FP-Upgrade - Gerätezustandsüberwachung

Inhalt

Einleitung Hintergrundinformationen Funktionsüberblick Funktionsdetails 7.0 FTD: Kennzahlen aus FP 7.0 Funktionsdetails 6.7 REST-APIs FMC REST APIs - Zusammenfassung REST-APIs für FTD-Geräte Fehlerbehebung/Diagnose Häufig gestellte Fragen Interne Nachverfolgungsinformationen

Einleitung

In diesem Dokument wird die neue Funktion zur Überwachung der Geräteintegrität beschrieben, die in Version 6.7 und 7.0 hinzugefügt wurde.

Hintergrundinformationen

Migration von:

https://confluence-eng-rtp2.cisco.com/conf/display/IFT/Change+Management+FP+7.0

https://confluence-engrtp2.cisco.com/conf/pages/viewpage.action?spaceKey=IFT&title=Device+Health+Monitoring

Das Problem:

Das Systemüberwachungssystem bietet Einblick in die Geräteleistung für reaktives Debuggen und proaktive Aktionen.

Umfassende Transparenz und Analyse wird erzielt durch:

- Trenddiagramme für wichtige Kennzahlen
- Ereignis-Overlay
- Anpassbare Dashboards
- Einheitliche Architektur für die Systemüberwachung gleiche Daten für alle Manager anzeigen

• Viele neue Kennzahlen und Erweiterbarkeit von Kennzahlen, um viele weitere hinzuzufügen

Neuerungen in Version 7.0

Neuerungen oder Unterschiede gegenüber FP 7.0

- FMC-Dashboard mit HA-Unterstützung
- Mehr als 110 neue Kennzahlen für FTD
- Gesundheitswarnung für FTD Split Brain Szenario
- Benutzerdefiniertes Laufzeitintervall für neuere Integritätsmetriken

Vorteile

- Hilft beim Debuggen von Systemen, indem Daten aus verschiedenen Subsystemen und Ressourcen auf Geräten korreliert werden können
- Transparenz für verschiedene Systemleistungsmetriken
- Kapazitätsplanung

Neu bei 6.7

Neu oder anders als die unmittelbar vorangehende Version (allgemein):

- Neue Benutzeroberfläche für die Überwachung des Gerätestatus auf dem FMC
- FTD Device REST API: Device-Metrik API: Viele neue Metriken hinzugefügt
- FMC-APIs: Neue APIs: Integritätswarnungen, Integritätsmetriken und Bereitstellungsdetails
- Allgemeiner Überblick über den Marktplatz, reale Anwendungen
- Hilft beim Debuggen von Systemen, indem Daten aus verschiedenen Subsystemen und Ressourcen auf Geräten korreliert werden können
- Transparenz
- Kapazitätsplanung

Funktionsüberblick

So funktioniert es

- Überwachung der Geräteintegrität in FP 7.0
- Neues Health Dashboard für FMC mit Trenddiagrammen, Overlays und benutzerdefinierten Dashboards
- Neue FTD-Kennzahlen in FTD-Dashboards verfügbar
- Über 110 Kennzahlen für 12 Kategorien
- FTD-APIs: ermöglicht die Abfrage von Metriken durch externe Einheiten

Unter der Haube

- Erfasst den Zustand eines Geräts mit Telegraf (ein Open-Source-Framework zur Metriksammlung)
- Exportiert die Daten an FMC (mit Prometheus, das auf FMC läuft und angeschlossene Geräte abfragt)

Zusätzliche Hinweise

Systemüberwachungsdaten sind verfügbar

- Im FMC Health Dashboard, über das Systemmenü zugänglich (System > Health > Monitor)
- Von der FMC REST API
- Wenn das Gerät von FDM verwaltet wird, über die REST-API des FTD-Geräts

Einige Kennzahlen (FMC und FTD) sind standardmäßig deaktiviert.

• Integritätsmodule in der Integritätsrichtlinie müssen aktiviert und bereitgestellt werden, damit Metriken angezeigt werden.

Implementierung der von den IFTs des RP 6.7 angeforderten Verbesserungen

- Standardmäßig automatisch aktualisieren
- Filter mit benutzerdefiniertem Zeitbereich auf Dashboard
- Auswahl von Schnittstellen anhand des benutzerdefinierten Namens (sowie des physischen Schnittstellennamen) in der Schnittstellenauswahl
- Starten Sie das Geräte-Dashboard über die Startseite des Systemmonitors.

Überwachung des Gerätestatus in FP 6.7

 Neue Benutzeroberfläche auf FMC mit Trend-Diagrammen, Overlays und benutzerdefinierten Dashboards.

• FTD-APIs: Bereitstellung derselben Metriken für Abfragen durch externe Einheiten Unter den Deckblättern:

- Erfasst den Zustand eines Geräts mithilfe des Open-Source-Tools Telegraf.
- Exportiert die Daten in FMC (mithilfe der Open Source-Datenbank der Zeitreihe Prometheus, die auf FMC ausgeführt wird, indem alle Geräte eine Minute abgefragt werden).
- Manager: FMC, FMC REST API, FTD Device REST API

Zusammenfassung der Einschränkungen:

- Die Funktion wird auf der FDM-GUI oder CDO nicht unterstützt.
- Die Überwachung von FMC selbst innerhalb der neuen Benutzeroberfläche für die Systemüberwachung wird nicht unterstützt.
- Abfrageintervalle sind nicht konfigurierbar. Sie können keine unterschiedlichen Abfrageintervalle für verschiedene Geräte konfigurieren. Alle werden in einem festen Intervall von einer Minute abgefragt.

Bereitstellungsbeispiele

- Es ist keine spezielle Bereitstellung zum Testen der Funktion erforderlich. Aktualisieren Sie einfach FMC und Gerät auf FP 6.7.
- Die Statusüberwachungsdaten sind im FMC-Statusdashboard verfügbar, auf das Sie über die Systemregisterkarte zugreifen können.

	Q Deploy	🚱 🌣 🙆 admin		
Configuration	Logging	Monitoring		
Users	Stealthwatch Logging	Audit		
Domains		Syslog		
Integration	Health	Statistics		
Updates	Monitor			
	Policy	Tools		
Licenses	Events	Backup/Restore		
Smart Licenses	Blacklist	Scheduling		
Classic Licenses	Monitor Alerts	Import/Export		
		Data Purge		

Voraussetzungen und unterstützte Plattformen

Mindestanzahl unterstützter Software- und Hardwareplattformen

Min. unterstützte Manager-Version	Verwaltete Geräte	Min. unterstützte Version des verwalteten Geräts erforderlich	Hinweise
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	Nur auf FTDs unterstützt
REST-API für FTD- Geräte	FTD 6.7	FXOS 2.9.1 FTD 6.7	Nur REST-API für FTD- Geräte (keine FDM- oder CDO- GUIs)

Interoperabilität

Keine spezifischen Anforderungen an die Interoperabilität.

