Upgrade FP - Device Health Monitoring

Contents

Introduction	
Background Info	
Feature Overview	
Feature Details 7.0	
FTD: Metrics Introduced in FP 7.0	
Feature Details 6.7	

Introduction

This document describes the new Device Health monitoring feature added in 6.7 and 7.0 releases.

Background Info

The problem:

The health monitoring system provides visibility into device's performance for reactive debugging and proactive actions.

Comprehensive visibility and analysis is obtained by:

- Trend charts for key metrics
- Event Overlay
- Customizable dashboards
- Unified health monitoring architecture see same data for all managers
- Lot of new metrics and extensibility of metrics to add many more

What's New in 7.0 release

What's new or different compared to FP 7.0

- FMC Dashboard with HA support
- 110+ new metrics for FTD
- Health alert for FTD split brain scenario
- Custom run time interval for newer health metrics

Benefits

- Aids in system debugging by providing ability to correlate data from different sub-systems and resources on device
- Visibility to various system performance metrics
- Capacity planning

New on 6.7

New or different compared to the release immediately preceding (high-level):

- New user interface for device health monitoring on FMC
- FTD Device REST API: device-metric API: A lot of new metrics added
- FMC APIs: New APIs: health alerts, health metrics and deployment details
- High-level marketplace overview, real world applications
- Aids in system debugging by providing ability to correlate data from different sub-systems and resources on device
- Visibility
- Capacity planning

Feature Overview

How it Works

- Device Health Monitoring in FP 7.0
- New health dashboard for FMC which provides Trend charts, overlays and custom dashboards
- New FTD metrics available in FTD dashboards
- 110+ metrics covering 12 categories
- FTD APIs: makes metrics available to query by external entities

Under the hood,

• Collects the health of a device with Telegraf (an open-source metric collection framework)

Additional Notes

Health monitoring data is available

- In the FMC Health Dashboard, accessible from the system menu (System > Health > Monitor)
- From the FMC REST API
- When the device is managed by FDM, via the FTD Device REST API

Some of the metrics (both FMC and FTD) are disabled by default

• Health modules in Health Policy need to be enabled and deployed for some metrics to appear.

Implementation of enhancements requested by FP 6.7 IFT'ers

- Auto refresh by default
- Filter with custom time range on dashboard
- Select interfaces by user-defined name (as well as physical interface name) in the interface selector
- Cross launch device dashboard from Health Monitor 'Home' page

Device Health Monitoring in FP 6.7

- New UI on FMC which provides Trend charts, overlays and custom dashboards.
- FTD APIs: makes same metrics available to query by external entities

Summary of Limitations:

- The feature is not supported on FDM GUI or CDO
- Monitoring FMC itself within the new health monitoring UI is not supported.
- Poll intervals are not configurable. You cannot configure different poll intervals for different devices. All are polled at fixed one-minute interval.

Deployment Examples

- No Specific deployment needed to test the feature. Just upgrade FMC and device to FP 6.7.
- Health monitoring data is available in the FMC health dashboard, accessible from system tab.



Prerequisites and Supported Platforms

Minimum Supported Software and Hardware Platforms

Min Supported Manager Version	Managed Devices	Min Supported Managed Device Version Required	Notes
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	Supported only on FTDs
FTD Device REST API	FTD 6.7	FXOS 2.9.1 FTD 6.7	FTD Device REST API only (not FDM or CDO GUIs)

Interoperability

No specific requirements for interoperability.

Feature Details 7.0

FMC UI: Standalone and HA Support

Health Monitoring Page Navigation

FMC CISCO Monitor Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	0	۵	Ø syed▼
Monitoring In Home FMC Active FMC Standby FMC Devices (2) 192.168.0.216 9 192.168.0.217	Health S	tatus 2 critical ices ices ice iC_Active IC_Standby 2.168.0.217	0 warnings	1 normal	1 disabled	C. Filter ut	ing device	name	C		

- Standalone FMC is shown as a single node
- FMC HA shown as a pair of nodes
- Each FMC is shown with health status

Health Status

- FMC HA is shown in twin-hexagon.
- FMC Active and Standby devices are listed in the alert table as well.

