Mise à niveau de Snort 2 vers Snort 3 via FDM

Table des matières

Introduction

Ce document décrit comment mettre à niveau la version de Snort 2 vers Snort 3 dans Firepower Device Manager (FDM).

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Gestionnaire de périphériques Firepower (FDM)
- Renifleur .

Exigences

Assurez-vous que vous disposez des conditions suivantes :

- Accès au Gestionnaire de périphériques Firepower.
- Privilèges d'administration sur le FDM.
- FTD doit être au moins la version 6.7 pour pouvoir utiliser snort 3.

Composants utilisés

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

- DFT 7.2.7

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

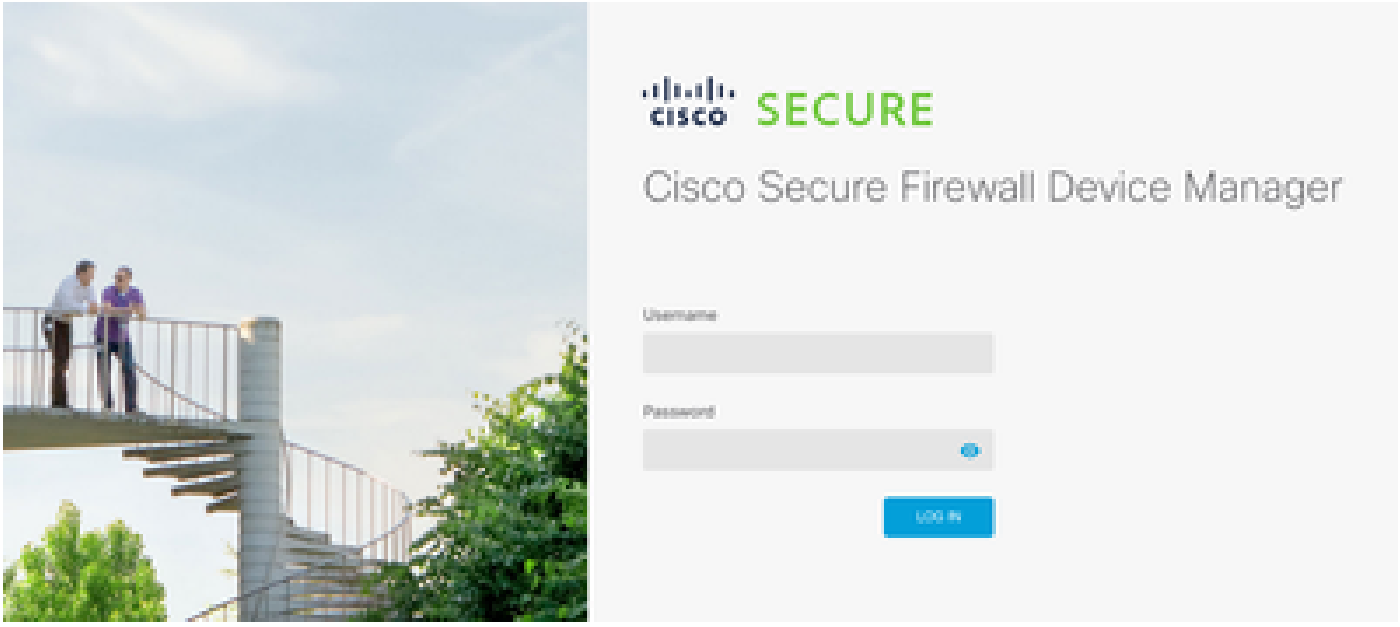
La fonctionnalité snort 3 a été ajoutée dans la version 6.7 de Firepower Device Manager (FDM). Snort 3.0 a été conçu pour relever ces défis :

- Réduisez l'utilisation de la mémoire et du processeur.
- Améliorer l'efficacité du contrôle HTTP.
- Chargement plus rapide de la configuration et redémarrage du sniffeur.
- Meilleure programmabilité pour un ajout de fonctionnalités plus rapide.

