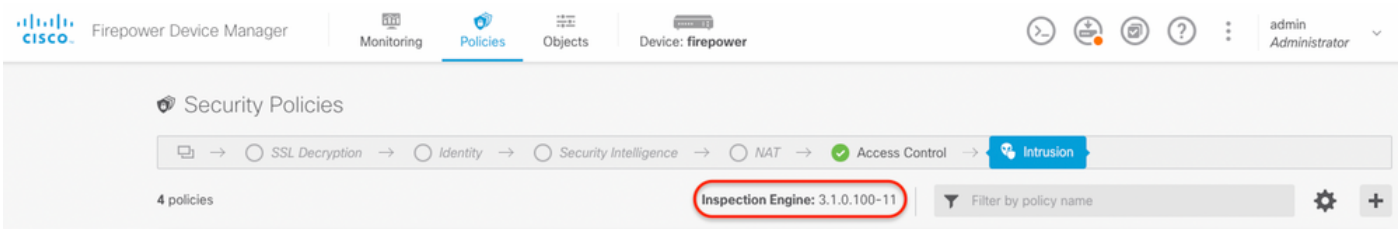
لتحديد إصدار البرنامج النشط الذي يتم تشغيله على FTD الذي تتم إدارته بواسطة Cisco FDM، أكمل الخطوات التالية:

1. قم بتسجيل الدخول إلى Cisco FTD من خلال واجهة الويب FDM.
2. من القائمة الرئيسية، حدد سياسات.
3. ثم حدد علامة التبويب إقتحام.
4. ابحث عن إصدار snort أو قسم محرك الفحص لتأكيد إصدار snort النشط في FTD.

مثال 1: يشغل FTD الإصدار 2 من snort.



مثال 2: يشغل FTD الإصدار 3 من snort.



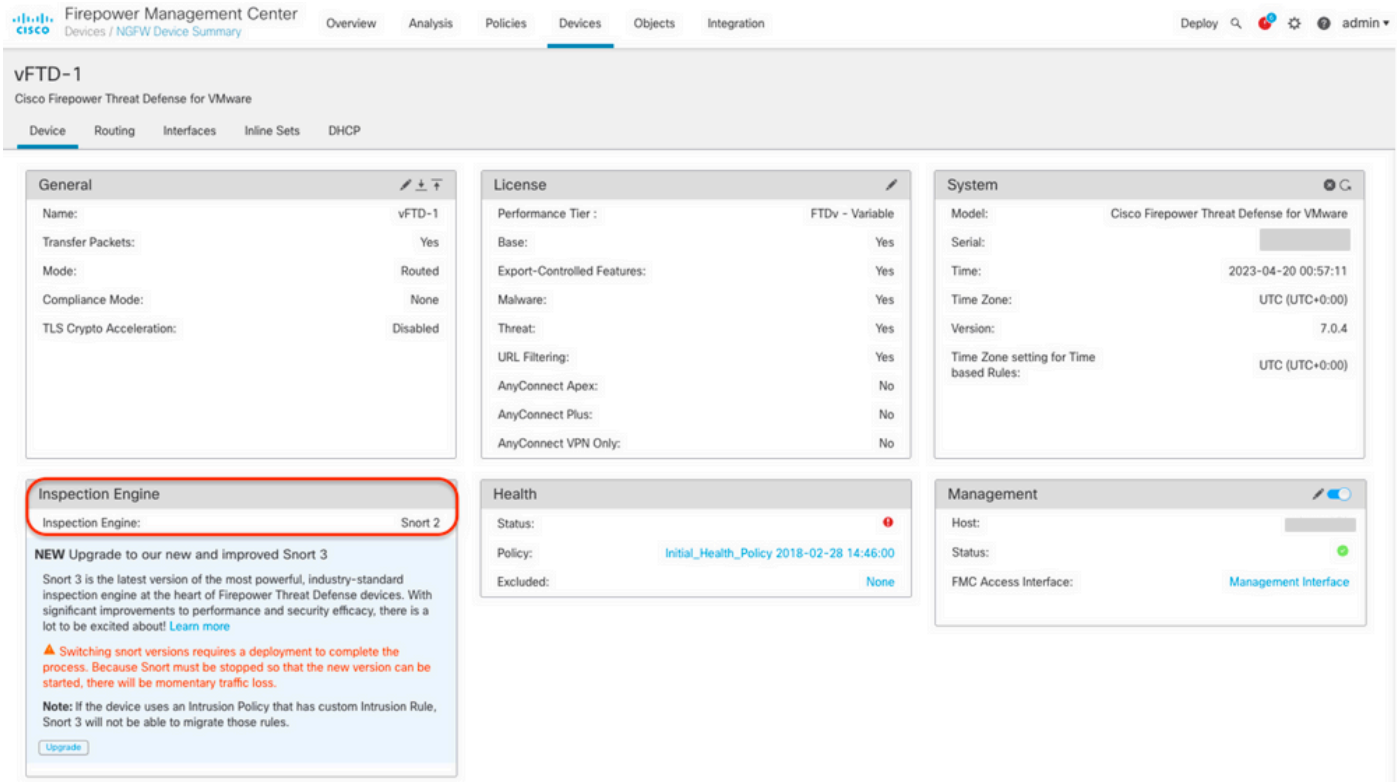
تتم إدارة FTD بواسطة Cisco FMC

لتحديد إصدار التمثال النشط الذي يتم تشغيله على FTD تتم إدارته بواسطة وحدة التحكم في الإدارة الأساسية (FMC) من Cisco، أكمل الخطوات التالية:

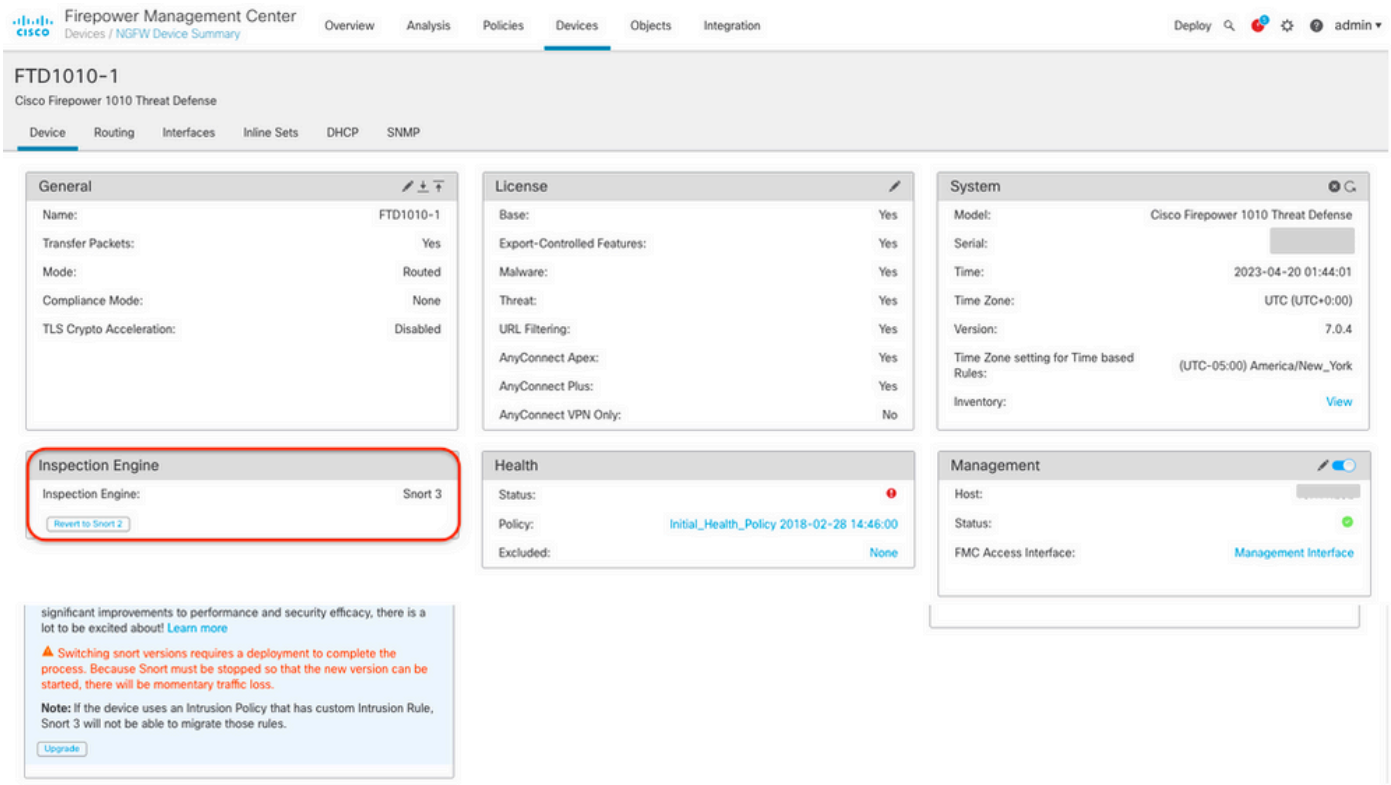
1. سجل الدخول إلى واجهة ويب Cisco FMC.
2. من قائمة الأجهزة، حدد إدارة الجهاز.
3. ثم حدد جهاز FTD المناسب.

4. انقر أيقونة تحرير القلم الرصاص.
5. حدد علامة التبويب الجهاز وابحث عن قسم محرك الفحص لتأكيد إصدار snort النشط في FTD:

مثال 1: يشغل FTD الإصدار 2 من snort.



مثال 2: يشغل FTD الإصدار 3 من snort.