FMC Dashboard

FMC Health Monitoring Dashboard in 7.0

Firepower Manage System / Health / Monitor	ment Cen	nter ov	erview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deplo	w Q 📀 🛱	g syed▼
Monitoring () 없 Home	Health: F View System Overview	MC_Activ & Troubleshoo Process	e 🕒 Critica t Details	al						2	Select 020-12-08 04:04 -	2020-12-08 05:04
	High Availa	ability					Manage HA	Event Rate	3			
 Standby FMC Devices (2) 192.168.0.216 192.168.0.217 	Primar	y- Active	Last s	Degraded ync: a few sec d- Synchroniza	onds ago tion incomplete	e Second	ary- Standby	38k 28k 19k 9.5k 0.0 04.04	04:09 04:14 04:19 04:24	I 04:29 04:34 04:	39 04:54 04:59	04:54 04:59
	Process He	ealth		(Critical Proce	esses A	II Processes	Event Capa	acity			Configure
	ActionQ	DCCSM	ESS	Msg Service	Perl MsgHandler	Pruner	RabbitMQ	c	Intrusion 39 days 3 hrs 14 mi	ins .		526.79K/1M 0/1M
	SEDC	SF Data	Sync D	Torncat	Provisioning	ADI	Disk	Security In	ntelligence 57 days 3 hrs 13 mi	ina ina		100K/1M
	Mojo	Monet DB	Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Connection	Summary No Events			0/1M
									Malware No Events			0/2M
	sftunnel	SLA		Sybase Arbiter	Symmetrie	c Syb	ase DB		User No Events			0/1M
	CPU 100% 75% 50% 25% 0%	04:09 04:14	04:19 04:24	0129 013	4 04:39 04:	Avg CP	U ~	Memory - 100% 75% 50% 25% 0%	Used	4 04.29 04.34 04	39 04/4 04/9	0454 0459
	Interface - #644.3K 133.2K 11.1K 0 04.54	Input Rate	Output Ra	ate	4 06:39 04:	64 C4:49	D4:54 04:59	Disk Usage	e Entire Disk		Critical Partitio	ons

Summary view of:

- High Availability
- Event Rate and Capacity
- Process Health
- CPU
- Memory
- Interface
- Disk

This dashboard is available to both Active and Standby FMCs. User can create custom dashboards to monitor metrics of their choice.

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 0 0 21 Top 5 Alerts File system integrity check FMC HA Status Host Limit Classic License Expiration Monitor AMP for Endpoints Status

HA Panel shows

- Current HA status
- Active vs. Standby
- Last sync time
- Device Health

FMC Dashboard: Event Rate and Capacity

Event Rate

- Maximum event rate as base line
- Overall event rate FMC receives

Event Capacity

- Current consumption by event categories
- Retention time of events
- Current vs. Maximum

event capacity

• Capacity overflow marker

Health: Fl View System & Overview	MC Orit & Troubleshoo Process	tical ot Details s											Last 2021-	1 hour -02-22	r 06:32 - 2	021-02	-22 07:3; -22 +
Process He	alth			Cri	tical Proce	sses A	II Processes	Event Capacity Connection	3 days 16 hrs 3 r	nins					1	Co 1/1M	nfigure
ActionQ	DCCSM	ESS	Msg Service	Perl MsgHandler	Pruner	RabbitMQ	SFDC Notifier	Intrusion File	No Events						0	0/1M 0/1M	
SF Data Correlator	Sync D	Tomcat	Provisioning Process	ADI	Disk Manager	Mojo	Monet DB	Security Intelligence	No Events							0/1M	
Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Sftunnel	SLA	Sybase Arbiter	Malware	No Events							0/2M	
Symmetric				Sybase DB	1			User	No Events No Events						(0/1M 0/1M	¥
CPU Data col shown.	llection for C	CPU modul	e is disabled	in the healt	h policy, p	Avg CP artial or no	U 🗸	Event Rate 5.0k 3.8k 2.5k 1.3k 0.0 06:35 06:40	06:45 06:50	06:55	07:00	07:05	07:10	07:15	07:20	07:25	07:30

FMC Dashboard: Event Capacity

Normal Event Capacity Consumption State

Normal:				
Connection	182 days 4 hrs 23 mi	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
0	2020-09-18 14:28:30			
Connection	18h	2 Sk/min	118245455/10000000	11.6 M / 10 M
	Retention Duration	Incoming Rate	Capacity 🛆 🔫	

Overflow scenario, when events are stored beyond the configured maximum capacity.