Funktionsdetails 7.0

FMC-Benutzeroberfläche: Standalone und HA-Unterstützung

Navigation zur Seite "Systemüberwachung"

CISCO FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	0	\$ 🕽 syed 🕶
Monitoring The Home FMC Active FMC Standby FMC Devices (2) 192.168.0.21 9 192.168.0.21	a	Health S	Catus 2 critical ices MC_Active MC_Standby 2.168.0.217	0 warnings	1 normal	1 disabled	C. Filter us	ing device	name	\$	

- Standalone-FMC wird als einzelner Knoten angezeigt
- FMC HA als Paar von Knoten dargestellt
- Für jedes FMC wird der Status "Health" angezeigt.

Integritätsstatus

- FMC HA ist in Doppelhexagonal dargestellt.
- Aktive und Standby-Geräte des FMC werden ebenfalls in der Warnmeldungstabelle aufgeführt.

FMC-Dashboard

FMC Health Monitoring Dashboard in 7.0

Firepower Manage System / Health / Monitor	ement Cente	er _{ove}	erview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deplo	y Q 📀 🌣		
Monitoring () 없 Home ~ FMC	Health: FM View System & Overview	C_Active Troubleshoot Process	e \rm Critica Details	1						S 20	ielect 020-12-08 04:04 -	2020-12-08 05:04	
Active FMC	High Availabi	ility					Manage HA	Event Rate	B				
 Standby FMC Devices (2) 192.168.0.216 192.168.0.217 	Primary-	Local Degraded Remote Last sync: a few seconds ago Primary- Active Degraded Synchronization incomplete						386 286 856 0.0 DLD4 04:09 04:14 04:19 04:24 04:29 04:34 04:39 04:44 04:49 04:54 04:59				04:54 04:59	
	Process Health Critical Processes All Processes							Event Cap	acity			Configure	
	ActionQ	DCCSM	ESS	Msg Service	Peri MsgHandler	Pruner	RabbitMQ		Intrusion No Events	nits	526.79K/1M 0/1M 1.23W/1M		
	SFDC Notifier	SF Data Correlator	Sync D	Torncat	Provisioning Process	ADI	Disk Manager	Security I	ntelligence 57 days 3 hrs 13 mi	ina		100K/1M	
	Mojo	Monet DB	Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Connection	Malware No Events			0/1M	
	sftunnel	SLA		Sybase Arbiter	Symmetric	: Syt	ase DB		Discovery No Events User No Events			0/1M 0/1M	
	CPU 100% 75% 50% 25% 0% 0%	09 04:14	04:19 04:24	0129 043	4 04:39 04:2	Avg CF	₽ U ~	Memory - 100% 75% 50% 25% 0% 0%	Used	4 04:29 04:34 04:3	59 04.44 04.49	04.54 04.59	
	Interface - Input Rate Output Rate 44.3K 22.2K 11.1K 0 04.04 04.09 04.14 04.19 04.24 04.29 04.34 04.39 04.44 04.49 04.54 04.59					Disk Usag	e Entire Disk		Critical Partitio	ns			

Zusammenfassende Ansicht von:

- Hohe Verfügbarkeit
- Ereignisrate und -kapazität
- Prozesssicherheit
- CPU
- Arbeitsspeicher
- Schnittstelle
- Festplatte

Dieses Dashboard ist für aktive und Standby-FMCs verfügbar. Benutzer können benutzerdefinierte Dashboards erstellen, um Metriken ihrer Wahl zu überwachen.

FMC-Dashboard: FMC HA-Panel

High Availability		Configure
Local Primary- Active	Degraded Last sync: a few seconds ago Degraded- Synchronization incomplete	Remote Secondary- Standby FMC_Standby - Critical Alerts: 2 40 21 Top 5 Alerts File system integrity check FMC HA Status Host Limit Classic License Expiration Monitor AMP for Endpoints Status View all alerts

HA-Panel zeigt

- Aktueller HA-Status
- Aktiv und Standby
- Letzte Synchronisierungszeit
- Geräteintegrität

FMC-Dashboard: Ereignisrate und Kapazität

Ereignisrate

- Maximale Ereignisrate als Grundlinie
- Gesamtereignisrate, die FMC erhält

Event-Kapazität

- Stromverbrauch nach Ereigniskategorien
- Aufbewahrungszeit von Ereignissen
- Aktuell vs. Maximum

Ereigniskapazität

Kapazitätsüberlaufmarkierung

Health: Fl View System 8 Overview	MC () Crit & Troubleshoo Process	tical ot Details s						La 20	ist 1 hour 21-02-22 06:32 - 2021-02-2	2 07:32
Process He	alth			Cri	tical Proces	sses A	I Processes	Event Capacity	Conf	hgure
ActionQ SF Data Correlator Mongo DB	DCCSM Sync D MySQL DB	ESS Tomcat Run HM	Msg Service Provisioning Process SFIP Proxy	Perl MsgHandler ADI SF Mgr	Pruner Disk Manager Sftunnel	RabbitMQ Mojo SLA	SFDC Notifier Monet DB Sybase Arbiter	Connection 3 days 16 hrs 3 mins Intrusion No Events File No Events Security Intelligence No Events Connection Summary No Events Malware No Events Discovery No Events	1/1M 0/1M 0/1M 0/1M 0/1M 0/2M 0/1M	*
CPU A Data col shown.	lection for C	CPU module	e is disabled	in the healt	h policy, pa	Avg CPI	J v	User No Events	0/1M	¥ 17:30

FMC-Dashboard: Event-Kapazität

Normaler Kapazitätsverbrauchszustand bei Ereignissen

Normal:				
Connection	182 days 4 hrs 23 m	ins		5.6 M / 10 M
Connection	182 days 4 hrs 23 mi	ns		5.6 M / 10 M
	Jun 12, 2020 7:00 PM Oldest Event	3.6k/min Incoming Rate	56458978/10000000 Capacity	
Overflow	v:			
Connection	18h			11.6 M / 10 M
Connection	2020-09-18 14:28:30 18h			11.6 M / 10 M
	18 hours Retention Duration	3.6k/min Incoming Rate	116245455/100000000 Capacity 🛆 🔫	

Überlaufszenario, wenn Ereignisse über die konfigurierte maximale Kapazität hinaus gespeichert werden.

- Fettformatierter Text weist auf Überlauf hin
- Ein Warnsymbol zeigt den Kapazitätsüberlauf an.

