Mise à niveau de Snort 2 vers Snort 3 via FMC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Mettre à niveau la version Snort
    - Méthode 1
    - Méthode 2
  - Mise à niveau des règles d'intrusion
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment mettre à niveau la version de Snort 2 et de Snort 3 dans Firepower Manager Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Centre de gestion Firepower
- Renifleur

Composants utilisés

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

- FMC 7.0
- DFT 7,0

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.

Informations générales

La fonctionnalité Snort 3 a été ajoutée à la version 6.7 pour Firepower Device Manager (FDM) et Cisco Defense Orchestrator (CDO) ; dans la version 7.0 de Firepower Management Center (FMC).

Snort 3.0 a été conçu pour relever ces défis :

1. Réduisez l'utilisation de la mémoire et du processeur.
2. Améliorer l'efficacité du contrôle HTTP.
3. Chargement plus rapide de la configuration et redémarrage de Snort.
4. Meilleure programmabilité pour un ajout de fonctionnalités plus rapide.

Configurer

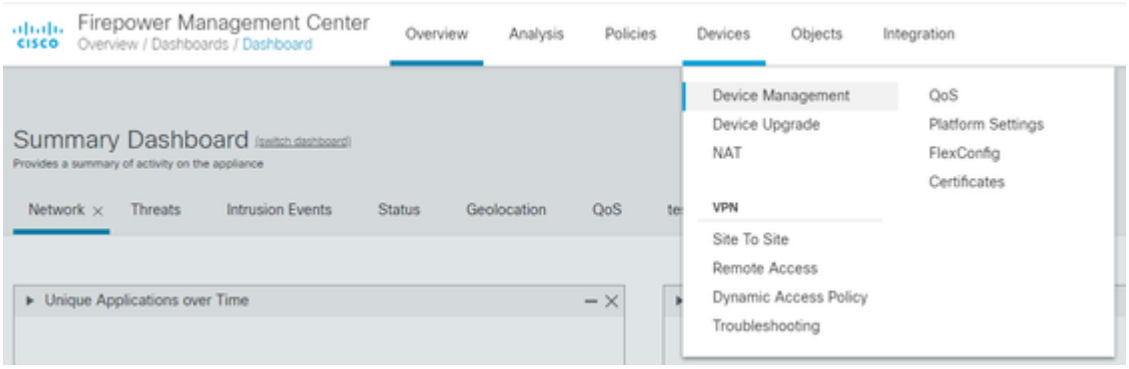
Mettre à niveau la version Snort

Méthode 1

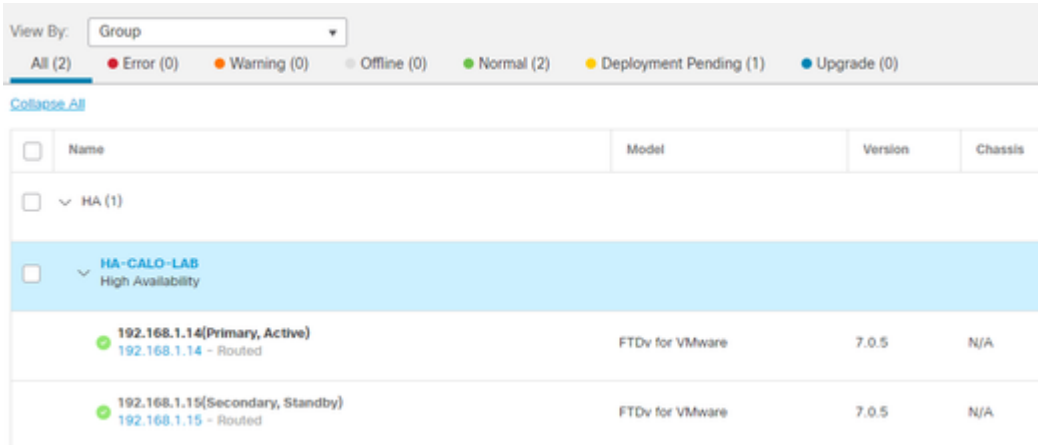
1. Connectez-vous à Firepower Management Center.