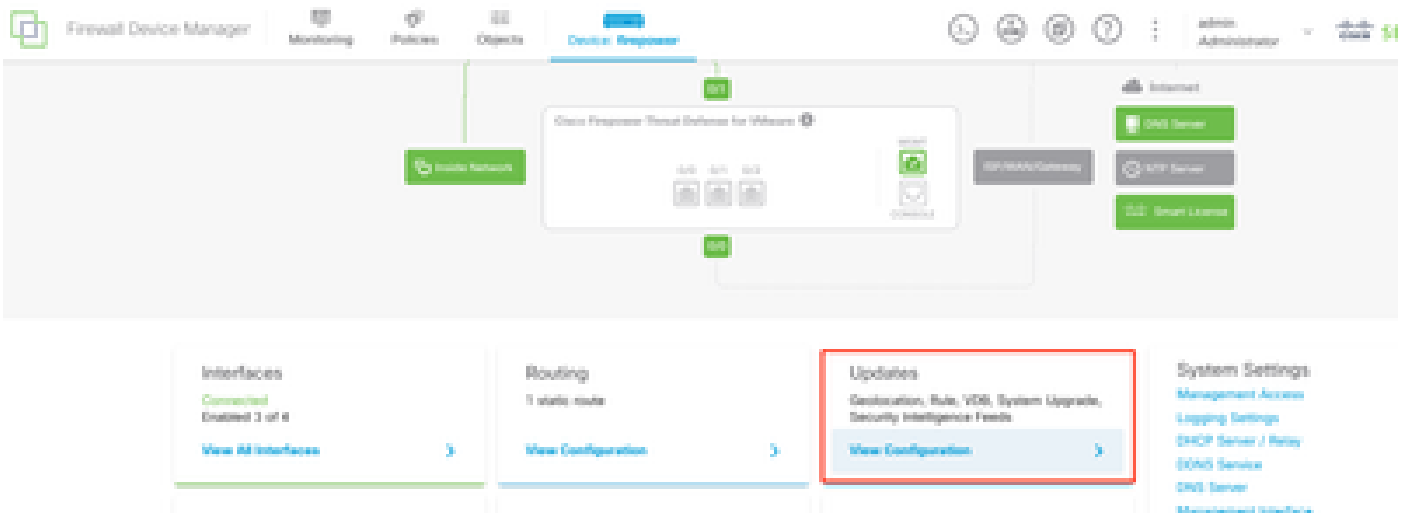
Configurer

Configurations

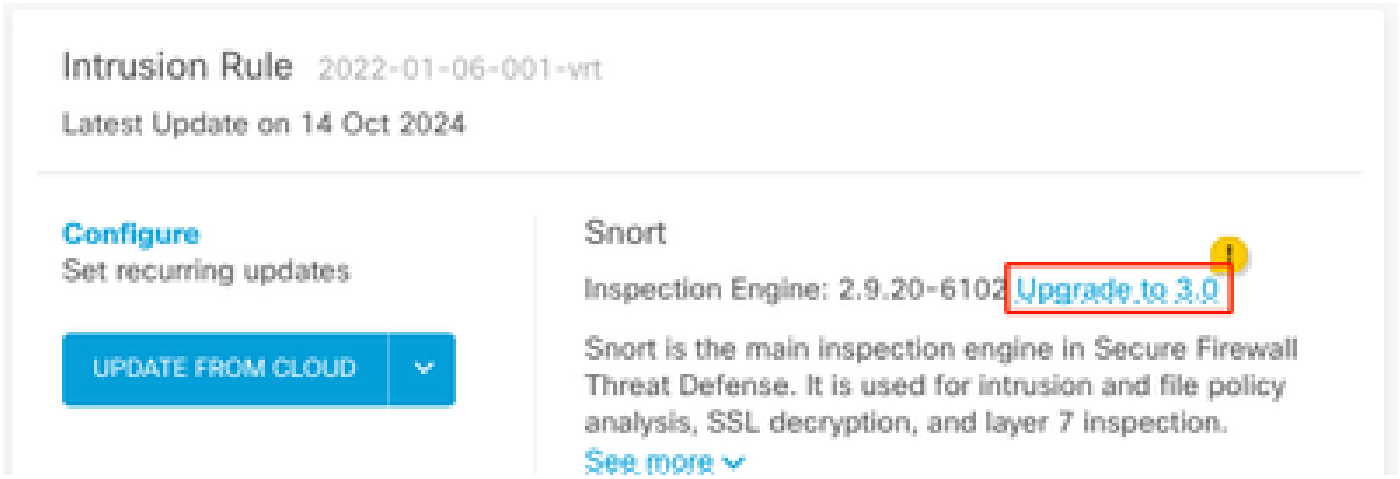
1. Connectez-vous au Gestionnaire de périphériques Firepower.