FMC-Dashboard: FMC-Prozess-Panel

Anzeige "Kritische Prozesse"

Aktuellen Status verarbeiten

Anzahl der Prozessneustarts

Process H	ealth					Criti	ical Proc	esses A	All Processes
ActionQ	DCCSM	ESS	Msg Service	Perl MsgHand	Pruner		RabbitMQ	SFDC Notifier	SF Data Correlator
Sync D	Tomcat	Provisioning Process	ADI	Disk Manager	Mojo		Monet DB	Mongo DB	MySQL DB
Run HM	SFIP Prov	ky SF Mgr	Sftunne	I SL	A	Syba: Arbite	se er	Symmetric	Sybase DB

Das Prozess-Panel zeigt die folgenden Metriken für alle "pmconfig"-Prozesse an:

- Aktueller Status
- CPU-Nutzung
- Arbeitsspeichernutzung

Process Health		Critica	al Processes	All Processes
Process status at: Dec 14, 2020 3	22 AM			
Process *	Status	CPU (%)	Mem U	sed
ActionQ	Running	0	66	5.23KB
CSD App	Waiting	0		0
CSM Event Server	Running	0.6	18	32.1KB
CloudAgent	Running	0.9	12	2.03KB
DCCSM	Running	0	104	.49KB
ESS	Running	0.1	448	3.26KB
Event DS	Running	0	34	.59KB

FMC-Dashboard: FMC-CPU

CPU-Anzeige

- Durchschnittliche CPU (Standard)
- Alle Kerne





FMC-Dashboard: Andere Bereiche

Speicherbereich zeigt die gesamte Speichernutzung auf FMC an



Schnittstellenanzeige zeigt die Ein-/Ausgaberate des Durchschnitts aller Schnittstellen an



Das Datenträgerfeld wird angezeigt.

- Gesamte Festplattenkapazität
- Kritische Partitionskapazität, in der FMC-Daten gespeichert werden



Laufzeitintervall

- Das Laufzeitintervall für das alte Integritätsmodul wird in "Legacy-Laufzeitintervall"
 umbenannt.
- "Run Time Interval" bezieht sich auf die neuen Telegraf-basierten Statusmodule
- Globale Einstellung, wirkt sich auf alle Geräte aus
- Prometheus Scrape-Zeit zurücksetzen und startet den Health Monitoring-Prozess neu.

cisco Edit Overview Analysi	s Policies Devices	Objects AMP	Intelligence	Deploy Q 🄇	¢	🛛 admin 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Policy: Initial_H	ealth_Policy 2021-0	1-29 04:40:49			Alerts
AMP For Endpoints Status AMP for Firepower Status	Policy Name Policy Description	Initial_Health_Policy 2	2021-01-291			
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status	Legacy Run Time Interval (mins) Run Time Interval (mins) Note : Changes to Run Time Int monitoring process.	I 5) 1 terval will restart the health	7			
Backlog Status CPU Usage (per core) CPU Usage Data Plane CPU Usage Snort			Gancel Save Poli	cy and Exit		
CPU Usage System Card Reset Chassis Status FTD						
Cluster/Failover Status Configuration Database Connection Statistics						
Critical Process Statistics Deployed Configuration Statistics Disk Status						

Verfügbare Kennzahlen

Verfügbare Kennzahlen für benutzerdefinierte Dashboards

- Wenn ein Benutzer ein benutzerdefiniertes Dashboard erstellen möchte, dienen diese Folien als Leitfaden für die verfügbaren Metriken.
- Einige Kennzahlen müssen in der Integritätsrichtlinie aktiviert sein, bevor sie in einem benutzerdefinierten Integritäts-Dashboard verwendet werden können.

CISCO Edit Overview Analysis	Policies Devices	Objects AMP	Intelligence	Deploy	q 💕	≎	0	syed •
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status AMP For Endpoints Status	Editing Policy: Initial_He [en_US/admin:policy_la	ealth_Policy 2020-12 ast_modified])	2-08 08:49:46 (Last Mod	ified:				Alerts
AMP for Firepower Status ASP Drop	Policy Name Policy Description	Initial_Health_Policy 20 Initial Health Policy)20-12-08 (
Advanced Short Statistics Appliance Heartbeat Automatic Application Bypass Status	Description	Monitors CPU usage on all cores, threshold set here w applicable to all the cores	the vill be					
Backlog Status CPU Usage (per core)	Critical Threshold %	90						
CPU Usage Data Plane	Warning Threshold %	80						
CPU Usage System			Cancel Save Polic	y and Exit				
Chassis Status FTD								
Configuration Database								
Connection Statistics Critical Process Statistics								
Deployed Configuration Statistics Disk Status								
Disk Usage Event Stream Status								
FMC Access Configuration Changes								

FMC-Benutzeroberfläche: FMC Custom Dashboard

Neue FMC Monitoring Metrics-Kategorien in 7.0

- CPU
- Arbeitsspeicher
- Schnittstelle
- Festplatte
- Veranstaltung
- Prozess
- KaninchenMQ
- Sybase
- MySQL

Health: FN View System 8 Overview	MC Orit Troubleshoo Process	ical t Detail:	S	Last 1 hour C 2021-02-22 07:07 - 2021-02-22 08:07
Process He	alth		Critical Processes All Processes Event Capacity	Configure
ActionQ	DCCSM	ESS	Add Dashboard Ø X	1/1M 0/1M
SF Data Correlator	Sync D	Tomca	Name*	0/1M
Mongo DB	MySQL DB	Run HI	my_custom_dashboard 5	0/1M 0/2M
Symmetric			Chosen metrics will be displayed as portlets in the dashboard.	0/1M
CPU			Add Metrics	
			Cancel Add Dashboard	

FMC-Benutzeroberfläche: FMC-Kennzahlen

40 Metriken, die über verschiedene Kategorien hinweg hinzugefügt wurden (im benutzerdefinierten Dashboard verfügbar). Um die deaktivierten Metriken zu aktivieren, aktivieren Sie das entsprechende Integritätsmodul in der zugeordneten Integritätsrichtlinie (**System > Health > Policy**).

Metrik- Gruppenname	Standardmäßig aktiviert	Beschreibung
CPU	Nein	Überwacht FMC-CPU
Arbeitsspeicher	Ja	Überwacht FMC-Speicher
Festplatte	Ja	Überwachung der FMC- Festplattennutzung
Schnittstelle	Ja	Überwacht FMC-Schnittstelle
Prozess	Ja	Überwacht FMC-Prozesse
Veranstaltung	Ja	Überwacht die Ereignisrate
MySQL	Nein	Überwacht MySQL
KaninchenMQ	Nein	Monitore RabbitMQ
Sybase	Nein	Überwacht Sybase

FTD: Kennzahlen aus FP 7.0

Standardmäßig aktiviert: Metriken werden standardmäßig gesammelt. Um die deaktivierten Metriken zu aktivieren, aktivieren Sie das entsprechende Integritätsmodul in der zugeordneten Integritätsrichtlinie (System > Health > Policy).