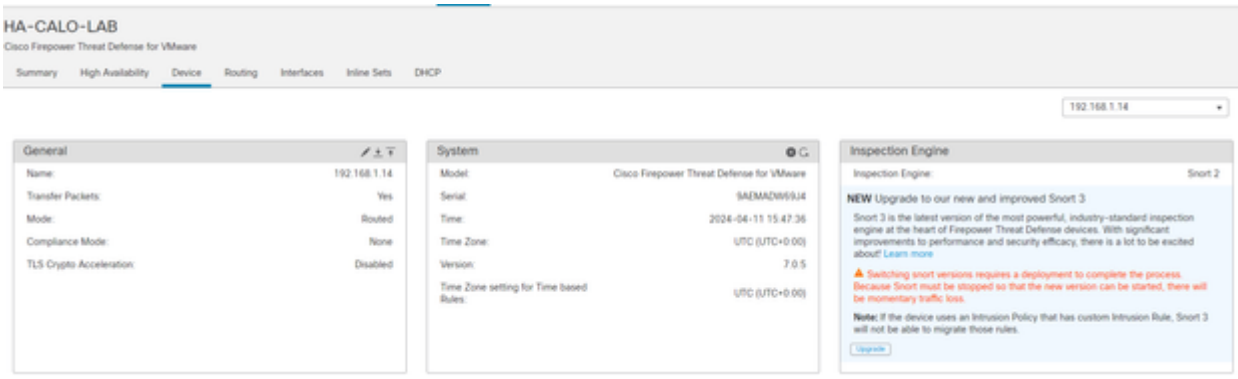
2. Dans l'onglet Périphérique, accédez à Périphériques > Gestionnaire de périphériques.



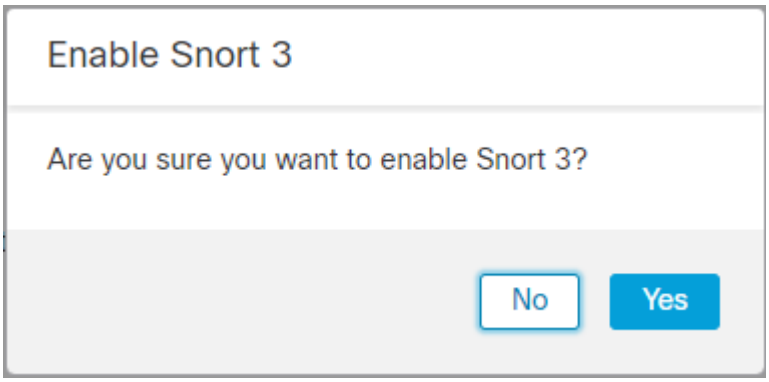
3. Sélectionnez le périphérique que vous souhaitez modifier la version de Snort.



