الترقية من Snort 2 إلى Snort 3 عبر FMC

المحتويات

المقدمة

يوضح هذا المستند كيفية الترقية من إصدار Snort 2 و Snort 3 في مركز مدير الطاقة النارية (FMC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Firepower Threat Defense
- مركز إدارة Firepower
- Snort

المكونات المستخدمة

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

- FMC 7.0
- FTD 7.0

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

تمت إضافة ميزة snort 3 في الإصدار 6.7 لـ FirePOWER Device Manager (FDM) و Cisco Defense Orchestrator (CDO)؛ في الإصدار 7.0 لمركز إدارة FirePOWER (FMC).

تم تصميم برنامج Snort 3.0 لمعالجة هذه التحديات:

1. تقليل إستخدام وحدة المعالجة المركزية والذاكرة.
2. تحسين فعالية فحص HTTP.
3. تحميل التهيئة بسرعة فائقة وإعادة التشغيل بسرعة مذهلة.
4. قابلية برمجة أفضل لزيادة الميزات بشكل أسرع.

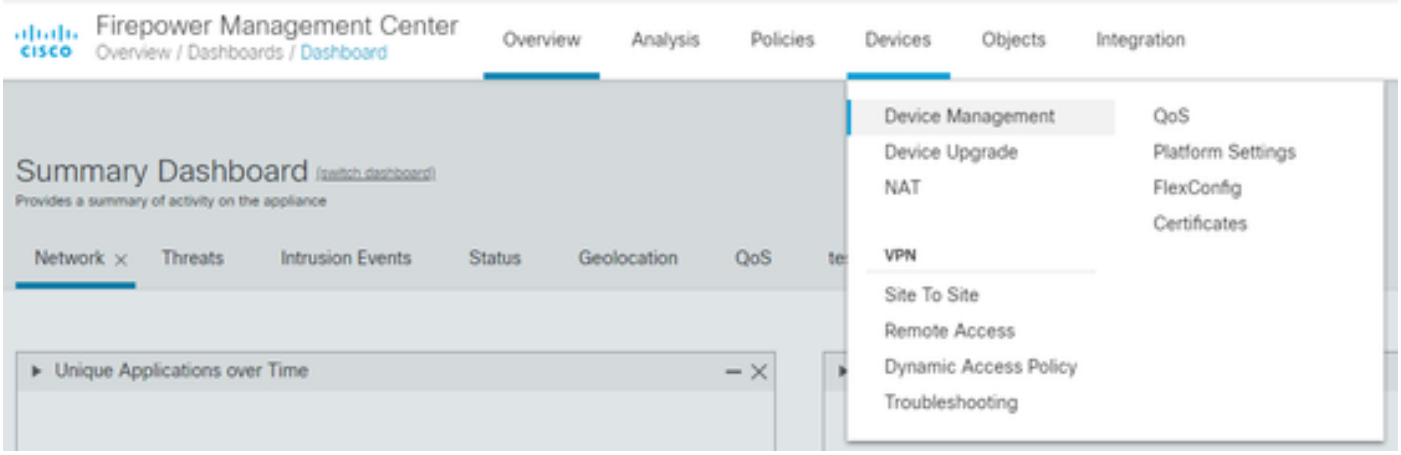
التكوين

ترقية إصدار الشبكة

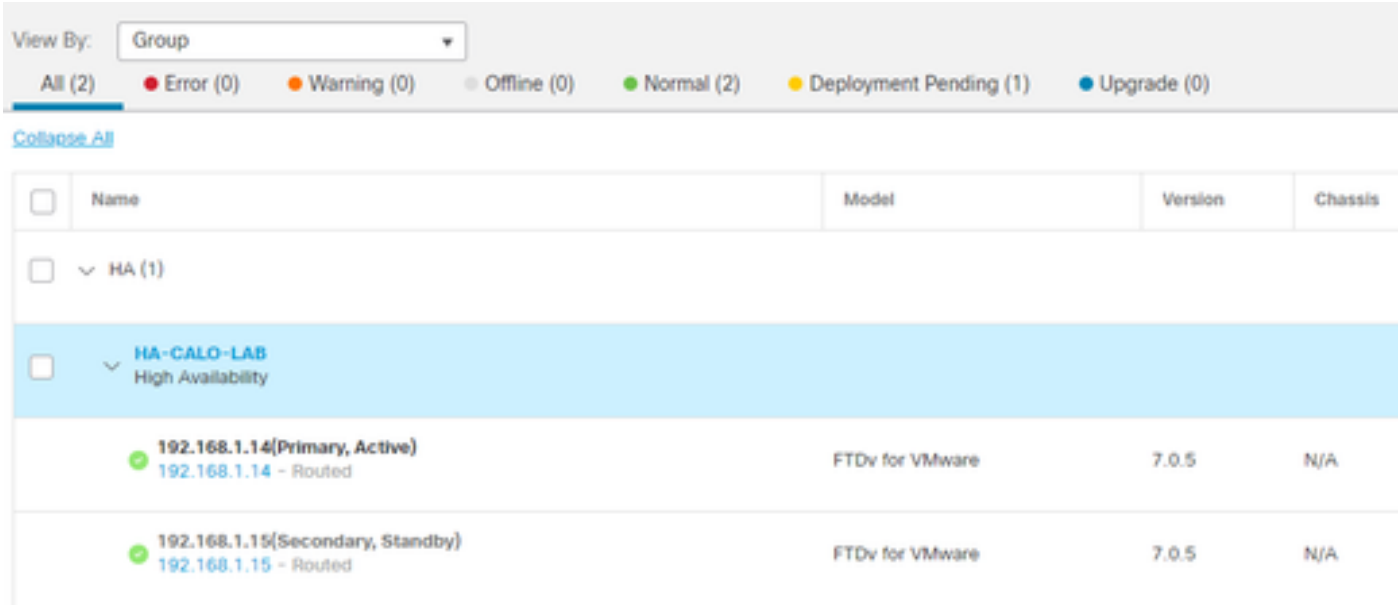
الطريقة 1

1. تسجيل الدخول إلى مركز إدارة Firepower.

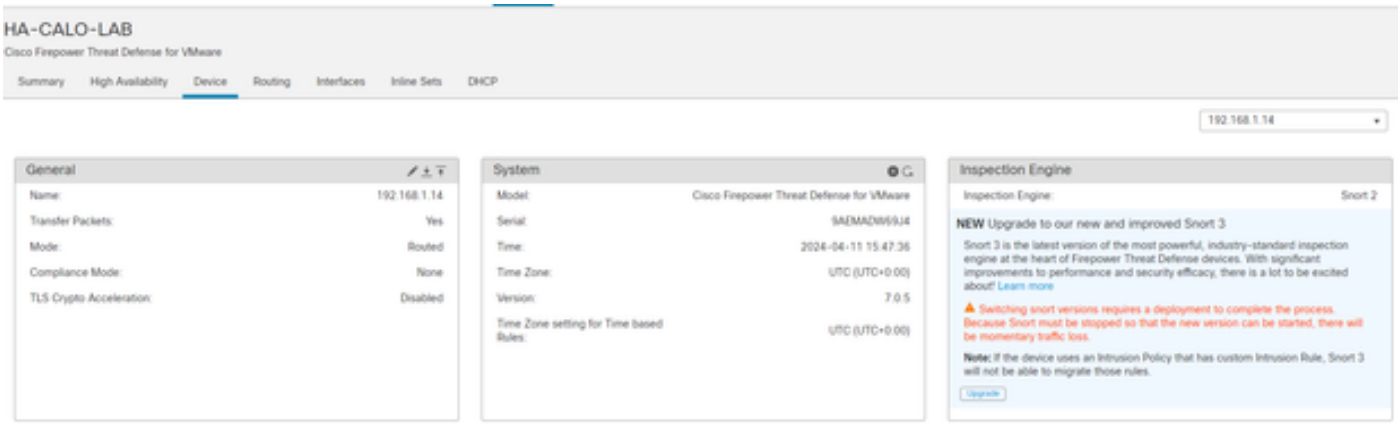
2. في علامة التبويب الجهاز، انتقل إلى الأجهزة > إدارة الأجهزة.



