# 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
<u>Dépannage</u>
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
- 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 dans la version 6.7 pour Firepower Device Manager (FDM) et Cisco Defense Orchestrator (CDO) ; dans la version 7.0 pour 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.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devi	ces Objects	Integration
Summary Dashboard (setter dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Ge	eolocation	QoS	De De NJ e: VP	vice Management vice Upgrade N	QoS Platform Settings FlexConfig Certificates
<ul> <li>Unique Applications over Time</li> </ul>			- ×	Si Re Dy Tr	e To Site mote Access namic Access Policy publeshooting	

3. Sélectionnez le périphérique dont vous souhaitez modifier la version Snort.

View By:	Group	•				
All (2)	Error (0)     Warning (0)	<ul> <li>Offline (0)</li> </ul>	Normal (2)	Deployment Pending (1)	Upgrade (0)	
Collapse All						
Na	me			Model	Version	Chassis
	IA (1)					
• •	HA-CALO-LAB High Availability					
	92.168.1.14(Primary, Active) 192.168.1.14 - Routed			FTDv for VMware	7.0.5	N/A
	2 192.168.1.15(Secondary, Stand 192.168.1.15 - Routed	iby)		FTDv for VMware	7.0.5	N/A.

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

IA-CALO-LAB sco Frepower Threat Defense for VMware Summary High Availability Device 1	Routing Interfaces Inline Sets D	HCP			
				192.168.1.1	14 ·
General	/±∓	System	<b>e</b> G	Inspection Engine	
Name:	192.168.1.14	Model:	Cisco Firepower Threat Defense for VMware	Inspection Engine:	Snort 2
Transfer Packets:	Yes	Serial.	SAEMADW9934	NEW Upgrade to our new and improved Snort 3	
Mode:	Routed	Time.	2024-04-11 15:47:36	Snort 3 is the latest version of the most powerful, industry-sta	indard inspection
Compliance Mode:	None	Time Zone:	UTC (UTC+0.00)	engine at the neart of Prepower Inneat Determs devices, with improvements to performance and security efficacy, there is a	lot to be excited
TLS Crypto Acceleration:	Disabled	Version:	7.0.5	about Learn more	
		Time Zone setting for Time based Rules.	UTC (UTC+0.00)	Because Snort must be stopped so that the new version can b be momentary traffic loss.	te started, there will
				Note: If the device uses an Intrusion Policy that has custom int will not be able to migrate those rules.	trusion Rule, Snort 3
				Uppede	

5. Confirmez votre sélection.



Méthode 2

1. Connectez-vous à Firepower Management Center.

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

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration
Summary Dashboard (setter destinant) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Ge	olocation	QoS 1	Device Device NAT e: VPN	Management Upgrade	QoS Platform Settings FlexConfig Certificates
<ul> <li>Unique Applications over Time</li> </ul>			- ×	Site To Remot Dynam Trouble	Site e Access ic Access Policy eshooting	

3. Sélectionnez le périphérique dont vous souhaitez modifier la version Snort.

View By:	Group	*				
All (2)	Error (0)     Warning (0)	<ul> <li>Offline (0)</li> </ul>	Normal (2)	Deployment Pending (1)	<ul> <li>Upgrade (0)</li> </ul>	
Collapse All						
Na	me			Model	Version	Chassis
	IA (1)					
• •	HA-CALO-LAB High Availability					
	192.168.1.14(Primary, Active) 192.168.1.14 - Routed			FTDv for VMware	7.0.5	N/A
	2 192.168.1.15(Secondary, Stand 192.168.1.15 - Routed	by)		FTDv for VMware	7.0.5	N/A

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.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
lescription, or l	Base Policy			Object M Intrusion	lanagement Rules	

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.

Snort 2 All Rules	Snort 3 All Rules
< Intrusion Policy	
67 items	Q Search Rule Group
All Rules	

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



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

Convert and import
The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.
Cancel OK

### 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

- <u>Comment migrer de Snort 2 vers Snort 3</u>
- 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.