Metrik-Gruppenname	Standardmäßig aktiviert	Beschreibung	Plattform
Chassis-Status	Ja	Unterschiedliche Chassis- Parameter wie Lüftergeschwindigkeit und Temperatur werden überwacht.	Nur für Plattformen FPR2100 und FPR1000 geeignet
Flow-Offload	Ja	Überwacht Statistiken zum Hardware-Fluss-Offload	Gilt für FPR9300 und FPR4100- Plattformen
ASP-Drops	Ja	Überwachung von Paketverlusten auf der Lina-	Alle

		Seite Überwachung der	
Trefferanzahl	Nein	Trefferanzahl für Zugriffskontrollrichtlinien- Regeln	Alle
AMP Threat Grid-Status	Ja	Überwacht die Verbindung zu AMP ThreatGrid	Alle
AMP-Verbindungsstatus	Nein	Überwachung der AMP-Cloud- Konnektivität über FTD	Alle
Status des SSE- Connectors	Nein	Überwachung der SSE-Cloud- Konnektivität über die FTD Überwacht NTP-	Alle
NTP-Status	Nein	Uhrensynchronisierungsparam eter auf die FTD	Alle
VPN-Statistiken	Ja	Überwacht S2S- und RA VPN- Tunnelstatistiken Überwachung von	Alle
Routenstatistik	Ja	Paketverlusten auf der Lina- Seite	Alle
Snort 3 Perf Statistiken	Ja	Überwacht bestimmte Snort3- Leistungsstatistiken (perfstats) Überwachung von xTLS/SSL-	Alle
xTLS-Zähler	Nein	Datenflüssen, Arbeitsspeicher- und Cache-Effektivität	Alle

REST-APIs, Syslog, SNMP

In Version 7.0 wurden keine neuen REST-APIs für FMC- oder FTD-Geräte eingeführt. Die vorhandenen REST-APIs unterstützen neue Metriken, die in Version 7.0 hinzugefügt wurden.

Syslog und SNMP

Syslog

Keine Änderung im Syslog für die Integritätsüberwachung SNMP

• Separate TOI für "SNMP Device Health Monitoring"

SAL/CTR/Integration von Drittanbieterprodukten

- Separater TOI für "Azure Application Insights"-Support
- Keine spezifische Änderung zur Unterstützung der Integration von "Health Monitoring" mit SAL/CTR/SecureX
- REST-API kann für Drittanbieterintegration genutzt werden

Software-Technologie

Überblick über die Architektur

- Telegraf-Health-Agent wird in FMC hinzugefügt, um FMC-spezifische Metriken zu sammeln
- Prometheus sammelt die Metriken von Telegraf und speichert sie in Zeitreihenmode.

- Warnungen werden generiert, wenn die Werte den benutzerdefinierten Schwellenwert in der Integritätsrichtlinie überschreiten.
- Telegraf Health Agent ist ein Open-Source-Plugin-gesteuerter Agent zum Erfassen von Metriken. Es sammelt alle 1 Minute Daten.
- Prometheus, eine Open-Source-Zeitreihendatenbank auf FMC, ruft alle 1 Minute die Kennzahlen vom Gerät ab.



Funktionsdetails 6.7

Beschreibung der Funktionsmerkmale

Neue NGFW-Zustandsüberwachung für FTD-Zustand und -Leistung

Erleichtert Benutzern

- Reaktives Debuggen, wie Ursachenanalyse, das Problem nach dem Auftreten
- Proaktive Maßnahmen wie die Überwachung von Nutzung und Sättigung, um potenzielle Kapazitätsprobleme zu identifizieren und die Benutzer bei Kapazitätserweiterungen oder Umgestaltungen zu unterstützen.

Vorteile für unsere TAC- und Technikerteams:

- Isolierung und Behebung von Systemproblemen
- Identifizieren von Engpässen im System sowohl bei der Entwicklung als auch in der Produktion.

Highlights

- **Trenddiagramme**: Trenddiagramme erleichtern das Erkennen von Anomalien und das Ermitteln der Ursache von Problemen. Mithilfe visueller Inspektionen können Trends erkannt und Korrelationen zwischen verschiedenen Metriken aufgezeichnet werden, um einen kausalen Zusammenhang zwischen ihnen zu finden.
- Ereignis-Overlays: Ereignis-Overlays zeigen wichtige Informationen an, z. B. die Konfigurationsbereitstellung und SRU-Updates in Trenddiagrammen, die ursächliche Zusammenhänge anzeigen.
- Anpassbare Dashboards: Benutzer können ihre eigenen Dashboards erstellen, um die gewünschten Metriken auf einer Seite zusammenzufassen.
- Einheitliche Architektur für die Integritätsüberwachung: Zentrale Stelle für die Erfassung und den Export von Kennzahlen, unabhängig davon, welcher Manager an den Kennzahlen "interessiert" ist. FTD-APIs und das FMC verwenden Daten vom gleichen Kennzahlensammler.
- Erweiterbarkeit von Metriken: Eines der Ziele der Architektur für die Plattform war es, einfach neue Metriken hinzufügen zu können. Dies wird durch die Verwendung von Open Source-Tools zur Sammlung und Speicherung von Metriken und durch anpassbare Dashboards erreicht.

So funktioniert es

- Telegraf Health Agent ist ein Open Source Plugin-gesteuerter Agent zum Sammeln von Metriken. Es sammelt regelmäßig alle 1 Minute.
- Prometheus, eine Open-Source-Zeitreihendatenbank auf FMC, bezieht die Kennzahlen regelmäßig alle 1 Minute.
- Die Metrikwerte stellen aktuelle Daten dar.
- Prometheus speichert die Daten im Zeitreihenformat, das von der Benutzeroberfläche wiedergegeben wird.
- Warnungen werden generiert, wenn die Werte den konfigurierten Grenzwert überschreiten.



FMC-GUI

FMC-Benutzeroberfläche: Navigieren zum Integritätsstatus

Klicken Sie auf FMC auf das Symbol **System > Health > Monitor**, um zur Seite **Health Status** (**Systemstatus) zu** gelangen.



FMC-Benutzeroberfläche: Neue Statusseite

Die Seite "Health Status" (Status - Status - Status) soll eine Statusübersicht aller vom FMC verwalteten Geräte anzeigen, einschließlich des Status des FMC.

- Die Geräte werden nach ihrer Gruppe/ha/Cluster gruppiert.
- Ein Punkt links neben dem Gerät zeigt seinen Zustand an.
- Grün keine Alarme
- Orange mindestens eine Gesundheitswarnung
- Rot mindestens ein kritischer Statusalarm
- Die Statuszusammenfassung wird angezeigt, wenn der Mauszeiger auf das Sechseck zeigt, das den Gerätestatus darstellt.
- Grenzwerte für Warnungen und kritische Meldungen können in der Integritätsrichtlinie genauso konfiguriert werden wie vor FP 6.7.

Monitoring 😑	Health Alerts
ធ៌ HOME	7 total 1 critical 2 warnings 5 normal 0 disabled Search a device X V
 FMC Devices (5) Asia 	FMC Asia ungrouped
 Bangalore (HA) bangalore-main 	Device Alerts: 1 0 4 2 0 21
bangalore-standby	FNC ECPU Usage CPU usad by sustam
chennai	bangalore-main Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalcre-standby local Malware Analysis
A 192.168.0.25	Clickto view more distails
A 192.168.0.26	> 🧿 mumbai
	> 🛕 192.168.0.25
	> 192.168.0.26

FMC-Benutzeroberfläche: Gerätestatusereignisse

Klicken Sie auf das Gerät im unteren Bereich, um die Systemzustandsereignisse anzuzeigen, die mit den Gerätewarnungen verknüpft sind. Diese werden nach ihrem Systemzustand (Schweregrad) sortiert.

