Déterminez la version active de Snort qui s'exécute sur FTD

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Déterminez la version active du sniffeur qui s'exécute sur le FTD

- Interface de ligne de commande (CLI) FTD
- FTD géré par Cisco FDM
- FTD géré par Cisco FMC
- FTD géré par Cisco CDO

Informations connexes

Introduction

Ce document décrit les étapes pour confirmer la version active de snort qu'un FTD Cisco exécute lorsqu'il est géré par le FDM Cisco, le FMC Cisco ou le CDO.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Gestionnaire de périphériques Cisco Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

Composants utilisés

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

- Cisco Firepower Threat Defense v6.7.0 et 7.0.0
- Cisco Firepower Management Center v6.7.0 et 7.0.0
- Cisco Defense Orchestrator

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

Le système de prévention des intrusions SNORT® a officiellement lancé Snort 3, une mise à niveau complète qui propose des améliorations et de nouvelles fonctionnalités qui améliorent les performances, un traitement plus rapide, une évolutivité améliorée pour votre réseau, et une gamme de plus de 200 plugins afin que vous puissiez créer une configuration personnalisée pour votre réseau.

Les avantages de Snort 3 incluent, sans s'y limiter :

- Performances améliorées
- Inspection SMBv2 améliorée
- Nouvelles fonctionnalités de détection de script
- Inspection HTTP/2
- Groupes de règles personnalisés
- Syntaxe qui facilite l'écriture des règles d'intrusion personnalisées.
- Les raisons pour lesquelles il aurait été abandonné en ligne entraînent des événements d'intrusion.
- No Snort redémarre lorsque des modifications sont déployées sur la VDB, les stratégies SSL, les détecteurs d'applications personnalisés, les sources d'identité de portail captif et la découverte d'identité de serveur TLS.
- Facilité de maintenance améliorée grâce aux données de télémétrie spécifiques à Snort 3 envoyées à Cisco Success Network et à de meilleurs journaux de dépannage.

La prise en charge de Snort 3.0 a été introduite pour la version 6.7.0 de Cisco Firepower Threat Defense (FTD), juste au moment où le FTD est géré via Cisco Firepower Device Manager (FDM).

Remarque : Pour les nouveaux déploiements FTD 6.7.0 gérés par FDM, Snort 3.0 est le moteur d'inspection par défaut. Si vous mettez à niveau le FTD vers 6.7 à partir d'une version plus ancienne, alors Snort 2.0 reste le moteur d'inspection actif, mais vous pouvez passer à Snort 3.0.

Remarque : Pour cette version, Snort 3.0 ne prend pas en charge les routeurs virtuels, les règles de contrôle d'accès basées sur le temps ou le déchiffrement des connexions TLS 1.1 ou inférieures. Activez Snort 3.0 uniquement si vous n'avez pas besoin de ces fonctionnalités.

Ensuite, la version 7.0 de Firepower a introduit la prise en charge de Snort 3.0 pour les périphériques Firepower Threat Defense gérés par les deux ; le Cisco FDM et le Cisco Firepower Management Center (FMC).

Remarque : Pour les nouveaux déploiements FTD 7.0, Snort 3 est désormais le moteur d'inspection par défaut. Les déploiements mis à niveau continuent d'utiliser Snort 2, mais vous pouvez basculer à tout moment.

Mise en garde : Vous pouvez basculer librement d'avant en arrière entre Snort 2.0 et 3.0, de sorte que vous pouvez revenir à votre modification si nécessaire. Le trafic est interrompu chaque fois que vous changez de version.

Mise en garde : Avant de passer à Snort 3, il est fortement recommandé de lire et de comprendre le Guide de configuration de Snort 3 de Firepower Management Center. Soyez particulièrement attentif aux limitations des fonctionnalités et aux instructions de migration. Bien que la mise à niveau vers Snort 3 soit conçue pour un impact minimal, les fonctionnalités ne correspondent pas exactement. Le plan et la préparation avant la mise à niveau peuvent vous aider à vous assurer que le trafic est traité comme prévu.