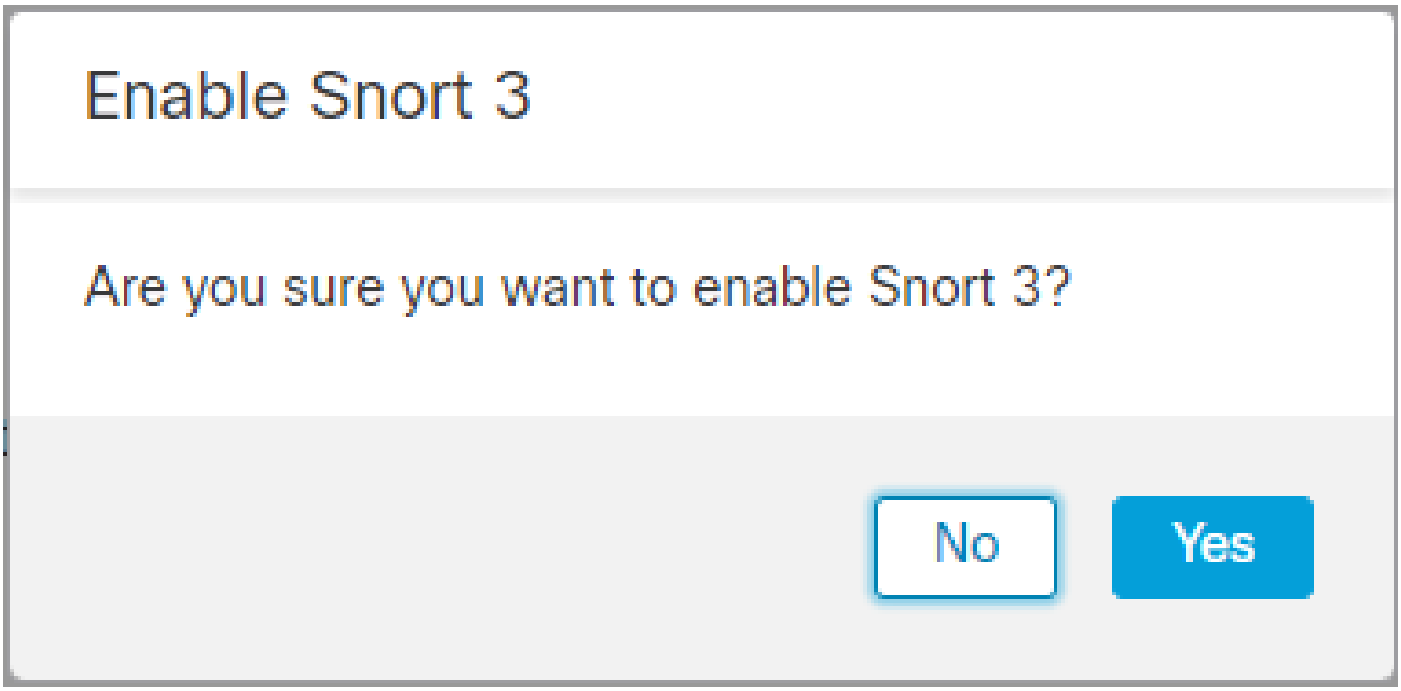
3. حدد الجهاز الذي تريد تغيير إصدار Snort.



4. انقر فوق علامة التبويب الجهاز وانقر فوق الزر ترقية في قسم محرك الفحص.



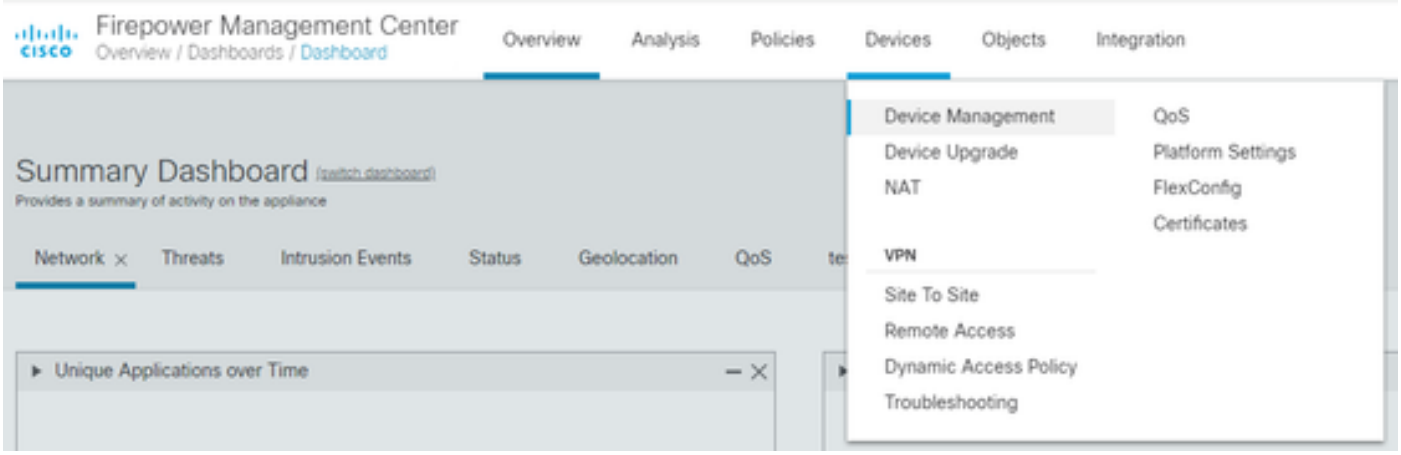
5. تأكد من إختيارك.