Seite "Systemüberwachung"

>	A 192.168.0.25	
~	A 192.168.0.26	
	▲ CPU Usage Using CPU03 16%	Jun 23, 2020 2:54 AM
	 Automatic Application Bypass Status No applications were bypassed 	Jun 23, 2020 2:54 AM
	 Cluster/Failover Status Process is running correctly 	Jun 23, 2020 2:54 AM
	 Configuration Database Does not apply to this platform 	Jun 23, 2020 2:54 AM
	© CPU Usage Using CPU01 1%	Jun 23, 2020 2:53 AM
	© CPU Usage Using CPU02 0%	Jun 23, 2020 2:53 AM
	CPU Usage Using CPU00 0%	Jun 23, 2020 2:54 AM

FMC-Benutzeroberfläche: FMC-Zustandsüberwachung unverändert

Die FMC-Diagnoseseite ist nach wie vor die Legacy-Seite. Die neue Benutzeroberfläche wird nur für FTD mit 6.7+ unterstützt.

Monitoring =	Health	Monitor				
e 1140 e wm-101	0	Applance vfmc-10	Generate Troubleshooting Files Advanced Troubleshooting		Normal (50-	Module Status Summary Dealer Dong
	Alert D	etail (vfmc-10)		Time	Description	
	0	Process Status		2020-06-18 08:50:44	All processes are running correctly	
	۰	AMP for Endpoints Status		2020-06-18 08:50:44	Process is running correctly	
	0	AMP for Firepower Status		2020-06-18 08:50:44	Successfully connected to cloud	

FMC-Benutzeroberfläche: Neu! Geräte-Dashboards

- Klicken Sie im linken Bereich auf den Gerätenamen, um zur Übersichtsseite des Geräts zu gelangen.
- Die Statusübersicht enthält alle wichtigen Trenddiagramme für die Integritätsmetriken.
- Verschiedene Zeitbereiche sind verfügbar (Standard ist die letzte Stunde)
- Automatische Aktualisierung zum erneuten Laden des Diagramms

Monitoring 😑	Health: 192.168.0.25 Warning View System & Troubleshoot Details	Last 1 hour 2020-06-23 01:58 - 2020-06-23 02:58
ଜି HOME	Overview CPU Memory Interfaces Connections Snort	± +
Ø FMC	CPU	Memory
 Devices (5) 	LINA rog 15% Short rog 0.7% System Avg 17.5% 1 core 12% - 2.6% 2 cores 0.5% - 1.0% 1 core 15.0% - 24.0%	LINA Avg a9.7 % Short Avg 28.1 % System Avg 68.8 % 4.0468 49.7 % - 49.7 % 3.9668 28.1 % - 28.1 % 7.858 68.8 % - 69.4 %
✓ Asia	100	100
Bangalore (HA)	80	80
bangalore-main	60 10	60
bangalore-standby		10 00
chennai	Vienna.	00
o mumbai ∽ ungrouped	01:45 01:50 01:55 02:00 02:05 02:16 02:15 02:20 02:25 02:30 02:35 02:40	01:45 01:50 01:55 02:00 02:05 02:10 02:15 02:20 02:25 02:30 02:35 02:49
▲ 192.168.0.25	Throughput Avg Data Interfaces V	Connection Statistics
▲ 192.168.0.26	In sut Rate Avg 0 0 - 0 Output Rate Avg 0 0 - 0	Connections $A_{0+0}^{A_{0}}$ NAT Translations $A_{0+0}^{A_{0}}$
	2 800 2	100
	640	80
	480	40
	320	20
	0	0.0
	01.45 01.50 01.55 02.00 02.05 02.10 02.15 02.20 02.25 02.30 02.35 02.40	01:45 01:50 01:55 02:30 02:05 02:10 02:15 02:20 02:25 02:30 02:35 02:49
	Disk Usage	Critical Processes
	9%, 15%, 18%, Used	AMP Java LINA SF Data Consistor Strainel SSE Convector
		Short01 Short02
	Full Disk /ngfw /ngfw/Volume How To	

FMC-Benutzeroberfläche: Overlay der Bereitstellungsdaten

Klicken Sie auf das Bereitstellungssymbol, um Details zum Bereitstellungs-Overlay in dem Diagramm für den ausgewählten Zeitraum anzuzeigen.

- Symbol gibt die Anzahl der Bereitstellungen während des ausgewählten Zeitbereichs an
- Band zeigt den Beginn und das Ende der Bereitstellung an.
- Bei mehreren Bereitstellungen werden mehrere Bänder/Leitungen angezeigt.
- Klicken Sie auf das Symbol oben in der gepunkteten Linie, um die Details anzuzeigen.

	Health: 192.168.0.21 Normal View System & Troubleshoot Details Overview CPU Memory Interfaces Connections S	Last 1 hour C 2020-06-23 02:26 - 2020-06-23 03:26
	CPU Snort Avg 0.9 % System Avg 16.0 % 1 core 0.5 % - 1.6 % 2 cores 0.0 % - 8.5 % 1 core 13.0 % - 75.0 % 100	
CPU LINA Avg 2.7 % Snort of 1 core 0.5 % -7.8 % 2 cores of 80	Avg 3.7 % 0 % - 10.5 % 1 core 14.0 % - 300 %	CPU LINA Avg 2.7 % 1 core Snort Avg 4.3 % 2 cores System Avg 20.6 % 1 core 100 100 100 % - 75.0 % 100 100 100 % - 75.0 % 00 100 100 % - 75.0 % 00 100 100 % - 75.0 % 00 100 100 % - 75.0 % 00 100 100 % - 75.0 % 00 100 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00 100 % - 75.0 % 100 % - 75.0 % 00

FMC-Benutzeroberfläche: Vorgefertigte Dashboards für Geräte

- In der FMC-Benutzeroberfläche sind vordefinierte Status-Dashboards vorhanden.
- Diese vordefinierten Dashboards enthalten zusammengehörige Kennzahlen.
- Das Schnittstellen-Dashboard verfügt über ein Trenddiagramm für alle schnittstellenbezogenen Metriken wie Eingabe-/Ausgabe-Bytes, Pakete und die durchschnittliche Paketgröße für verschiedene Schnittstellen.

Hea	alth: wm	-101 🕑	Normal				
View	System & T	roubleshoot D	Details				
Ov	erview	CPU	Memory	Interfaces	Connections	Snort	
Int	erface - In	put Bytes, (Output Bytes				
s in Bps	1.6K						
value	1.2K						
	800						
	400						
	0						
		07:45		07:50	07	55	08:00
Int	erface - In	put Packets	s, Output Pack	ets, Drop Pack	ets		
1(0						
1	30						

FTD Snort Memory - Von wo stammt es?