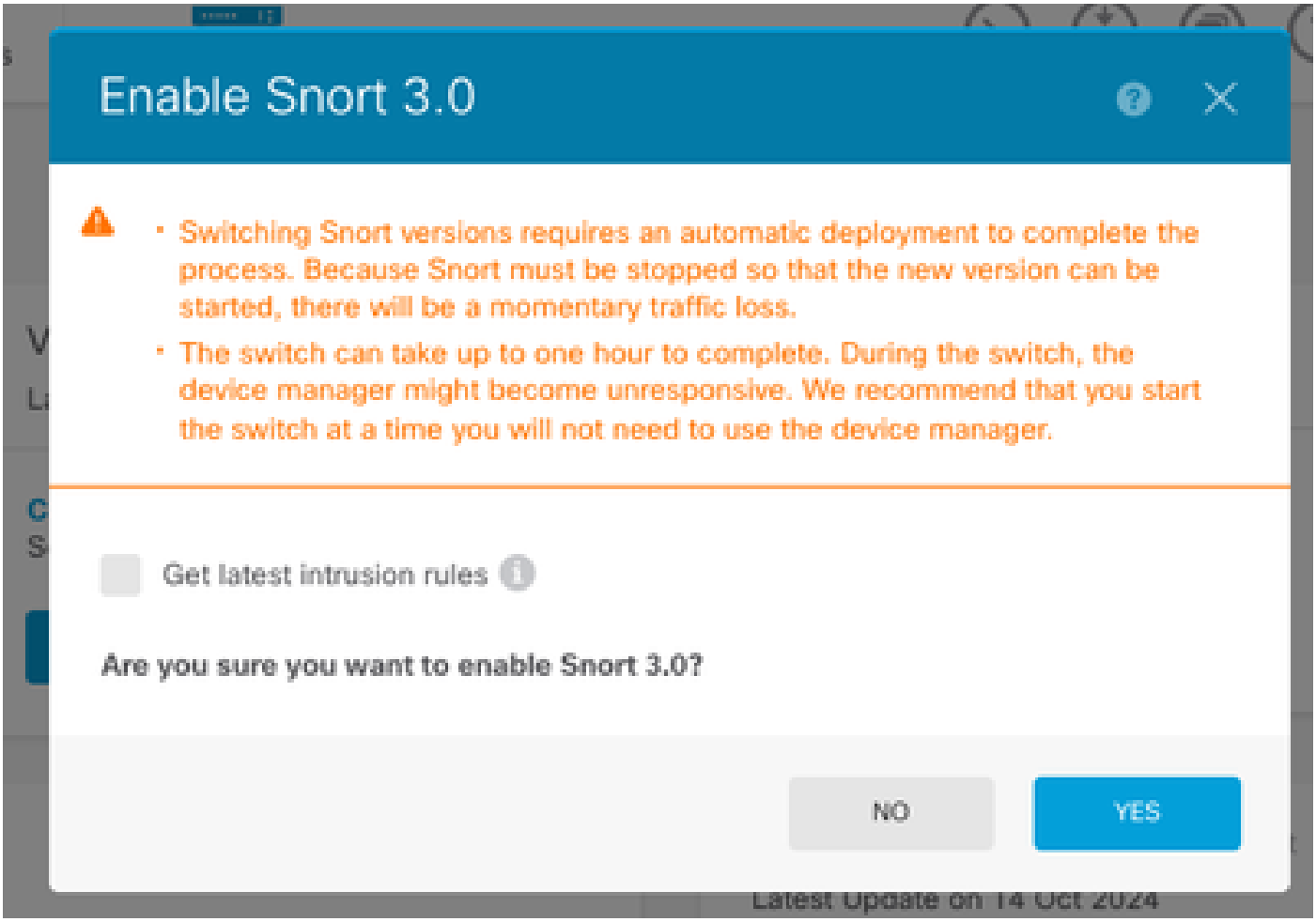
2. Accédez à Device > Updates > View configuration.