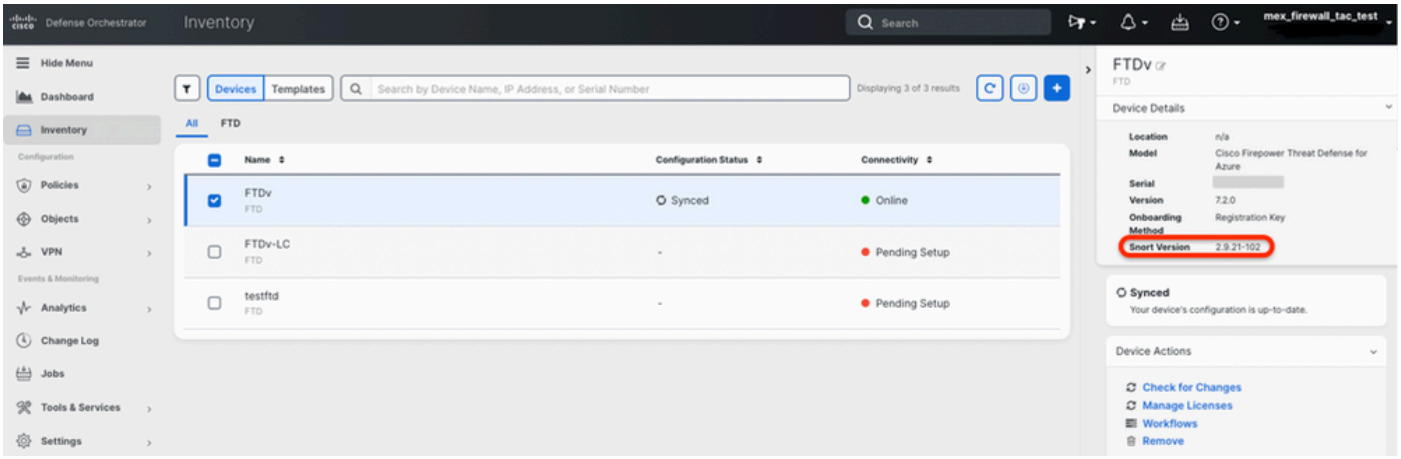


تتم إدارة FTD بواسطة Cisco CDO

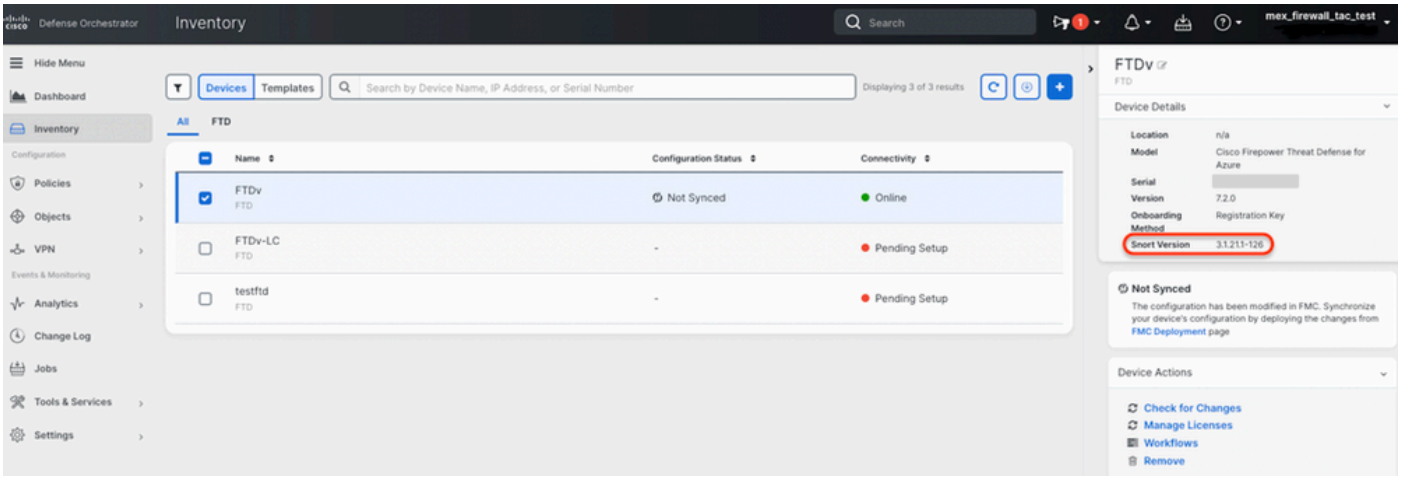
لتحديد إصدار البرنامج النشط الذي يتم تشغيله على FTD تتم إدارته بواسطة Cisco Defense Orchestrator، أكمل الخطوات التالية:

1. سجل الدخول إلى واجهة الويب Cisco Defense Orchestrator.
2. من قائمة المخزون، حدد جهاز FTD المناسب.
3. في قسم تفاصيل الجهاز، ابحث عن إصدار snort:

مثال 1: يشغل FTD الإصدار 2 من snort.



مثال 2: يشغل FTD الإصدار 3 من snort.



معلومات ذات صلة

- ملاحظات إصدار Cisco Firepower، الإصدار 6.7.0
- ملاحظات إصدار Cisco Firepower، الإصدار 7.0
- موقع Snort 3 على الويب
- الدعم التقني والمستندات - Cisco Systems

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).