Firepower Manage System / Health / Monitor	ement Cente	r Overvie	w Anal	ysis Poli	cies De	evices (Objects	AMP In	itelligence		Dep	loy Q	6 ⁰⁰ ¢	Global \ mzafei	iro 🔻
Monitoring	Health: mza View System & T	afeiro_FTD1	150-1 (Act ills	ive) 🥝 Norma	əl							La 20	ist 1 week 21-10-05 10:	59 - 2021-10-12 10:	59
份 Home	Overview	CPU	Memory	Interfaces	Connectio	ons Sno	rt ASP	drops						(m) (+	1
FMC	Mamoni - M	aviaura Data E	lana Data B	10.0.0											·
 Devices (8) 	Memory - M	aximum Data P	nane, Data P	ane											
√ cisco	5.7 GB														
mzafeiro_FP4100_8	4.1 GB														
GTS-FTD-IPS-CLUSTER	3.3 GB														
▲ 10.62.148.228	2.5 GB														
mzafeiro_4125-1	12:00	Oct 08	12:00	Oct 07	12:00	Oct 08	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12	- 11
KSEC-FPR4145-1-2	Memory - M	aximum Snort.	Snort												
v mzafeiro_FP1150-HA	20.2 GB							2021-	10-08 22:15 CES	T					
mzafeiro_FTD1150-1 Ac	18.3 GB							Material Mat	ximum Snort 20.2 ort 4.7	GB GB					
mzafeiro_FTD1150-2 s	12.5 GB														
mzafeiro_FTD4115-2	8.6 GB														
Sami_10.62.148.194	47.08							1,							
	12:00	Oct 08	12:00	Oct 07	12:00	Oct 08	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12	
	Memory - Sy	stem Used, To	tal												
	31.4 GB			_											
	25.8 GB														
	20.2 GB														-
	14.6.GR														

Die Ausgabe der Benutzeroberfläche bezieht sich auf:

```
admin@FP1150-1:~$ sudo pmtool show CGroupsStatus | grep "Detectio" -A 20
[/dev/cgroups/memory/Detection]
Resources:
memory.memsw.failcnt: 0
memory.max_usage_in_bytes: 7,840,403,456
memory.limit_in_bytes: 21,719,199,744
memory.memsw.max_usage_in_bytes: 7,840,403,456
memory.usage_in_bytes: 5,035,372,544
memory.memsw.limit_in_bytes: 22,403,170,304
memory.failcnt: 0
memory.memsw.usage_in_bytes: 5,035,372,544
Procs:
<p9738> sfhassd
<p26746> snort
<p26747> snort
<p26748> snort
<p26749> snort
<p26750> snort
<p26751> snort
<p26752> snort
<p26753> snort
Diese Informationen wurden von Technikern unter https://jira-eng-
```

rtp3.cisco.com/jira/browse/FPSVZ-1033 bereitgestellt.

FMC-Benutzeroberfläche: Erstellung benutzerdefinierter Dashboards möglich

Benutzer können ein eigenes benutzerdefiniertes Dashboard erstellen

- Zusätzlich zu den vordefinierten Dashboards können Benutzer auch benutzerdefinierte Dashboards erstellen.
- Im benutzerdefinierten Dashboard kann eine beliebige Anzahl von Metriken hinzugefügt werden.
- In der Regel wird ein benutzerdefiniertes Dashboard erstellt, wenn Metriken aus verschiedenen Metrikgruppen korreliert werden können, um die Ursache eines Problems zu

ermitteln.

• Im Falle einer hohen Lina CPU kann man die eingehende Verbindung pro Sekunde (Connection Per Second, CPS), Schnittstellenstatistiken (und so weiter) sehen, die eine hohe CPU verursachen können.



FMC-Benutzeroberfläche: Erstellen eines benutzerdefinierten Dashboards

Dialogfeld "Metriken korrelieren"

- Wenn ein Benutzer auf "+" klickt, um ein benutzerdefiniertes Dashboard zu erstellen, wird das Fenster "Metriken korrelieren" geöffnet.
- Ein Benutzer kann verschiedene Metriken hinzufügen, die er gemeinsam überwachen möchte.

Correlate Metrics		×
Correlate the metrics that are in custom to specify your own me Correlation Group*	ter-related. Select predefined corrections.	lation groups or
CPU - Snort		~
Hide Details Dashboard Name*		
Correlation-CPU-Snort		
Metrics Chosen metrics will be displaye	d as portlets in the dashboard.	× ~ ₹
Interface v	Input Packets X	× ~ ¥
Deployed Configuration \lor	Number of rules X	× ~ ¥
Deployed Configuration \lor	Number of ACEs X	× ~ 🖣
Add Metrics		
	C	ancel Add

REST-APIs

FMC REST APIs - Zusammenfassung

FMC GET-API	Beschreibung
/api/fmc_config/v1/domain/{domainUID}/health/al	Dadurch wird der Status aller Statusmodule für
Warnungen	die angegebene UUID.
	Die API ruft die Kennzahlen intern vom
/api/fmc_config/v1/domain/{domainUID}/health/ metriken	Time Series DB - Prometheus und senden Sie sie zurück an
	Anrufer.

FMC REST-APIs - /health/alert

Verschiedene Filterkriterien:

- startTime und endTime: in Sekunden. Beide zusammen anzugeben. Gibt alle Warnungen zurück, die zwischen den beiden Zeitpunkten generiert wurden.
- deviceUUID: Alle Warnungen für angegebene UUID zurückgeben
- Status: Gibt alle Warnungen mit dem angegebenen Status zurück (rot, gelb, grün)
- ModuleIDs: Liste der Funktionsmodul-IDs

Beispiel für das Ergebnis:

```
{
   "items": [
    {
        "deviceUUID": "a04cb2da-8915-11ea-9d2e-da80fb1fedea",
        "moduleUUID": "980ca3ae-fd69-43c1-b3cc-d71ea394b2eb",
        "moduleID": "CPU",
        "timestamp": 1589271373,
        "status": "GREEN",
        "type": "HealthAlert"
    },
```

FMC REST-APIs - /health/metrics

Verschiedene Filterkriterien:

- startTime und endTime: in Sekunden. Beide zusammen anzugeben. Alle zwischen den beiden Zeitpunkten generierten Metriken zurückgeben
- deviceUUID: Gibt alle Metriken für das angegebene Gerät zurück.
- metric: Gibt alle Metriken mit dem angegebenen Namen zurück (cpu, mem, disk)
- step: Schritt in Sekunden. Metrische Werte bei jedem Schritt in Sekunden.
- regexFilter: Regex-Filter für Metriknamen. (Beispiel: snort)