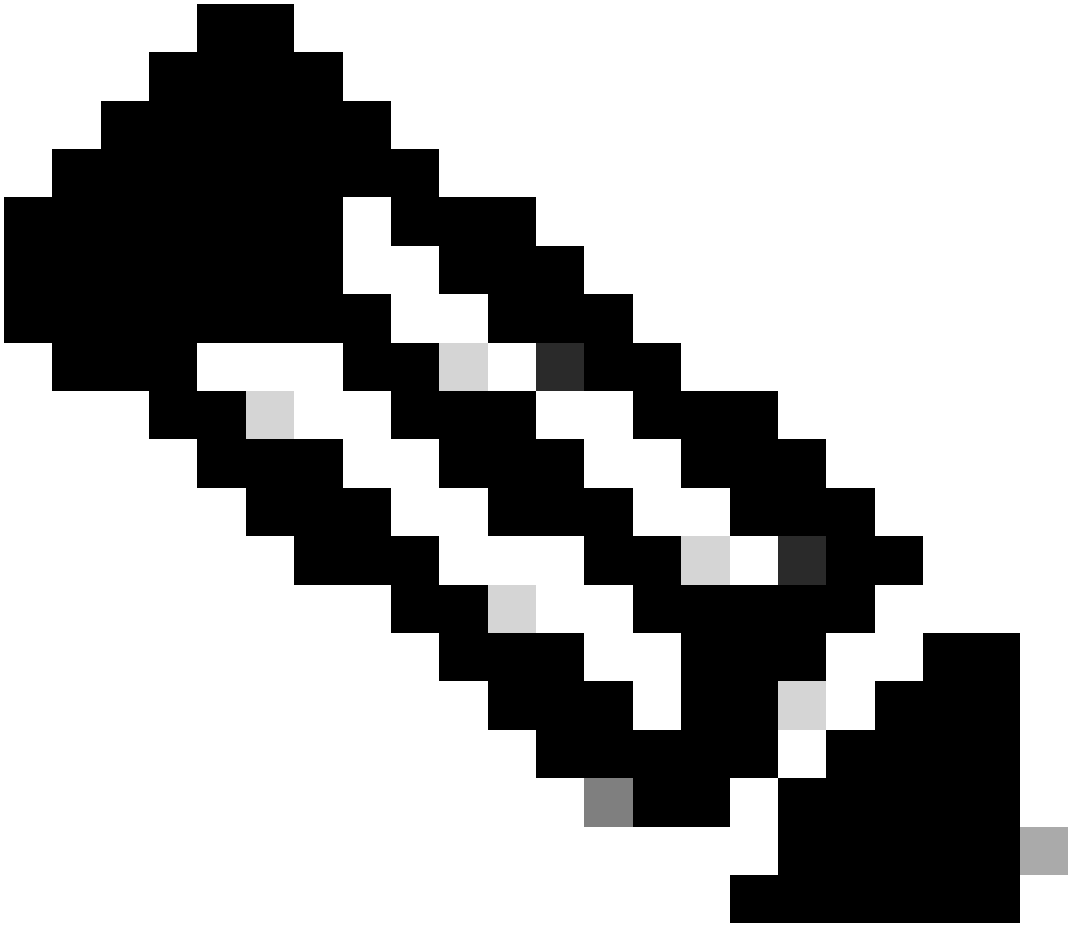


3. Dans la section des règles d'intrusion, cliquez sur upgrade to snort 3.

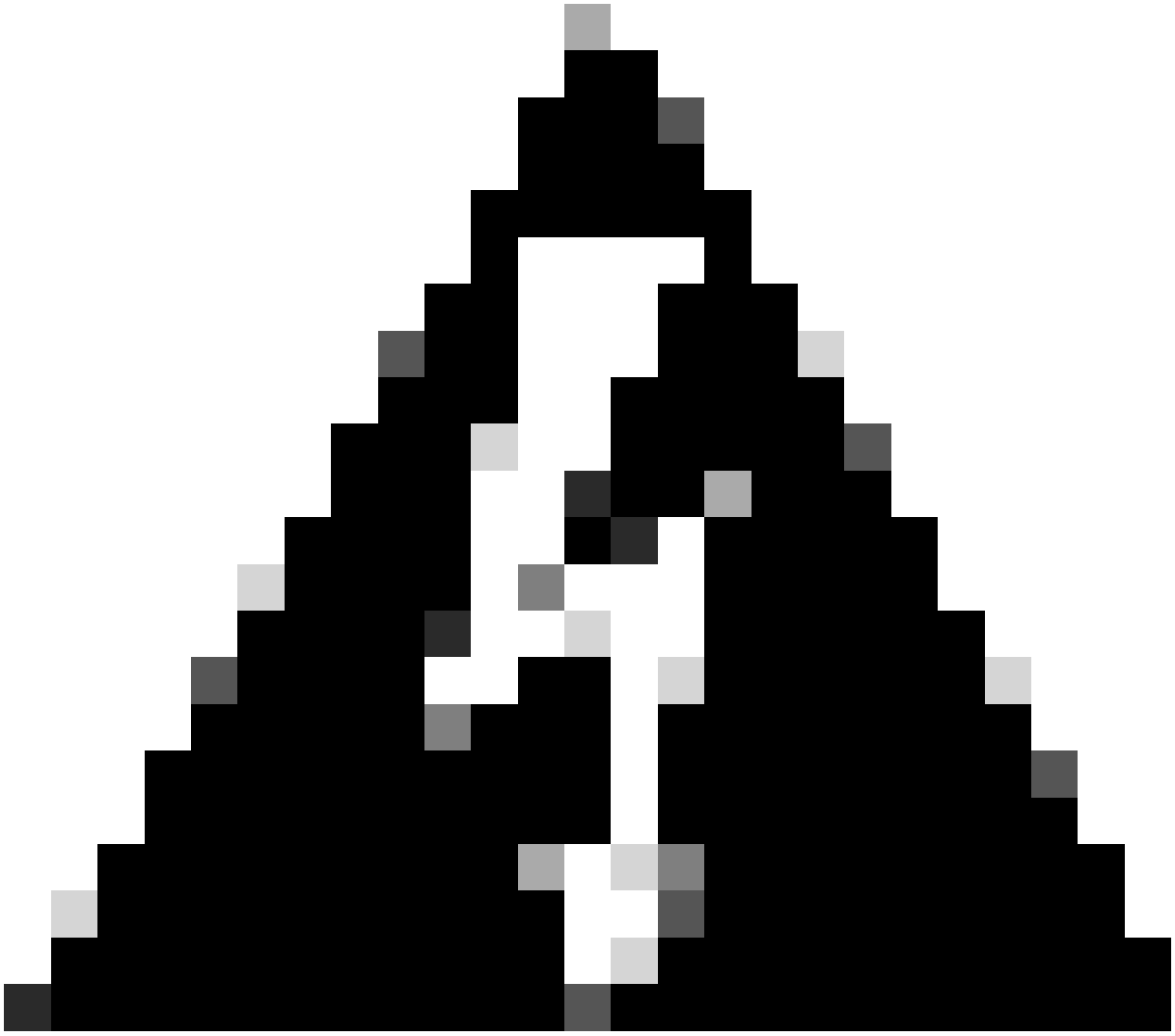


4. Dans le message d'avertissement pour confirmer votre sélection, sélectionnez l'option permettant d'obtenir le dernier package de règles d'intrusion, puis cliquez sur Oui.


Enable Snort 3.0
Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive. We recommend that you start the switch at a time you will not need to use the device manager.
Get latest intrusion rules
Are you sure you want to enable Snort 3.0?
NO
YES
Latest Update on 14 Oct 2024