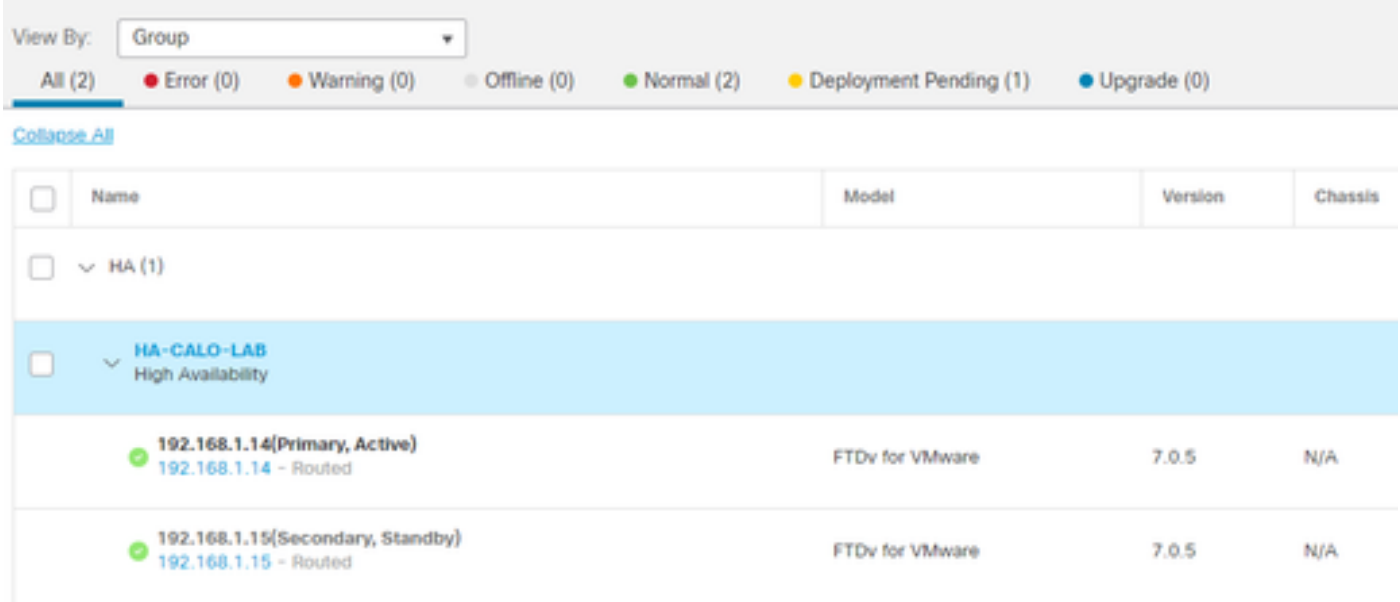
الطريقة 2

1. تسجيل الدخول إلى مركز إدارة Firepower.

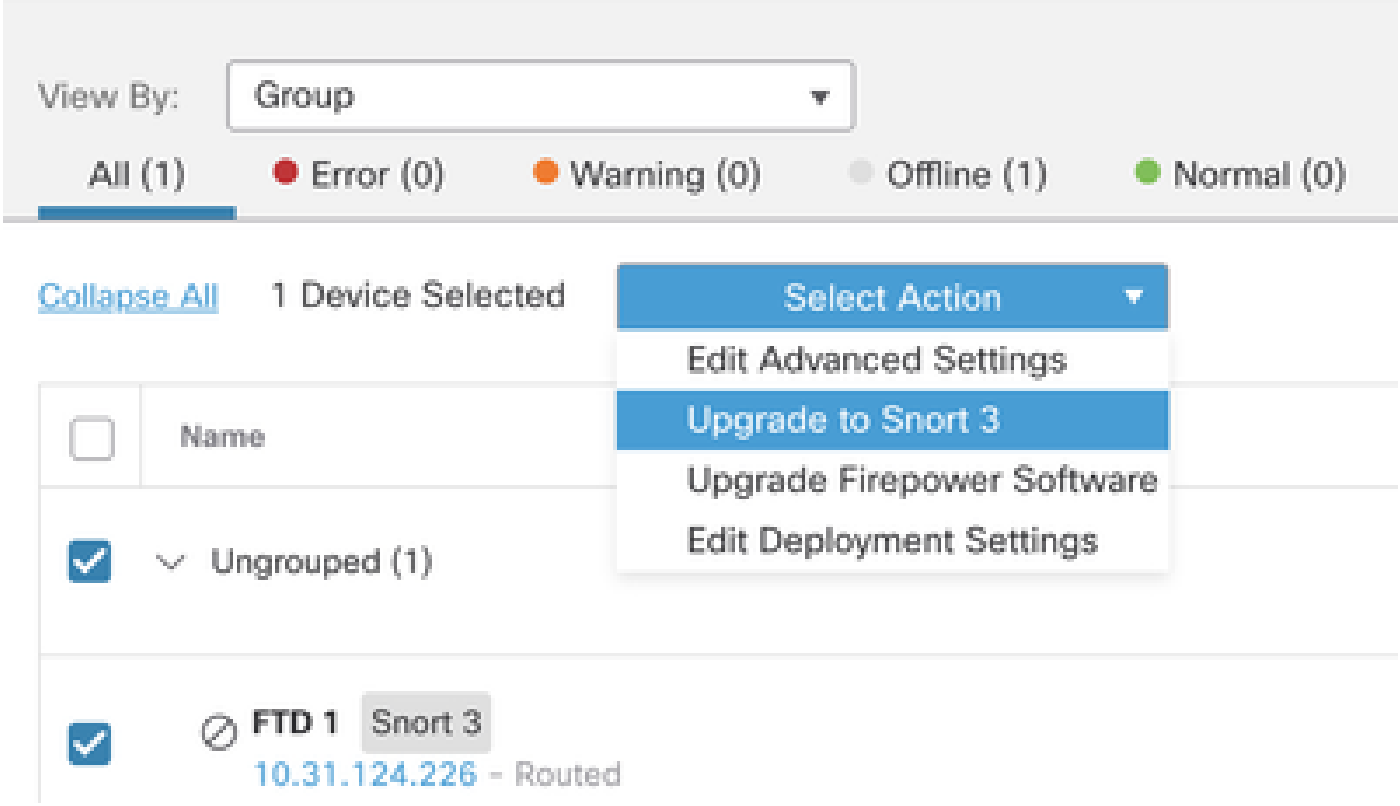
2. في علامة التبويب الجهاز، انتقل إلى الأجهزة > إدارة الأجهزة.