Beispiel für das Ergebnis



Beispiel für FMC REST-Eingang/Ausgang

Anforderungs-URL:

https://u32c01p12-vrouter.cisco.com:10213/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/health/metrics?filter=deviceUUIDs:c1f97434-d6dd-11ea-9df2dfc9e6fdf76d;metric:cpu;regexFilter:lina_cp_avg; startTime:1611294885.699;endTime:1611309285.699;step:60;

Antwort:

{

"Links":{

"Elemente":[{

"Antwort":{

"Status":"Erfolg",

"Daten":{

"resultType":"matrix",

"Ergebnis":[{

"metrisch":{

"__name__":"**CPU**",

"CPU":"lina_cp_avg",

"Instanz":"127.0.0.1:9273",

"Job":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",

"uuid":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d"},

"Werte":[

[1611309165,699,"0,5"],

[1611309225,699,"0,5"],

```
[1611309285,699,"0,5"]
```

```
]
}
]
}
"deviceUUID":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",
"metrisch":"CPU",
"regexFilter":"cpu=~"lina_cp_avg"",
"Typ":"Metrisch"
```

}

REST-APIs für FTD-Geräte

REST-API für FTD-Geräte /devices/default/operational/metrics	Beschreibung Alle Metriken auslesen. Momentane Werte von Metriken werden zurückgegeben.
/devices/default/operating/metrics/{objId}	Spezifische Metrik ausgeben, die von {objld} identifiziert wurde
/devices/default/operational/metricsschema	zurückgegeben werden gelöscht (erste Get-Anfrage) Ausgabeschema, das zurückgegeben wird, wenn
/devices/default/operating/metricsschema/{objld}	ein bestimmtes Die Metrik von übergebenem {objld} wird abgefragt.

REST-API für FTD-Geräte: GET-Metriken

Beispiel-Antworttext für Metriken

Curi
curl -X GETheader 'Accept: application/json' 'https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics'
Request URL
https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics
Response Body
<pre>{ "items": [{ "name": "mem.used_swap_snort", "metric": { "value": 0, "unit": "BYTE", "type": "numericdevicemetricvalue" }, "timestamp": 1592316305, "dateTime": "2020-06-16T14:05:05Z", "idetTime": "2020-06-16T14:05:05Z", "id": "mem.used_swap_snort", "type": "devicemetricdata", "links": { "self": "https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/mem.used_swap_snort" }, { rame": "mem.remaining_blocks_1550_bytes", "metric": { } // "metric": { } // "metric": { // "dateTime": "mem.remaining_blocks_1550_bytes", // "metric": { // "metric": {metric": { // "metric": { // "metric": { // "metric": { // "metric": {metric": { // "metric": {metric": {metric":</pre>
Response Code
200

REST-API für FTD-Geräte: GET-spezifische Kennzahl

Um eine bestimmte Metrik abzurufen, geben Sie deren Objekt-ID in der URL an. Die Objekt-ID ist das Namensfeld der Metrik.



Fehlerbehebung/Diagnose

Überblick über die Diagnose - Typischer Fehlerbehebungsablauf



Wichtige Befehle und Dateien zur Fehlerbehebung und Anmeldung am Gerät

Hinweis: In 7.0 NPI wird Port 9274 anstelle von 9273 erwähnt.

Befehl/Datei auf Gerät pmtool-Status grep hmdaemon curl localhost:9273/metrics curl localhost:9273/hm/ <metric Name> pmtool restartbyid hmdaemon /ngfw/var/log/hmdaemon.log</metric 	Wofür wird es verwendet? Überprüfen Sie, ob Telegraf auf dem Gerät ausgeführt wird. Dieser Befehl ruft alle Daten ab oder gibt Metriken aus telegraf aus. Ein leerer Ein-/Aus-Zustand bedeutet, dass das Telegramm nicht richtig funktioniert. So starten Sie hmdaemon neu Datei, in der Telegrafenprotokolle gespeichert werden. Die Datei die die Telegrafekonfiguration erfasst. Siehe Abschnitt zu
/ngfw/etc/sf/telegraf_api.conf	Die Datei, die die Telegrafekonfiguration erfasst. Siehe Abschnitt zu Telegraf-Konfigurationsänderungen.

Markierte Datei-/Befehlsausgabe in FMC enthalten Fehlerbehebung

Wichtige Befehle und Dateien zur Fehlerbehebung und Anmeldung bei FMC

Befehl/Datei auf FMC	Wofür wird es verwendet?
pmtool-Status grep Prometheus	Überprüfen Sie, ob Prometheus auf dem Gerät ausgeführt wird.
pmtool restartbyid Prometheus	So starten Sie Prometheus neu
curl localhost:9090/metrics	Prometheus. /metrics-Endpunkt würde seine eigenen Metriken zurückgeben.
curl localhost:9090/targets	HTML-Seite, die in Prometheus konfigurierte Ziele auflistet. Suchen Sie nach einem Textendpunkt. HTML-Seite mit allen aktiven Warnmeldungen. Es
curl localhost:9090/warnt	ist viel einfacher zu laden. Dies im Browser überprüfen und
curl localhost:9090/rules	HTML-Seite mit allen konfigurierten und akzeptierten Regeln. Dies kann anhand konfigurierter Regeln überprüft werden.
/var/opt/prometheus/	Verzeichnis, in dem alles Prometheus Zeug vorhanden ist
/var/opt/prometheus/devicehm.yml	Hauptkonfigurationsdatei für Prometheus Verzeichnis, in dem alle Ziele (ETD-
/var/opt/prometheus/targets/	Telegrafinstanzen) gespeichert sind. Dateien in diesem Verzeichnis werden erstellt, wenn Ziele

/var/opt/prometheus/rules/	von FMC erkannt werden. Verzeichnis, in dem alle Regeldateien gespeichert sind. Für jedes Gerät wird auf Grundlage der angewendeten Integritätsrichtlinie eine Regeldatei erstellt.
/var/opt/prometheus/data/	Die Datendatei enthält alle TSDB-Daten. "du -h ." in diesem Verzeichnis gibt den Speicher von Prometheus verwendet.
curl <target_ip>:9273/metrics /var/log/prometheus*</target_ip>	Abrufen von Metriken vom Gerät Prometheus-Protokolle

Hervorgehobene Datei-/Befehlsausgabe in Fehlerbehebung

Erfassen von Daten von (Gerät) - GUI

Daten für einen Zeitraum werden in GUI angezeigt

Wenn Prometheus nicht über Daten für den ausgewählten Zeitraum verfügt, zeigt die GUI im Dashboard-Bereich "No Data Available" (Keine Daten verfügbar) an:

Event Rate	
	No Data Available

Wenn Daten verfügbar sind, sieht die Grafik wie folgt aus:

Event I	Rate										
38k 28k				~		~			~		~
19k 9.5k											
0.0	04 04:09	04:14	04:19	04:24	04:29	04:34	04:39	04:44	04:49	04:54	04:59

Verwenden Sie die Browser-Registerkarten "Konsole" und "Netzwerk".