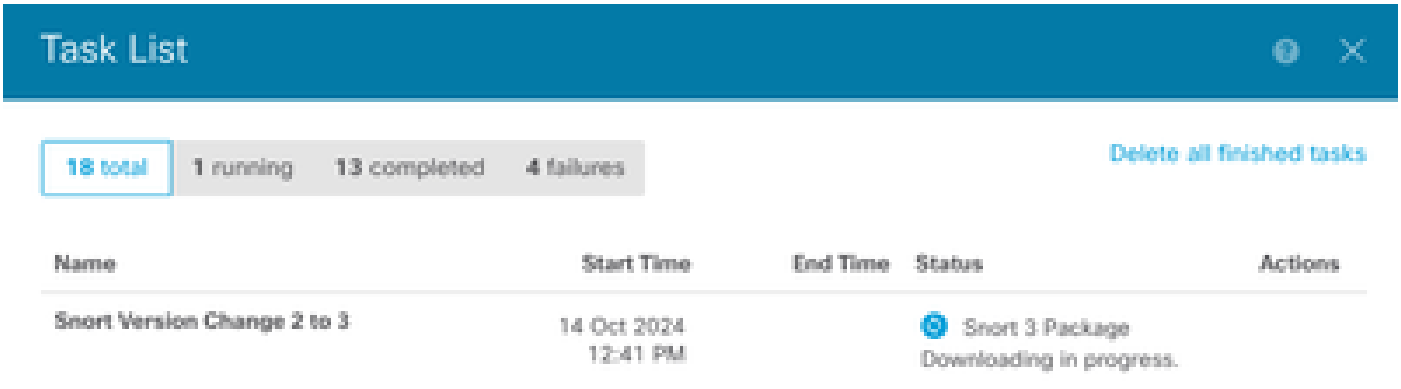


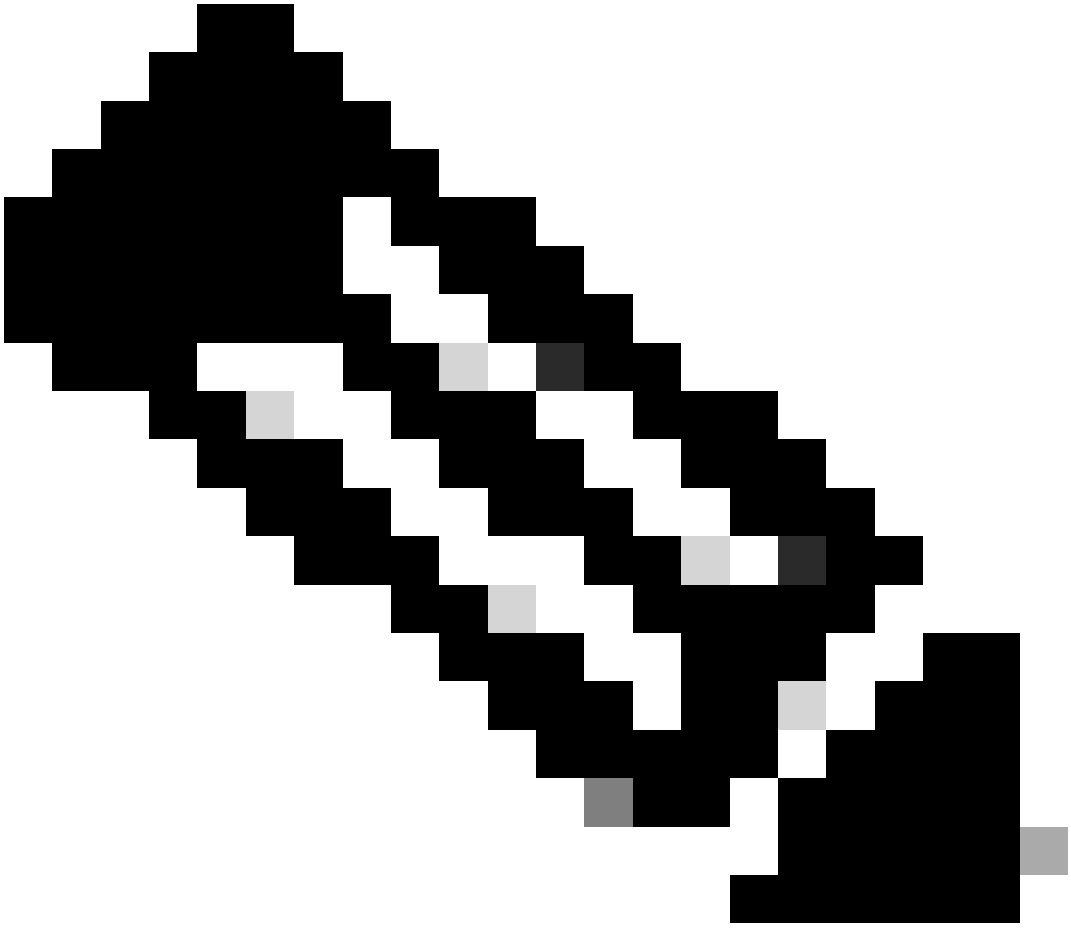
Remarque : le système télécharge uniquement les paquets de la version active de Snort. Il est donc peu probable que le dernier paquet soit installé pour la version de Snort vers laquelle vous basculez. Vous devez attendre la fin de la tâche de changement de version avant de pouvoir modifier les stratégies d'intrusion.



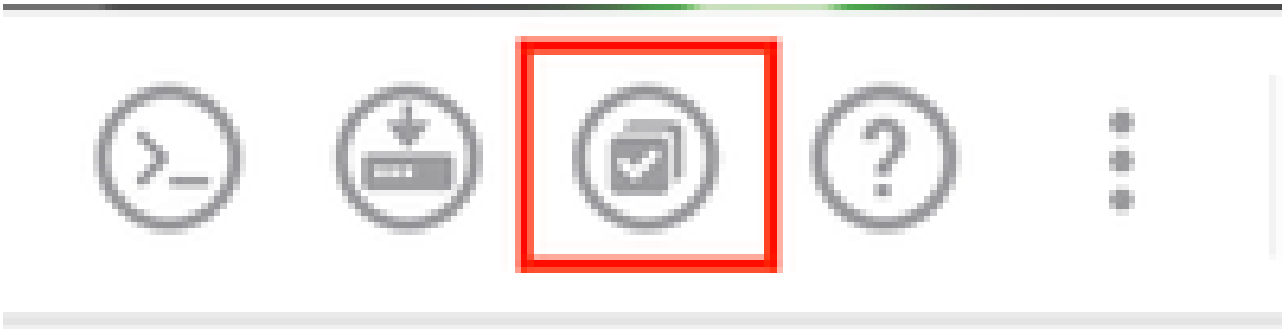
Avertissement : la commutation de la version Snort entraîne une perte de trafic momentanée.