3. حدد الجهاز الذي تريد تغيير إصدار Snort.



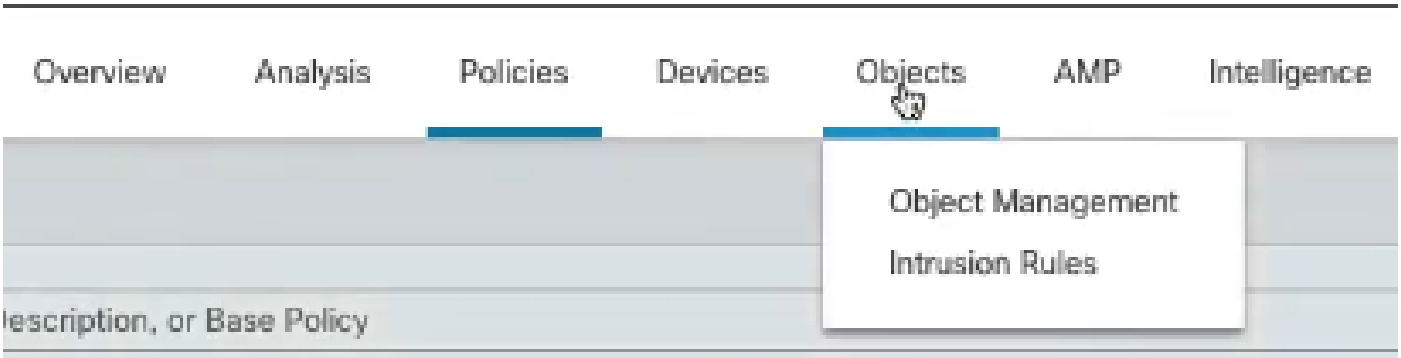
4. انقر فوق الزر تحديد الإجراء وحدد الترقية إلى Snort 3.



