# Aggiornamento da Snort 2 a Snort 3 tramite FMC

# Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Aggiorna la versione Snort
Metodo 1
Metodo 2
Aggiornamento delle regole di intrusione
<u>Verifica</u>
Risoluzione dei problemi
Informazioni correlate

# Introduzione

In questo documento viene descritto come eseguire l'aggiornamento dalle versioni Snort 2 e Snort 3 in Firepower Manager Center (FMC).

### Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense
- Firepower Management Center
- Snort

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FMC 7.0
- FTD 7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

### Premesse

La funzione Snort 3 è stata aggiunta nella versione 6.7 per Firepower Device Manager (FDM) e Cisco Defense Orchestrator (CDO); nella versione 7.0 per Firepower Management Center (FMC).

Snort 3.0 è stato progettato per affrontare queste sfide:

- 1. Riduzione dell'utilizzo della memoria e della CPU.
- 2. Migliorare l'efficacia dell'ispezione HTTP.
- 3. Caricamento più rapido della configurazione e riavvio automatico.
- 4. Migliore programmabilità per una più rapida aggiunta di funzionalità.

#### Configurazione

Aggiorna la versione Snort

Metodo 1

1. Accedere a Firepower Management Center.

۱۱۱۰۱۱۰ CISCO
Firepower
Management
Center
Username
Password
Log In

2. Nella scheda Periferica passare a Periferiche > Gestione periferiche.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Device	s Objects	Integration
Summary Dashboard (mitch.dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	itatus Ge	eolocation	QoS t	Devic Devic NAT	e Management e Upgrade	QoS Platform Settings FlexConfig Certificates
<ul> <li>Unique Applications over Time</li> </ul>			- ×	Site Rem Dyna Troul	To Site ote Access mic Access Policy pleshooting	

3. Selezionare il dispositivo di cui si desidera modificare la versione 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						
Nar	ne			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
	192.168.1.15(Secondary, Stand 192.168.1.15 - Routed	by)		FTDv for VMware	7.0.5	N/A

4. Fare clic sulla scheda Periferica e fare clic sul pulsante Aggiorna nella sezione Motore di ispezione.

HA-CALO-LAB Jaco Fergower Threat Defense for VMware Summary High Availability Device R	outing Interfaces Inline Sets D	HCP			
				192.5	48.1.14 +
General	/±1	System	<b>0</b> G	Inspection Engine	
Name:	192.168.1.14	Model:	Cisco Firepower Threat Defense for VMware	Inspection Engine:	Snort 2
Transfer Packets:	Yes	Serial	9AEMA2W99U4	NEW Upgrade to our new and improved Snort 3	
Mode:	Routed	Time:	2024-04-11 15:47:35	Snort 3 is the latest version of the most powerful, indust	try-standard inspection
Compliance Mode:	None	Time Zone:	UTC (UTC+0.00)	improvements to performance and security efficacy, the	re 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)	<ul> <li>Switching short versions requires a depoyment to co Because Short must be stopped so that the new version be momentary traffic loss.</li> </ul>	I can be started, there will
				Note: If the device uses an intrusion Policy that has cust will not be able to microite three rules.	Iom Intrusion Rule, Snort 3
				Copetite	

5. Confermare la selezione.



Metodo 2

1. Accedere a Firepower Management Center.

۱۱۱۰۱۱۰ CISCO
Firepower
Management
Center
Username
Password
Log In

2. Nella scheda Periferica passare a Periferiche > Gestione periferiche.

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

3. Selezionare il dispositivo di cui si desidera modificare la versione 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
	łA (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
	192.168.1.15(Secondary, Standb 192.168.1.15 - Routed	vy)		FTDv for VMware	7.0.5	N/A

4. Fare clic sul pulsante Seleziona azione e selezionare Aggiorna a Snort 3.



Aggiornamento delle regole di intrusione

Inoltre, è necessario convertire le regole Snort 2 in regole Snort 3.

1. Selezionate dal menu Oggetti > Regole intrusione.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
lescription, or l	Base Policy			Object N Intrusion	lanagemen Rules	ıt

2.Selezionare dal menu Ordina 2 tutte le regole scheda > Raggruppa regole per > Regole locali.



3. Fare clic su Ordina 3 Tutte le regole scheda e assicurarsi che Tutte le regole sia selezionato.

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

4.Dal menu a discesa Task, selezionare Converti e importa.



5. Fare clic su OK sul messaggio di avvertenza.

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

### Verifica

La sezione Motore di ispezione mostra che la versione corrente di Snort è Snort 3.



La conversione della regola è riuscita quando viene visualizzato questo messaggio:



Infine, nel gruppo Regole locali è necessario trovare la sezione All Snort 2 Converted Global contenente tutte le regole convertite da Snort 2 a Snort 3.



# Risoluzione dei problemi

Se la migrazione non riesce o si interrompe, eseguire il rollback allo Snort 2 e riprovare.

### Informazioni correlate

- Migrazione da Snort 2 a Snort 3
- Cisco Secure Aggiornamento dispositivo Snort 3 (video esterno di YouTube)

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).