5. Vous devez confirmer dans la liste des tâches que la mise à niveau a démarré.



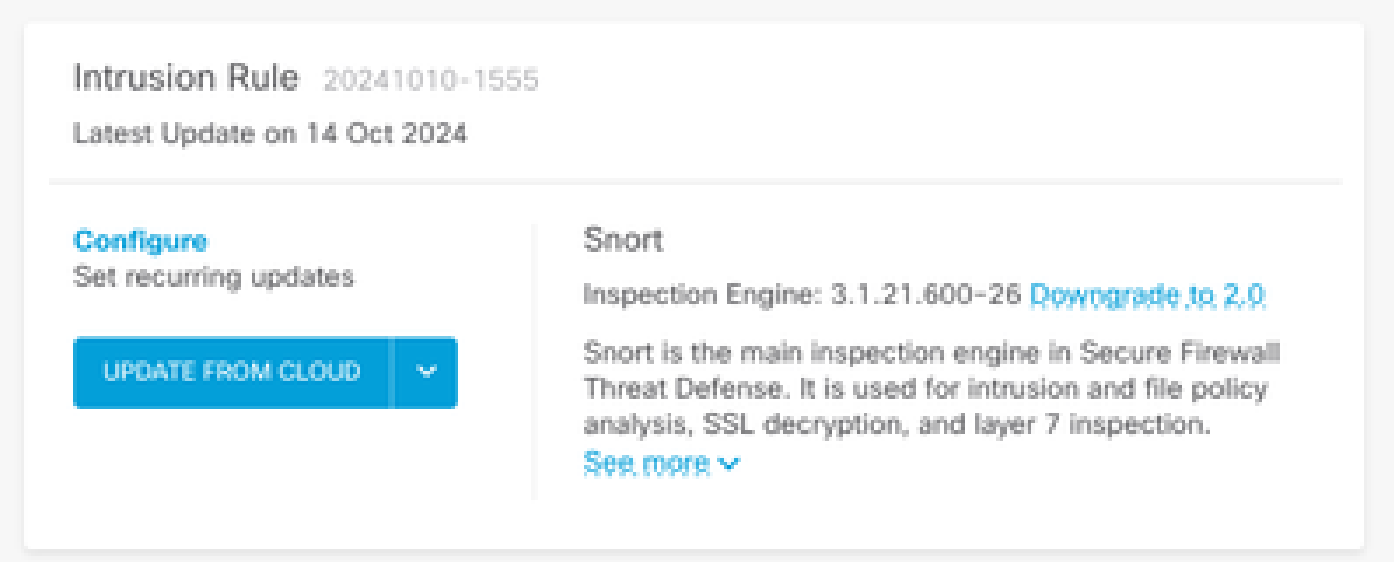


Remarque : la liste des tâches se trouve dans la barre de navigation en regard de l'icône des déploiements.