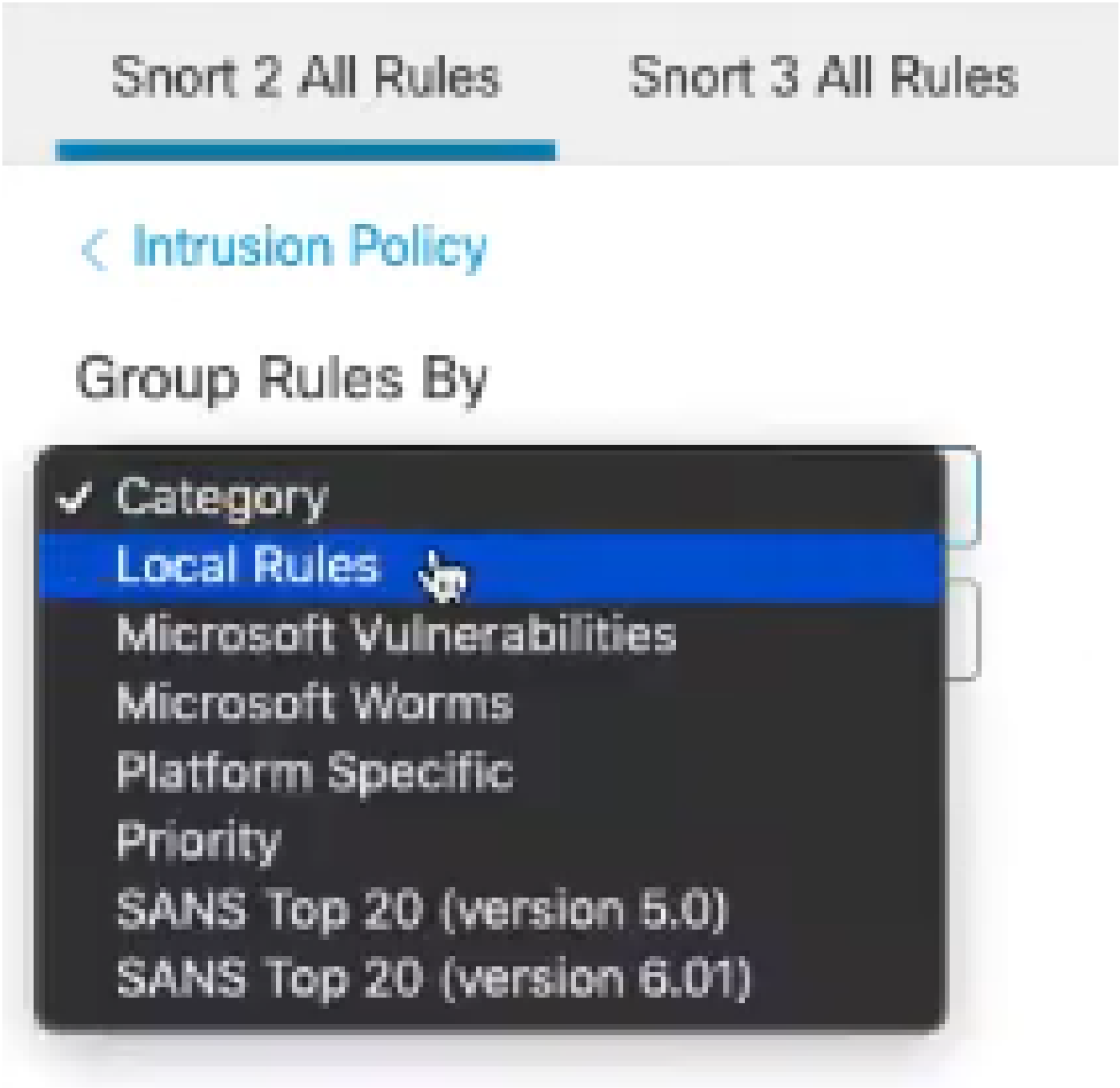
ترقية قواعد التطفل

وبالإضافة إلى ذلك، تحتاج إلى تحويل قواعد الشخير 2 إلى قواعد الشخر 3.

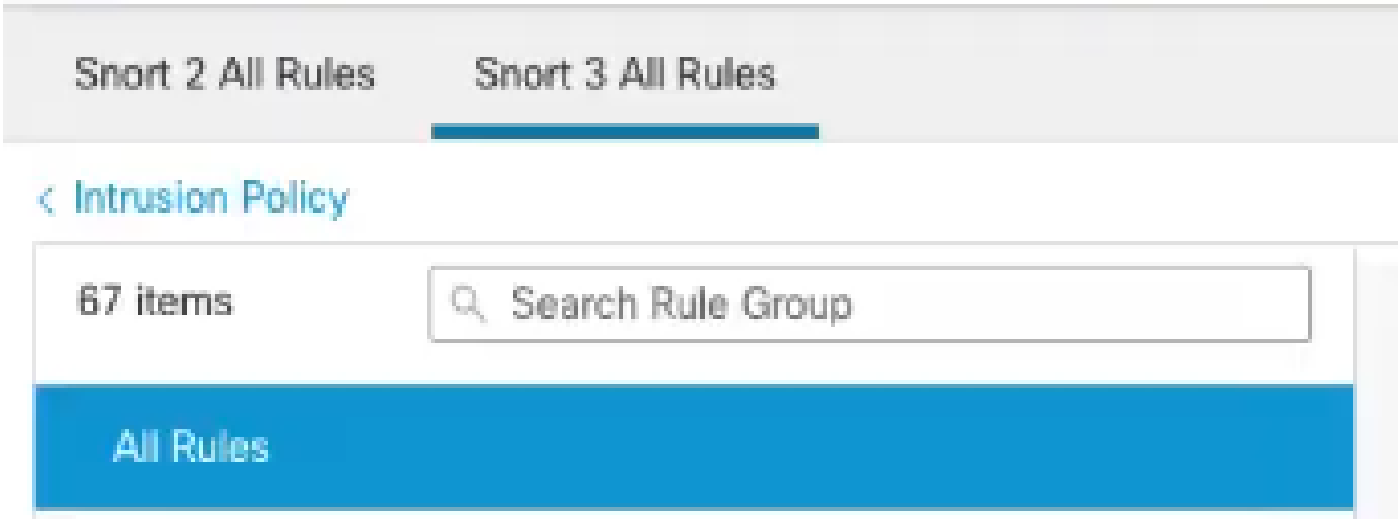
1. حدد من القائمة كائنات > قواعد التطفل.