Déterminez la version active du sniffeur qui s'exécute sur le FTD

Interface de ligne de commande (CLI) FTD

Afin de déterminer la version de snort active qui s'exécute sur un FTD, connectez-vous à l'ILC FTD et exécutez la commande show snort3 status :

Exemple 1 : Lorsqu'aucune sortie n'est affichée, le FTD exécute Snort 2.

```
<#root>

>

show snort3 status

>
```

Exemple 2 : Lorsque le résultat indique « Snort 2 en cours d'exécution », le FTD exécute « Snort 2 ».

```
<#root>

>

show snort3 status
```

```
Currently running Snort 2
```

Exemple 3 : Lorsque le résultat indique « Snort 3 en cours d'exécution », le FTD exécute « Snort 3 ».

```
<#root>

>

show snort3 status

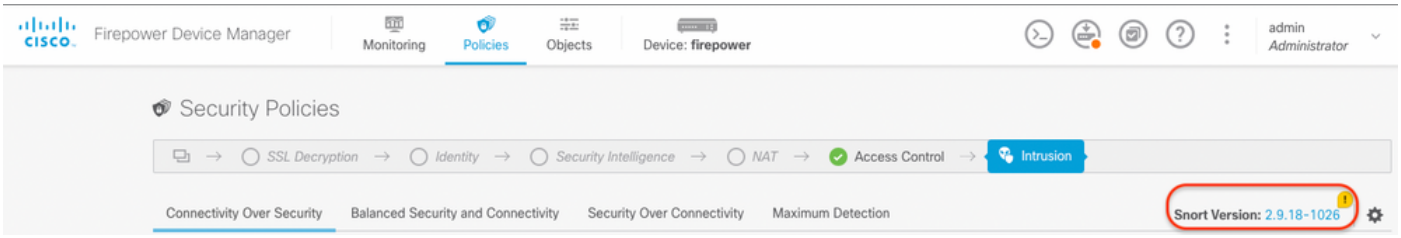
Currently running Snort 3
```

FTD géré par Cisco FDM

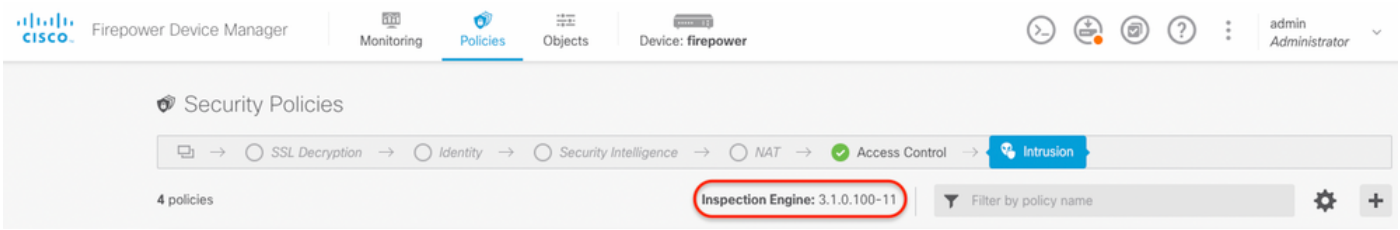
Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco FDM, passez aux étapes suivantes :

1. Connectez-vous au FTD Cisco via l'interface Web FDM.
2. Dans le menu principal, sélectionnez Politiques.
3. Sélectionnez ensuite l'onglet Intrusion.
4. Recherchez la section Snort Version ou Inspection Engine pour confirmer la version de Snort qui est active dans le FTD.

Exemple 1 : Le FTD exécute snort version 2.



Exemple 2 : Le FTD exécute snort version 3.