4. Cliquez sur l'onglet Device et cliquez sur le bouton Upgrade dans la section Inspection Engine.



5. Confirmez votre sélection.

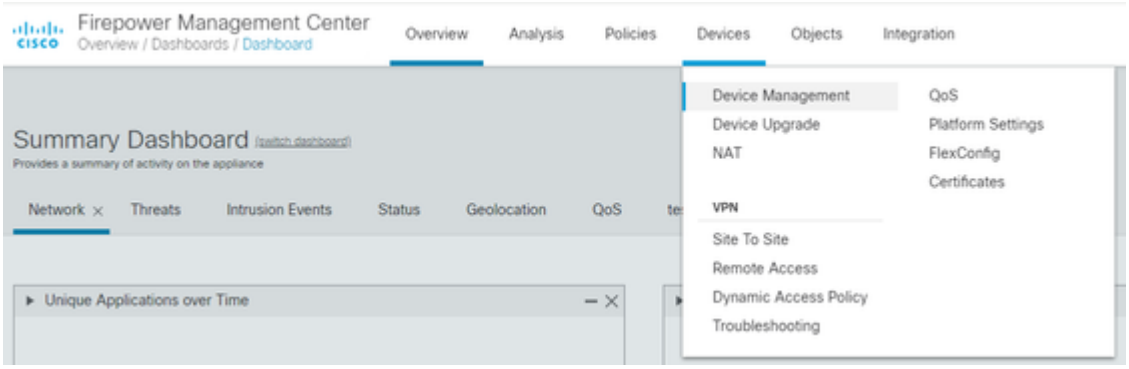


Méthode 2

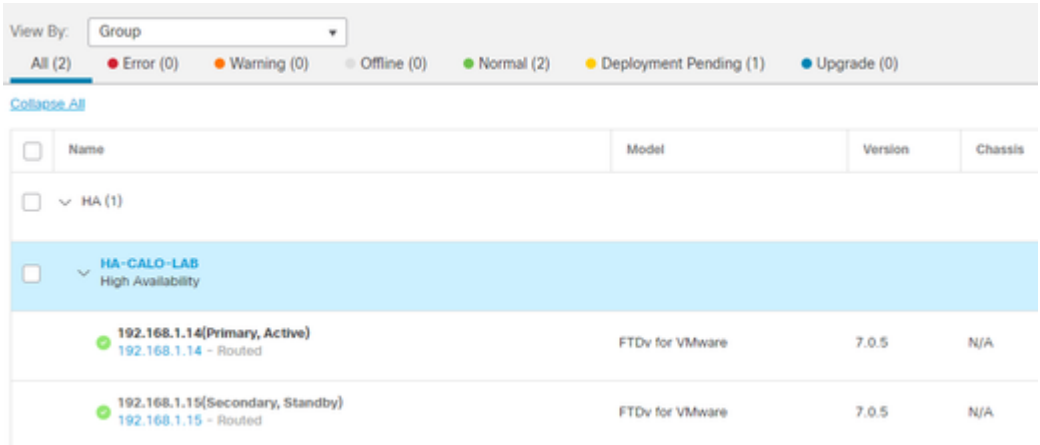
1. Connectez-vous à Firepower Management Center.



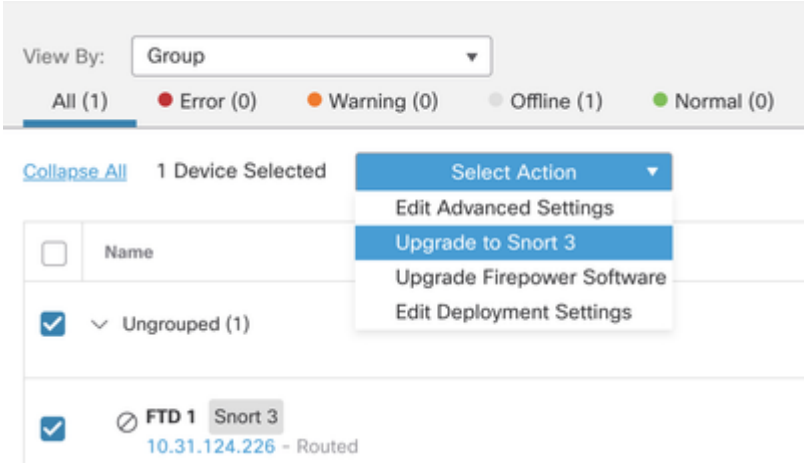
2. Dans l'onglet Périphérique, accédez à Périphériques > Gestionnaire de périphériques.



3. Sélectionnez le périphérique que vous souhaitez modifier la version de Snort.



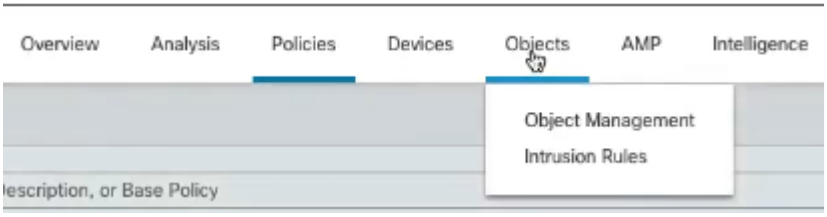
4. Cliquez sur le bouton Select Action et sélectionnez Upgrade to Snort 3.