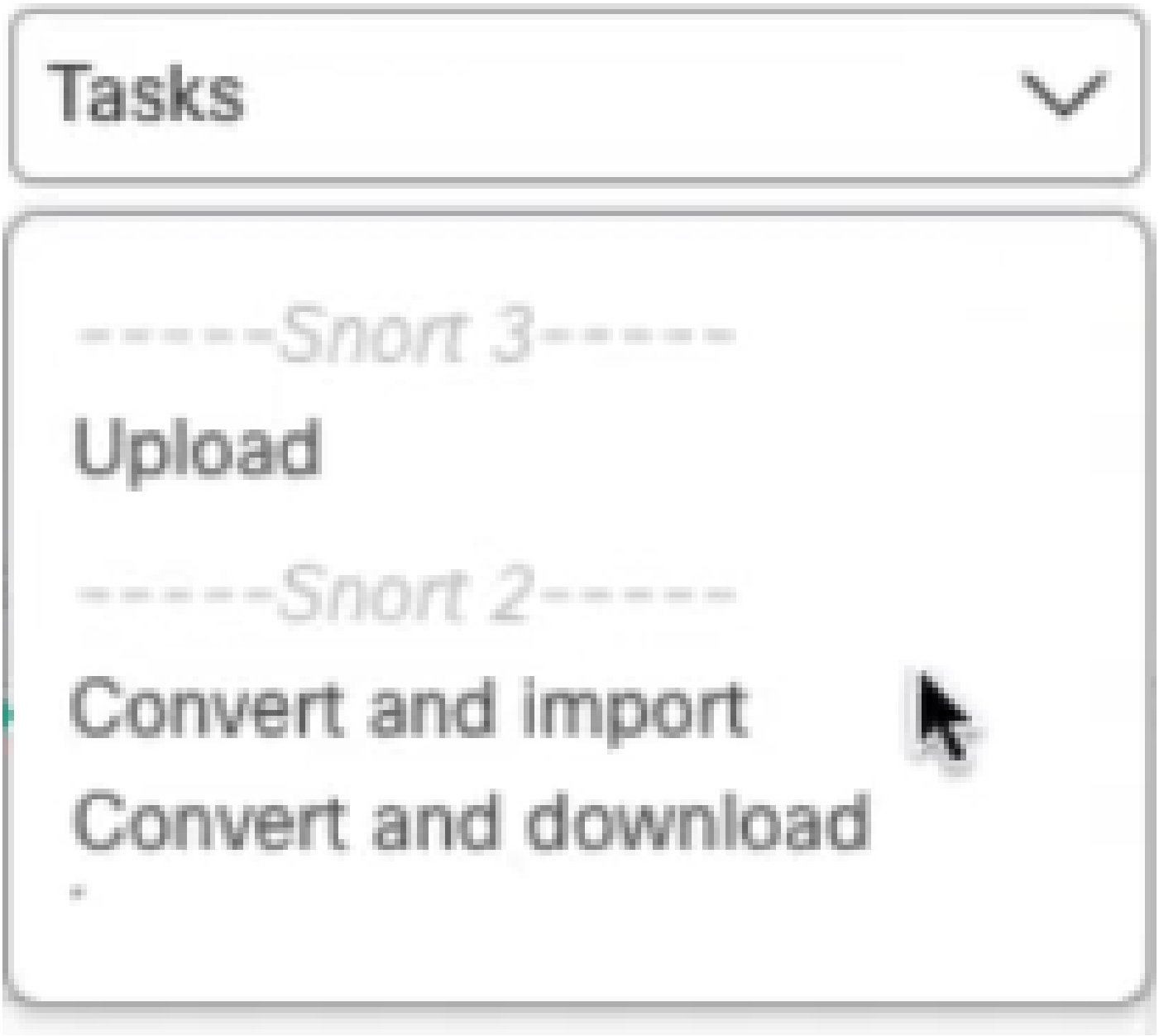
2.حدد من القائمة Snort 2 علامة التبويب "كافة القواعد" > "قواعد المجموعة" > "القواعد المحلية".