Browser-Konsolenprotokoll und Netzwerk-Anrufprotokoll

- In diesem Beispiel wird die Chrome-Browser-Entwicklerkonsole angezeigt.
- Im Fehlerfall werden die Ausnahmedetails im Konsolenprotokoll angezeigt.



Beispiel für ein Browser-Konsolenprotokoll

Console Tab Exception details					
R Elements Console Sources Network Performance Memory Application Security	Lighthouse Redux » 💁 3 🗛 1 🎄 🗄 🗙				
🕩 🛇 top 🔻 💿 Filter Default levels 🔻	\$				
v Validation using FMC HA State schema failed with 2 error(s)	validator.js:75				
<pre>> data.remote.status[2] = null should be string,number (per #/definitions/Status/properties/status/items/type)</pre>	react devtools backend.js:2430				
♥ bdta.remote.status[3] = null should be string,number (per #/definitions/Status/properties/status/items/type)					
▲ > Details > {data: {}, error: {}, schema: {}}					
Solution: Solution (a) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	react devtools backend.js:2430				
BaseLineChart - Render	BaseLineChart.js:376				
Baseline chart props changed	BaseLineChart.js:163				
undefined 0 100 100 undefined ▶ ({}] "area" undefined ▶ (2) [{}, {}] ▶ {type: "UTC_TIME", ran undefined 5	<pre>nge: e} "percent" undefined BaseLineChart.js:164</pre>				

Erfassen von Daten von (Gerät) - CLI

Aktivieren von Telegraf mit Debug-Modus in FMC

- 1. Wechseln Sie in den Expertenmodus für FTD, und melden Sie sich als Sudo-Root-Benutzer an.
- 2. Öffnen Sie die Datei /etc/sf/fmc_telegraf_api.conf im FTD.
- 3. Deaktivieren Sie die Option "debug".
- 4. Laden Sie Telegraf neu, indem Sie 'pmtool HUPByID hmdaemon' ausführen.
- 5. Telegraf läuft im Debug-Modus und gibt granulare Debug-Meldungen in der Datei /var/log/hmdaemon.log aus

Denken Sie daran, die "debug"-Option zu kommentieren, wenn fertig!

Einzelheiten zu Einschränkungen, häufige Probleme und Problemumgehungen

Implementierungshinweise

- Die Genauigkeit der Metrik hängt von der Häufigkeit der Abfrageinstanzen ab.
- Die maximale Datenauflösung für die Grafik beträgt 1440 (Dauer eines Tages). Wenn die Zeitspanne groß ist, sind einige Datenpunkte nicht sichtbar.
- Die Ausgabe der FTD Device REST API ist im JSON-Format.
- Die Ausgabe der FMC REST API ist im Prometheus-Format. Weitere Informationen zum Format Prometheus finden Sie unter

https://prometheus.io/docs/prometheus/latest/querying/api/

• Das Prometheus-Format ermöglicht Flexibilität bei der Integration externer Tools wie (Grafana)

Hinweis: Die CPU-Nutzungsmetrik ist in der FMC-Integritätsrichtlinie standardmäßig deaktiviert. Sie kann aktiviert werden, indem Sie die zugehörige Integritätsrichtlinie ändern.

Workarounds und Tipps

Anmerkung im Diagramm flackert am Ende des Diagramms.

• Bewegen Sie den Cursor langsam, um dieses Problem zu vermeiden.

Anmerkungen im Diagramm haben eine maximale Länge, die die angezeigten Daten begrenzt.

• Verwenden Sie in diesem Fall die im Metrikfenster verfügbare Filterfunktion.

Einschränkungen der Implementierung für Version 6.7

- Das Prometheus-Intervall für die Verschlüsselung aller Geräte und Metriken wird auf 1 Minute festgelegt.
- Das Prometheus-Abstreifintervall kann geändert werden, indem die Prometheus-Jamal-Datei auf dem FMC (/var/opt/prometheus/devicehm.yml) geändert wird.
- Die FTD API-Ausgabe ist im JSON-Format.
- Überwachung von FMC nicht unterstützt; nur FTDs
- Die Metrik für die CPU-Auslastung ist in der FMC-Integritätsrichtlinie standardmäßig deaktiviert. Sie kann aktiviert werden, indem Sie die zugehörige Integritätsrichtlinie ändern.

Was ist zu übermitteln, wenn ein Problem auftritt?

Zusammenfassung der Protokolle, die gesendet werden sollen:

- Screenshots der Benutzeroberfläche
- Protokolle von Prometheus und hmdaemon (siehe Abschnitt Fehlerbehebung/Diagnose).
- Dump der Prometheus-Datenbank (/var/opt/Prometheus/data directory)

Häufig gestellte Fragen

Frage: Ist dieses FMC nur verfügbar? Was ist mit FTD/FDM für die Benutzer, die zu CDO gegangen sind?

A: Dies ist nur FMC und die neue Benutzeroberfläche ist nur für FTD-Geräte unter 6.7.

F: Benutzerdefinierte Dashboards sind nur für Geräte in 6.7?

A: Die Dashboards sind nur für FTD-Geräte in 6.7.

Frage: Enthält diese Funktion gerätespezifische Merkmale? Ist es für IRGENDEINE Plattform, die FTD unterstützt, die all dies hat? Werden virtuelle Plattformen unterstützt?

A: Dies wird auch von virtuellen FTDv unterstützt. Es gibt mögliche gerätespezifische Variationen der Kennzahlen, die herangezogen werden. Die Funktion wird jedoch auf allen FTD-Plattformen unterstützt.

Frage: Gibt es mit der offenen API eine aktive Zusammenarbeit mit dem CDO-Team?

A: Mit "offene API" meine ich die REST-API. Die REST-API des FMC unterscheidet sich *von* der REST-API des FTD-Geräts. Die REST-API für FTD-Geräte ist bei der Verwaltung mit FMC nicht verfügbar. Nicht alle Funktionen in FMC verfügen über FMC REST APIs.

A: Die Infrastruktur für die REST-API des FTD-Geräts ist in Vorbereitung auf eine zukünftige Version vorhanden.

F: Die Download-Schaltfläche neben dem Zeitfenster (in der Nähe von "+") auf der Seite "Integritätsmonitor" würde den Integritätsbericht oder die Diagramme herunterladen, wie wir in diesem Fenster gesehen haben? Oder war es ein Widget?

A: In Bezug auf das Overlay-Symbol für die Bereitstellung, klicken Sie auf das Symbol Overlay Deployment Job, um die Zeit auf dem gewählten Diagramm auszulösen.

Interne Nachverfolgungsinformationen

CSC.content-security > sfims > ftd-plug-telemetrie, fmc_hm

- Verwendung von ftd-plug-Telemetrie zur Protokollierung von Fehlern im Zusammenhang mit FTD APIs und Telegrafen
- Verwenden Sie fmc_hm, um Probleme mit der FMC-Benutzeroberfläche und dem FMC-Backend zu protokollieren.
- FTD REST API => CSC.content-security > sfims > ftd-api-telemetrie
- EDCS-18385961

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.