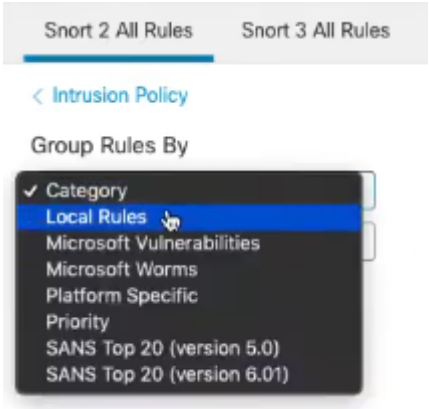
Mise à niveau des règles d'intrusion

En outre, vous devez convertir vos règles Snort 2 en règles Snort 3.

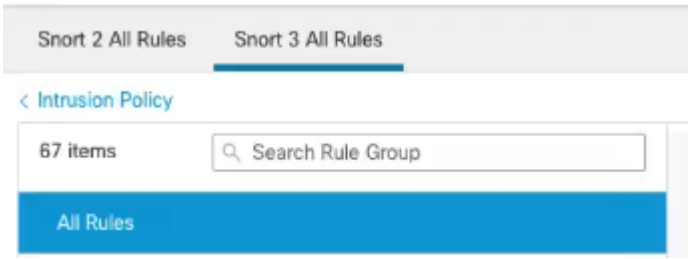
1. Sélectionnez dans le menu Objets > Règles d'intrusion.



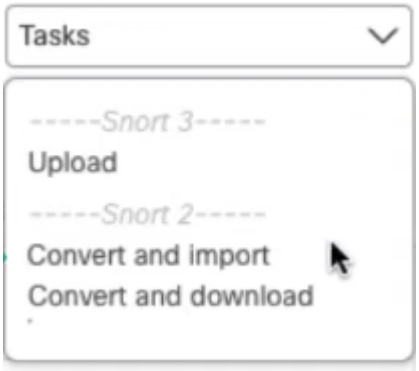
2.Sélectionnez dans le menu Snort 2 All Rules tab > Group Rules By > Local Rules.



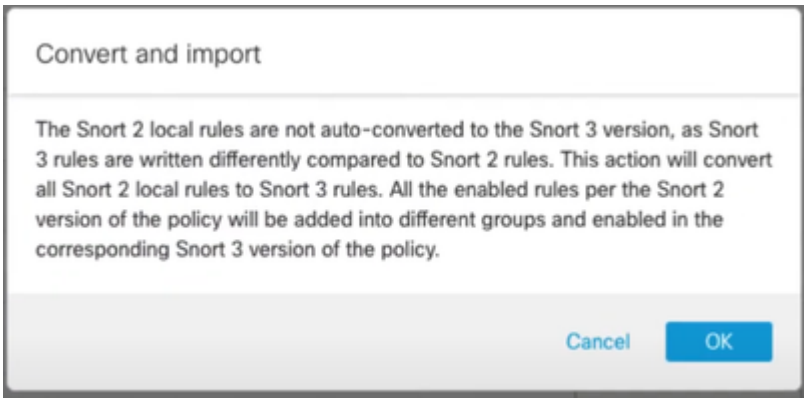
3. Cliquez sur Snort 3 Toutes les règles onglet et assurez-vous que Toutes les règles est sélectionné.



4. Dans le menu déroulant Tâche, sélectionnez Convertir et importer.



5. Cliquez sur OK dans le message d'avertissement.



Vérifier

La section Moteur d'inspection indique que la version actuelle de Snort est Snort 3.



La conversion de la règle a réussi lorsque le message suivant s'affiche :



Enfin, vous devez trouver dans le groupe Règles locales la section All Snort 2 Converted Global , qui contient toutes vos règles converties de Snort 2 à Snort 3.



Dépannage

Si la migration échoue ou tombe en panne, revenez à Snort 2 et réessayez.

Informations connexes

- Comment migrer de Snort 2 vers Snort 3
- Cisco Secure - Mise à niveau du périphérique Snort 3 (vidéo YouTube externe)

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.

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.