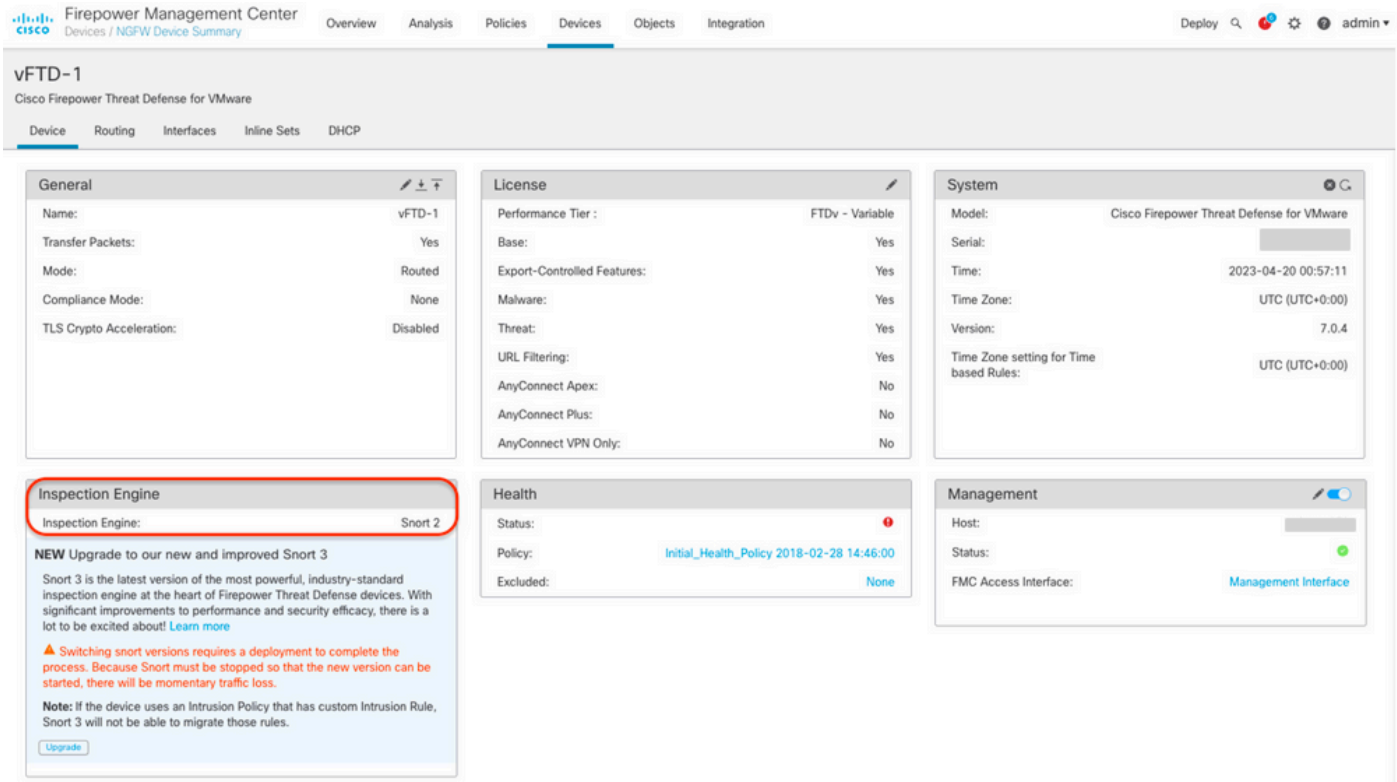


FTD géré par le Cisco FMC

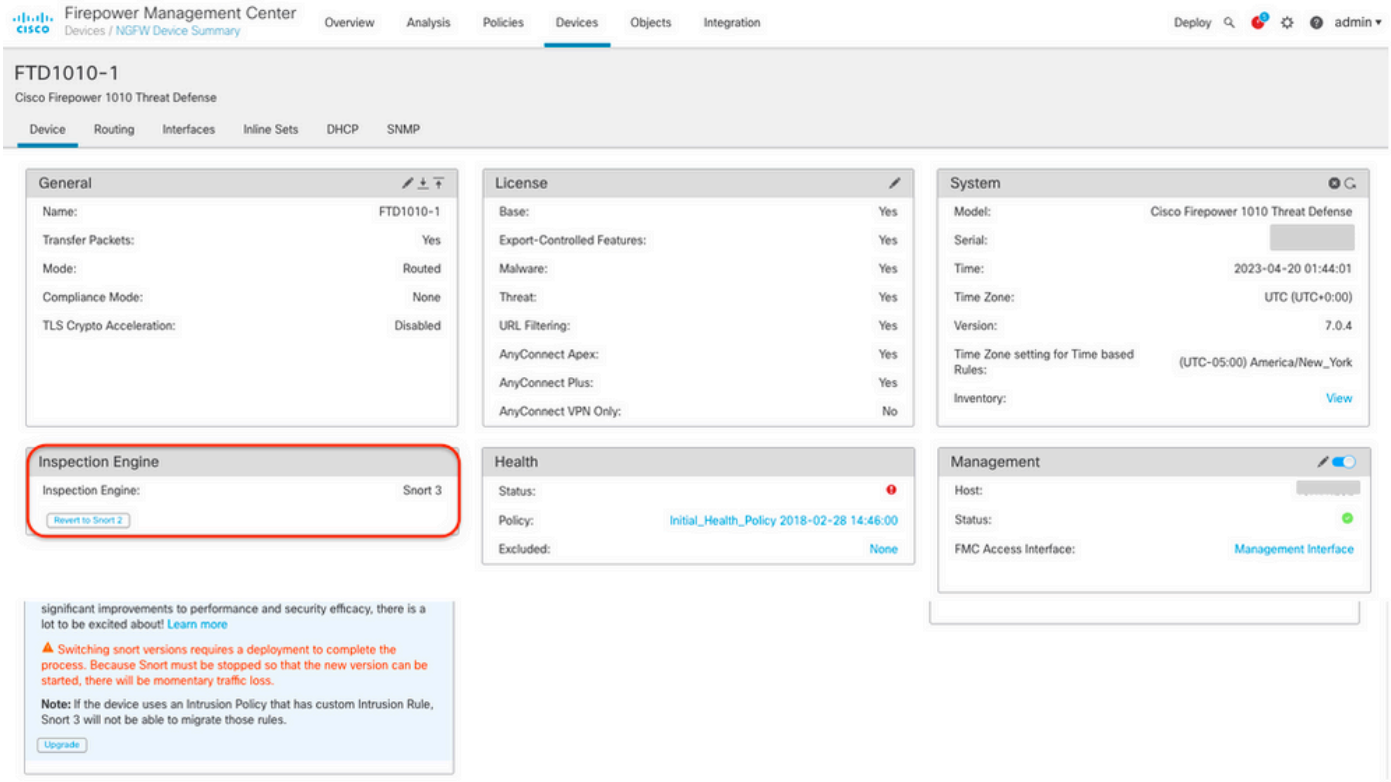
Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco FMC, passez aux étapes suivantes :

1. Connectez-vous à l'interface Web de Cisco FMC.
2. Dans le menu Périphériques, sélectionnez Gestion des périphériques.
3. Sélectionnez ensuite le périphérique FTD approprié.
4. Cliquez sur l'icône Modifier le crayon.
5. Sélectionnez l'onglet Device et recherchez la section Inspection Engine pour confirmer la version de snort qui est active dans le FTD :

Exemple 1 : Le FTD exécute snort version 2.



Exemple 2 : Le FTD exécute snort version 3.

