Actualización de Snort 2 a Snort 3 mediante FMC

Contenido

Introducción	
Prerequisites	
Requirements	
Componentes Utilizados	
Antecedentes	
Configurar	
Actualización de la versión de Snort	
Método 1	
Método 2	
Actualización de reglas de intrusión	
<u>Verificación</u>	
Resolución de problemas	
Información Relacionada	

Introducción

Este documento describe cómo actualizar desde la versión 2 y 3 de Snort en Firepower Manager Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense
- Centro de administración FirePOWER
- Snort

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FMC 7.0
- FTD 7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función Snort 3 se añadió en la versión 6.7 para Firepower Device Manager (FDM) y Cisco Defense Orchestrator (CDO); en la versión 7.0 para Firepower Management Center (FMC).

Snort 3.0 se ha diseñado para hacer frente a estos retos:

- 1. Reduzca el uso de memoria y CPU.
- 2. Mejore la eficacia de la inspección HTTP.
- 3. Carga de configuración más rápida y reinicio de Snort.
- 4. Mejor programabilidad para una incorporación más rápida de funciones.

Configurar

Actualización de la versión de Snort

Método 1

1. Inicie sesión en Firepower Management Center.

սիսիս cisco
Firepower
Center
Username
Password
Log In

2. En la pestaña Device, navegue hasta Devices > Device Manager.

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
 Unique Applications over Time 			- ×	Site Rem Dyna Troul	To Site ote Access mic Access Policy pleshooting	

3. Seleccione el dispositivo cuya versión de Snort desea cambiar.

View By: All (2)	Group • Error (0) • Warning (0)	• Offline (0)	Normal (2)	 Deployment Pending 	1 (1) • Upgrade (0)	
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, Stand 192.168.1.15 - Routed	by)		FTDv for VMware	7.0.5	N/A

4. Haga clic en la pestaña Device y haga clic en el botón Upgrade en la sección Inspection Engine.

IA-CALO-LAB isco Firepower Threat Defense for VMware					
Summary High Availability Device I	louting Interfaces Inline Sets D	HCP			
				192.9	•
General	/±=	System	0 G	Inspection Engine	
Name:	192.168.1.14	Model:	Cisco Firepower Threat Defense for VMware	Inspection Engine:	Snort 2
Transfer Packets:	Ves.	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, industr	ry-standard inspection
Compliance Mode:	None	Time Zone:	UTC (UTC+0.00)	engine at the heart of Finepower Threat Detense devices improvements to performance and security efficacy, then	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)	Switching snort versions requires a deployment to co Because Snort must be stopped so that the new version be momentary traffic loss.	can be started, there will
				Note: If the device uses an intrusion Policy that has cush will not be able to migrate those rules.	om Intrusion Rule, Snort 3
				Uppede	

5. Confirme su selección.



Método 2

1. Inicie sesión en Firepower Management Center.

սիսիս cisco
Firepower
Center
Username
Password
Log In

2. En la pestaña Device, navegue hasta Devices > Device Manager.

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
 Unique Applications over Time 			- ×	Si Re Dy Tr	e To Site mote Access namic Access Policy publeshooting	

3. Seleccione el dispositivo cuya versión de Snort desea cambiar.

View By:	Group	•				
All (2)	Error (0) Warning (0)	 Offline (0) 	Normal (2)	Deployment Pending (1)	 Upgrade (0) 	
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. Haga clic en el botón Select Action y seleccione Upgrade to Snort 3.



Actualización de reglas de intrusión

Además, debe convertir las reglas de Snort 2 en reglas de Snort 3.

1. Seleccione en el menú Objetos > Reglas de intrusión.

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

2. Seleccione en el menú Snort 2 All Rules (Todas las reglas) > Group Rules By (Agrupar reglas por) > Local Rules (Reglas locales).



3. Haga clic en Snort 3 All Rules pestaña y asegúrese de que All Rules está seleccionado.

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

4.En el menú desplegable Task, seleccione Convert and import.



5. Haga clic en Aceptar en el mensaje de advertencia.



Verificación

La sección Motor de inspección muestra que la versión actual de Snort es Snort 3.



La conversión de la regla se realizó correctamente una vez que aparece este mensaje:



Por último, debe encontrar en el grupo Local Rules la sección All Snort 2 Converted Global, que contiene todas las reglas convertidas de Snort 2 a Snort 3.



Resolución de problemas

En caso de que la migración falle o falle, vuelva a Snort 2 e inténtelo de nuevo.

Información Relacionada

- <u>Cómo migrar de Snort 2 a Snort 3</u>
- Cisco Secure Actualización de dispositivo Snort 3 (vídeo externo de YouTube)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).