Upgrade von Snort 2 auf Snort 3 über FMC

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
<u>Hintergrundinformationen</u>
Konfigurieren
Snort-Version aktualisieren
Methode 1
Methode 2
Aktualisierung von Angriffsregeln
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird das Upgrade von der Snort 2- und Snort 3-Version im Firepower Manager Center (FMC) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Threat Defence
- FirePOWER Management Center
- Snort

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FMC 7.0
- FTD 7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Snort 3-Funktion wurde in Version 6.7 für FirePOWER Device Manager (FDM) und Cisco Defense Orchestrator (CDO) sowie in Version 7.0 für FirePOWER Management Center (FMC) hinzugefügt.

Snort 3.0 wurde für folgende Herausforderungen entwickelt:

- 1. Reduzierung der Arbeitsspeicher- und CPU-Auslastung
- 2. Verbesserung der Effizienz von HTTP-Prüfungen.
- 3. Schnelleres Laden der Konfiguration und Neustart von Snort.
- 4. Bessere Programmierbarkeit für schnellere Funktionsbereitstellung

Konfigurieren

Snort-Version aktualisieren

Methode 1

1. Melden Sie sich bei FirePOWER Management Center an.

راندان cisco
Firepower
Management
Center
Username
Password
Log In

2. Navigieren Sie auf der Registerkarte Gerät zu Geräte > Geräte-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	atus Geolocation QoS ti		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. Wählen Sie das Gerät, das Sie die Snort-Version ändern möchten.

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. Klicken Sie auf die Registerkarte Gerät und dann im Abschnitt Inspektionsmodul auf die Schaltfläche Upgrade.

HA-CALO-LAB Cisco Firepower Threat Defense for Wilware					
Summary High Availability Device R	Routing Interfaces Inline Sets D	HCP			
(Annual		for the second sec		Assessment Facility	192.168.1.14 •
General	/17	System	ØG	Inspection Engine	
Name:	192.168.1.14	Modec.	Cisco Firepower Threat Defense for VMware	Inspecton Engine.	Snort 2
Transfer Packets:	Yes	Serial	SAEMADW69J4	NEW Upgrade to our new and improved Snor	13
Mode:	Routed	Time:	2024-04-11 15:47:36	Snort 3 is the latest version of the most powerful, i	ndustry-standard inspection
Compliance Mode:	None	Time Zone:	UTC (UTC+0.00)	improvements to performance and security efficac	y, 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 deployment Because Short must be stopped so that the new w be momentary traffic loss.	to complete the process, ersion can be started, there will
				Note: If the device uses an intrusion Policy that has will not be able to migrate those rules.	s custom Intrusion Rule, Snort 3
				Uppede	

5. Bestätigen Sie Ihre Auswahl.



Methode 2

1. Melden Sie sich bei FirePOWER Management Center an.

راندان cisco
Firepower
Management
Center
Username
Password
Log In

2. Navigieren Sie auf der Registerkarte Gerät zu Geräte > Geräte-Manager.

Firepower Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devi	ces Objects	Integration
Summary Dashboard (setter destinant) Provides a summary of activity on the appliance Network × Threats Intrusion Events S	Status Geolocation OoS		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. Wählen Sie das Gerät, das Sie die Snort-Version ändern möchten.

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. Klicken Sie auf die Schaltfläche Aktion auswählen und wählen Sie Auf Snort 3 aktualisieren.



Aktualisierung von Angriffsregeln

Außerdem müssen Sie Ihre Snort 2-Regeln in Snort 3-Regeln umwandeln.

1. Wählen Sie im Menü Objekte > Zugriffsregeln aus.

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

2.Wählen Sie im Menü Snort 2 All Rules (Alle Regeln) > Group Rules By (Regeln gruppieren nach) > Local Rules (Lokale Regeln).



3. Klicken Sie auf Snort 3 Alle Regeln Registerkarte und stellen Sie sicher, dass Alle Regeln ausgewählt ist.

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

4. Wählen Sie im Dropdown-Menü Task die Option Konvertieren und importieren aus.



5. Klicken Sie in der Warnmeldung auf OK.

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

Überprüfung

Der Abschnitt Inspection Engine zeigt, dass die aktuelle Version von Snort Snort 3 ist.

Inspection Engine Snort 3 Inspection Engine: Revert to Snort 2

Die Regelkonvertierung war erfolgreich, nachdem folgende Meldung angezeigt wurde:



Schließlich müssen Sie in der Gruppe Lokale Regeln den Abschnitt Alle Snort 2 konvertiert global finden, der alle von Snort 2 zu Snort 3 konvertierten Regeln enthält.



Fehlerbehebung

Wenn die Migration fehlschlägt oder abstürzt, setzen Sie den Rollback-Modus auf Snort 2 zurück, und versuchen Sie es erneut.

Zugehörige Informationen

- So migrieren Sie von Snort 2 auf Snort 3
- Cisco Secure Upgrade von Snort 3-Geräten (externes YouTube-Video)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.