Upgrade van Snort 2 naar Snort 3 via FMC

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Configureren
Upgrade de Snelversie
Methode 1
Methode 2
Upgrade van inbraakregels
Verifiëren
Probleemoplossing
Gerelateerde informatie

Inleiding

In dit document wordt beschreven hoe u kunt upgraden van de versie Snort 2 en Snort 3 in Firepower Manager Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defence
- Firepower Management Center
- Snort

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VCC 7.0
- FTD 7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De functie Snort 3 is toegevoegd in de 6.7-release voor Firepower Device Manager (FDM) en Cisco Defense Orchestrator (CDO), in de 7.0-release voor het Firepower Management Center (FMC).

Snort 3.0 is ontworpen om deze uitdagingen aan te gaan:

- 1. Minder geheugen en minder CPU-gebruik.
- 2. Verbeter de HTTP-inspectie-efficiëntie.
- 3. Snellere configuratie laden en Snelstart opnieuw starten.
- 4. Betere programmeerbaarheid voor snellere toevoeging van extra functies.

Configureren

Upgrade de Snelversie

Methode 1

1. Meld u aan bij Firepower Management Center.

2. Ga op het tabblad Apparaat naar Apparaten > Apparaatbeheer.

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

3. Selecteer het apparaat dat u de gescande versie wilt wijzigen.

View By: Group All (2) Error (0) Warning (0) Offline (0) Normal (2)	 Deployment Pending (1) 	• Upgrade (0)	
Collapse All			
Name	Model	Version	Chassis
□ ∨ HA (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
I92.168.1.15(Secondary, Standby) 192.168.1.15 - Routed	FTDv for VMware	7.0.5	N/A

4. Klik op het tabblad Apparaat en klik op de knop Upgrade in het gedeelte Inspection Engine.

A-CALO-LAB aco Firepower Thread Defense for VMware Summary High Availability Device F	outing Interfaces Inline Sets D	нср			
				192.168.1	.14
General	/±1	System	0 G	Inspection Engine	
Name:	192.168.1.14	Modet	Cisco Firepower Threat Defense for VMware	Inspection Engine:	Snort 2
Transfer Packets:	Yes	Serial.	9AEMA2W99J4	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, industry-s	standard inspection
Compliance Mode:	None	Time Zone:	UTC (UTC+0.00)	engine at the heart of Firepower Threat Detense devices. We 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)	 Switching short versions requires a depoyment to comp Because Short must be stopped so that the new version can be momentary traffic loss. 	ete the process. n be started, there will
				Note: If the device uses an intrusion Policy that has custom will not be able to migrate those rules.	Intrusion Rule, Snort 3
				Uspate	

5. Bevestig uw selectie.



Methode 2

1. Meld u aan bij Firepower Management Center.

2. Ga op het tabblad Apparaat naar Apparaten > Apparaatbeheer.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration
Summary Dashboard (matter: stantscord) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Ge	eolocation	QoS t	Device Device NAT	Management Upgrade	QoS Platform Settings FlexConfig Certificates
 Unique Applications over Time 			- ×	Site To Remote Dynami Trouble	Site Access c Access Policy shooting	

3. Selecteer het apparaat dat u de gescande versie wilt wijzigen.

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. Klik op de knop Actie selecteren en selecteer Upgrade naar snurk 3.



Upgrade van inbraakregels

Daarnaast moet u uw Snort 2 regels omzetten in Snort 3 regels.

1. Selecteer in het menu Objecten > Inbraakregels.

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

2. Selecteer in het menu Sneltoets 2 All Rules > Group Rules By > Local Rules.



3. Klik op Sneltoets 3 Alle regels en zorg ervoor dat Alle regels is geselecteerd.

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

4. Selecteer in het vervolgkeuzemenu Taak de optie Omzetten en importeren.



5. Klik op OK in het waarschuwingsbericht.

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

Verifiëren

De sectie Inspection Engine laat zien dat de huidige versie van Snort Snort 3 is.

Inspection Engine	
Inspection Engine:	Snort 3
Revert to Snort 2	

De regelconversie is voltooid zodra u dit bericht ziet:



Tot slot moet u in de groep Local Rules de sectie All Snort 2 Converted Global vinden, die al uw geconverteerde regels Snort 2 tot Snort 3 bevat.



Probleemoplossing

Als de migratie mislukt of crasht, draait u terug naar Snuit 2 en probeert u het opnieuw.

Gerelateerde informatie

- Hoe te migreren van Snort 2 naar Snort 3
- <u>Cisco Secure Video voor snort-3 apparaat (externe YouTube-video)</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.