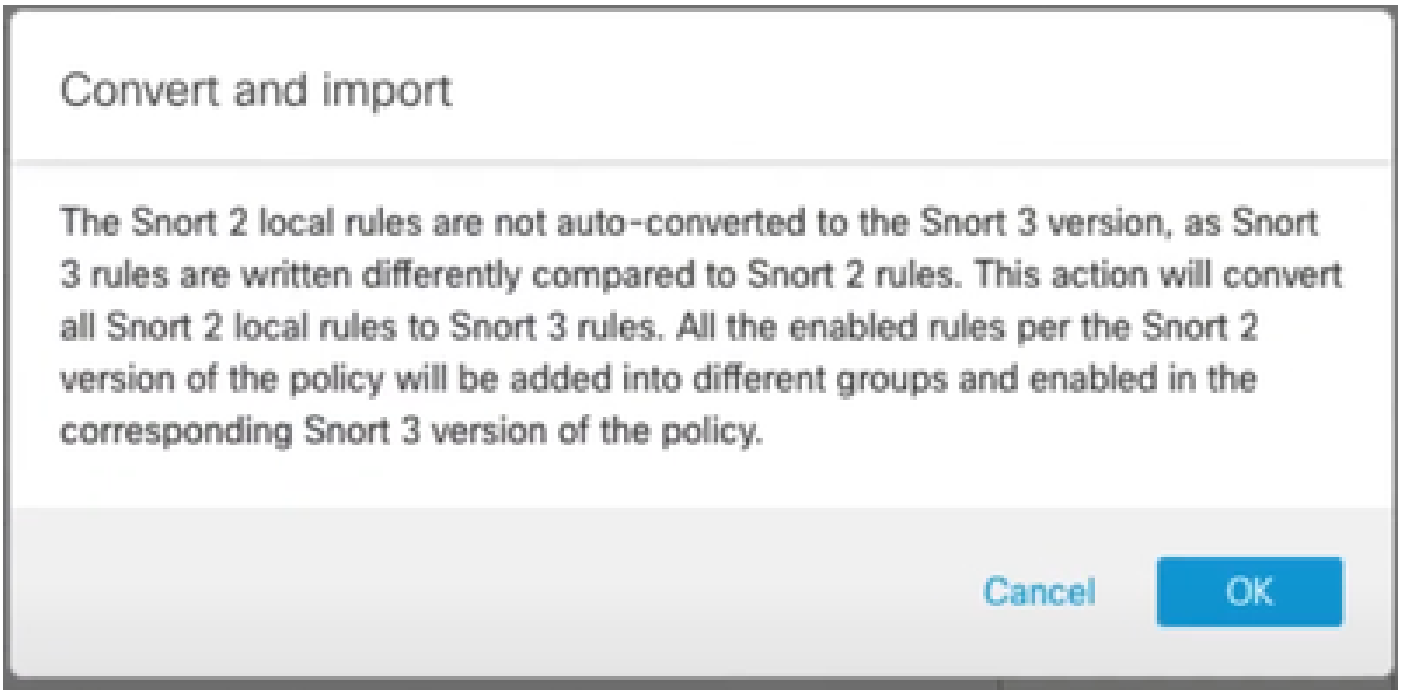
3. انقر فوق علامة التبويب Snort 3 All Rules وتأكد من تحديد جميع القواعد.



4.في القائمة المنسدلة المهمة، حدد تحويل واستيراد.



5. انقر فوق موافق" في رسالة التحذير.

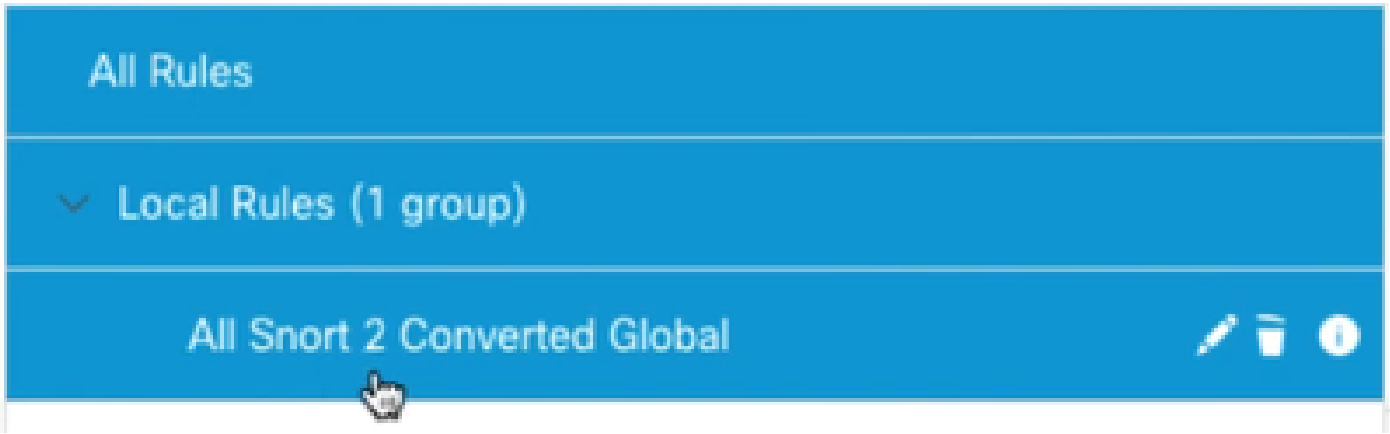


التحقق من الصحة

يظهر قسم محرك التفتيش أن الإصدار الحالي من snort هو snort 3.

تم تحويل القاعدة بنجاح بمجرد رؤية هذه الرسالة:

أخيرا، يجب أن تجد على مجموعة القواعد المحلية قسم كافة Snort 2 Convert Global ، والذي يحتوي على كافة قواعد Snort 2 إلى Snort 3 المحولة.



استكشاف الأخطاء وإصلاحها

في حالة فشل الترحيل أو تعطله، قم بالرجوع إلى إصدار Snort 2 وأعد المحاولة.

معلومات ذات صلة

- كيف تهاجر من نورت 2 إلى نورت 3
- Cisco Secure - ترقية جهاز Snort 3 (فيديو YouTube خارجي)

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).