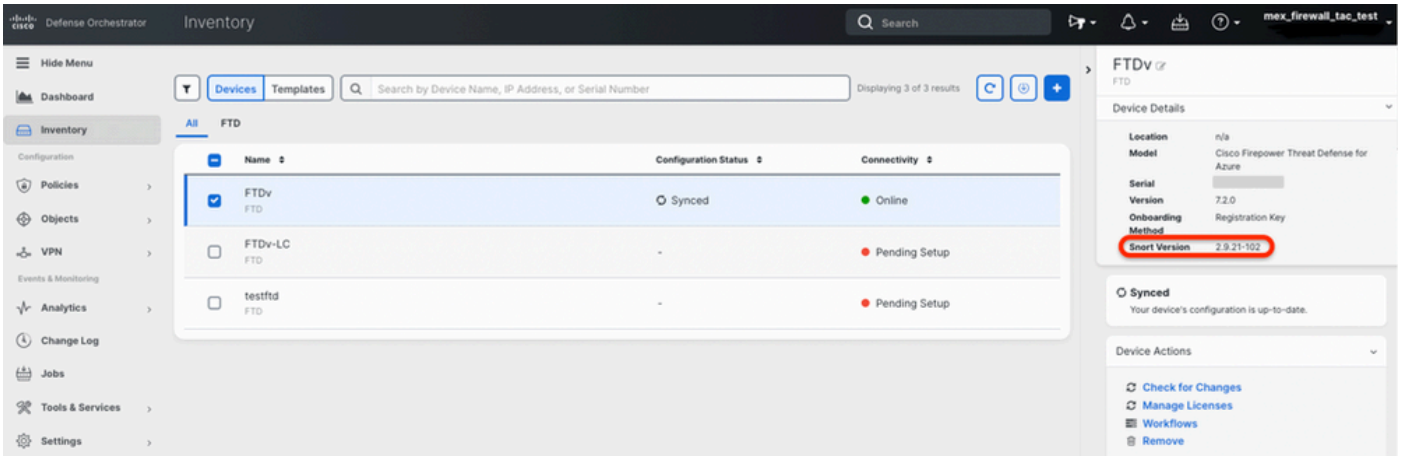


FTD géré par le Cisco CDO

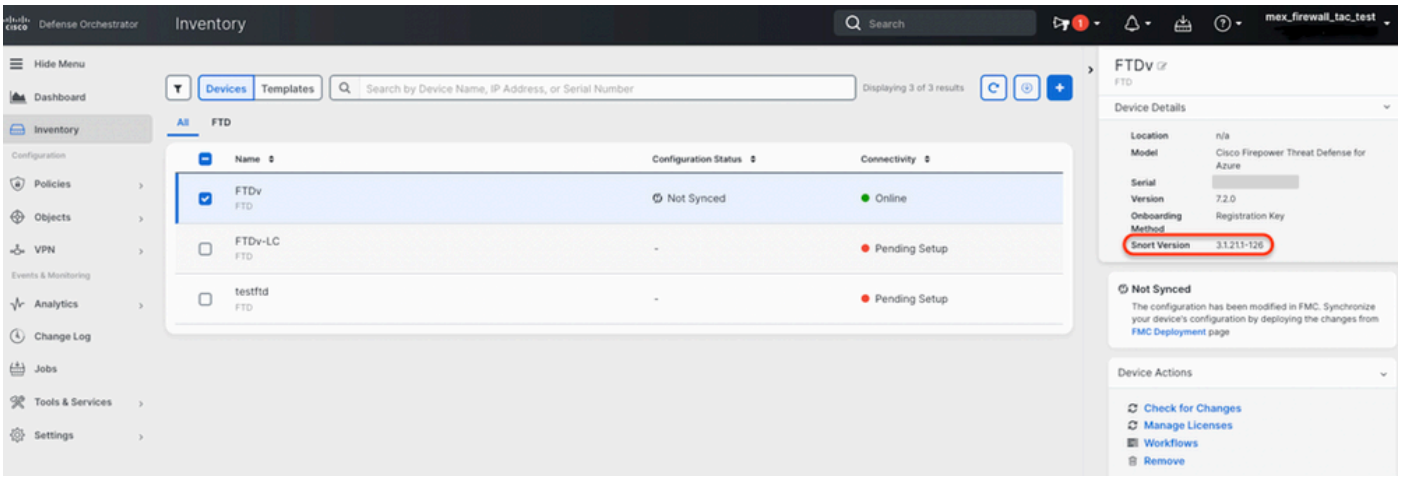
Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco Defense Orchestrator, passez aux étapes suivantes :

1. Connectez-vous à l'interface Web de Cisco Defense Orchestrator.
2. Dans le menu Inventaire, sélectionnez le périphérique FTD approprié.
3. Dans la section Device Details, recherchez Snort Version :

Exemple 1 : Le FTD exécute snort version 2.



Exemple 2 : Le FTD exécute snort version 3.



Informations connexes

- Notes de version de Cisco Firepower, version 6.7.0
- Notes de version de Cisco Firepower, version 7.0
- Site Web Snort 3
- Assistance et documentation techniques - Cisco Systems

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.