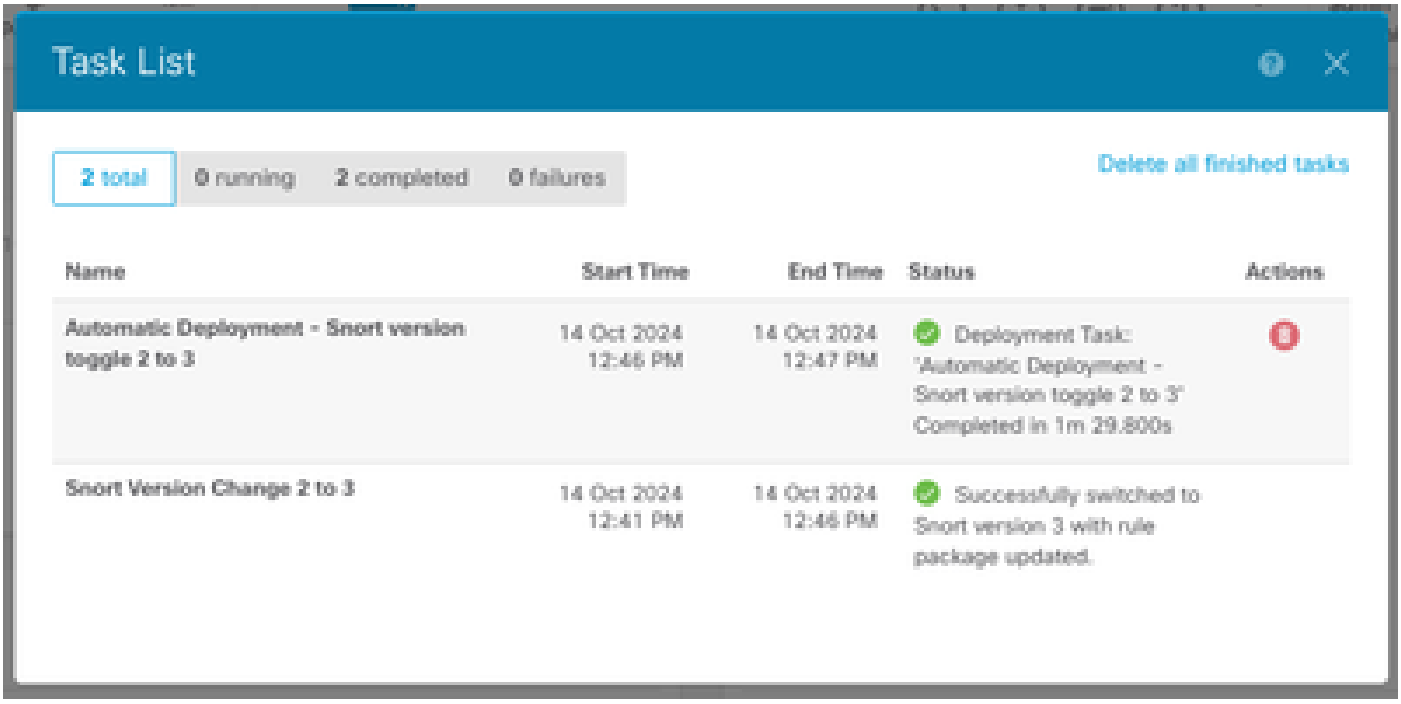


Vérifier

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



Enfin, dans la liste des tâches, assurez-vous que la modification de Snort 3 a été correctement effectuée et déployée.



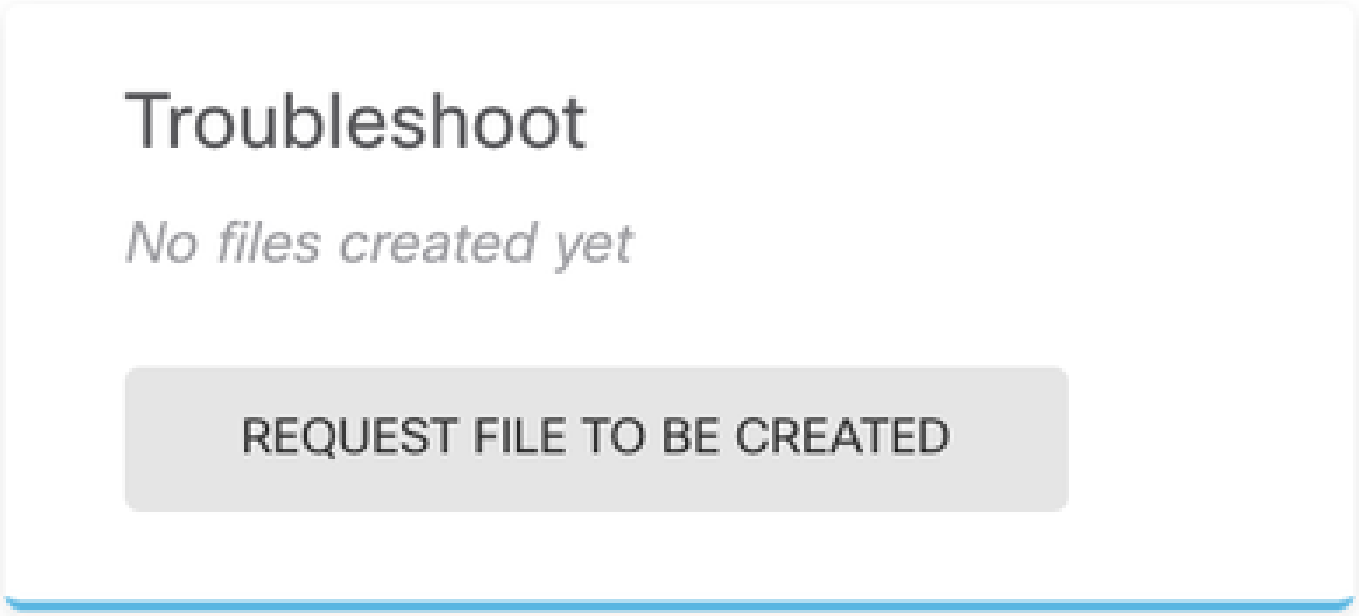
Dépannage

Si vous rencontrez des problèmes lors de la mise à niveau, procédez comme suit :

- Assurez-vous que vos versions FTD sont compatibles avec Snort 3.

Pour plus d'informations, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense

- Collectez les fichiers de dépannage sur le FDM en naviguant vers l'onglet Device, puis en cliquant sur Request file to be create. Une fois la collecte effectuée, ouvrez un dossier auprès du centre d'assistance technique et téléchargez le fichier dans le dossier pour obtenir de l'aide.



Informations connexes

- Adoption de Snort 3
- Snort Documents
- Guide de configuration de Cisco Secure Firewall Device Manager, version 7.2

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.