- Bold text indicates overflow
- A warning icon highlights the capacity overflow

FMC Dashboard: FMC Process Panel

Critical processes panel shows

- Process current state
- Process restart count

rocess He	ealth					Cri	tical Proc	cesses A	All Processes
ActionQ	DCCSM	ESS	Msg Service	Perl MsgHandle	Pruner r		RabbitMC	SFDC Notifier	SF Data Correlator
Sync D	Tomcat	Provisioning Process	ADI	Disk Manager	Mojo		Monet DB	3 Mongo DB	MySQL DB
Run HM	SFIP Proxy	SF Mgr	Sftunne	I SLA		Syba Arbi	ase ter	Symmetric	Sybase DB

The process panel shows these metrics for all 'pmconfig' processes:

- Current State
- CPU Usage
- Memory Usage

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	1.49KB
ESS	Running	0.1	448	3.26KB
Event DS	Running	0	34	4.59KB

FMC Dashboard: FMC CPU

CPU Panel shows

- Average CPU (default)All Cores





FMC Dashboard: Other Panels

Memory panel shows overall memory usage on FMC



Interface panel shows input/output rate of average of all interfaces



Disk panel shows

- Entire disk capacity
- Critical partition capacity where FMC data is stored



Run Time Interval

- Run time interval for old health module is renamed as 'Legacy Run Time Interval'
- 'Run Time Interval' targets the new Telegraf based health modules
- Global setting, affects all devices

cisco Edit Overview Analys	is Policies	Devices	Objects	AMP	Intelligence	Deplo	γQ	0	¢	0	admin 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Polic	cy: Initial_H	ealth_Polic	y 2021-(01-29 04:40:4	9					Alerts
AMP For Endpoints Status AMP for Firepower Status ASP Drop	Poli	Policy Name cy Description	Initial_Hea	alth_Policy Ith Policy	2021-01-291						
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status	Run Time Note : Changes	n Time Interval (mins) Interval (mins) to Run Time Int	5 1 erval will restar	t the health							
Backlog Status CPU Usage (per core) CPU Usage Data Plane											
CPU Usage Snort CPU Usage System Card Reset					Cancel	Save Policy and Ex	C.				
Chassis Status FTD Cluster/Failover Status Configuration Database											
Connection Statistics Critical Process Statistics Deployed Configuration Statistics Disk Status											
INTER DECEM											

Available Metrics

Metrics Available for Custom Dashboards

- If a user wants to make a custom dashboard, these slides are a guide to available metrics.
- Some metrics have to be enabled in Health Policy before they can used in a Custom Health Dashboard

CISCO Edit Overview Analysis	Policies	Devices	Objects	AMP	Intelligence	De	ploy	٩	¢	¢	0	syed •
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Policy: [en_US/admir	: Initial_He n:policy_la	alth_Policy	/ 2020-1 d])	2-08 08:49:46) (Last Modified:						Alerts
AMP for Firepower Status ASP Drop	F Policy	Policy Name Description	Initial_Heal	h Policy	2020-12-08 (
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status		Description	Monitors CPU cores, thresho applicable to	J usage on a old set here all the cores	ull the will be							
Backlog Status	Critical 1	Enabled Threshold %	● On ○ O. 90	ſſ								
CPU Usage Data Plane	Warning 1	Threshold %	80									
CPU Usage Short CPU Usage System					Cancel	Save Policy and Ex	sit					
Card Reset Chassis Status FTD												
Cruster/Failover Status Configuration Database												
Connection Statistics Critical Process Statistics												
Deployed Configuration Statistics Disk Status												
Disk Usage Event Stream Status												
FMC Access Configuration Changes												

FMC UI: FMC Custom Dashboard

New FMC Monitoring Metrics categories in 7.0

- CPU
- Memory
- Interface
- Disk
- Event
- Process
- RabbitMQ
- Sybase
- MySQL

Health: FN View System & Overview	AC Crit Troubleshoo Process	tical t Details	S	Last 1 hour C 2021-02-22 07:07 - 2021-02-22 08:07
Process Hea	alth		Critical Processes All Processes Event Capacity	Configure
ActionQ	DCCSM	ESS	Add Dashboard • * * * *	1/1M 0/1M
SF Data Correlator	Sync D	Tomca	Name*	0/1M
Mongo DB	MySQL DB	Run H	my_custom_dashboard	0/1M 0/2M
Symmetric			Chosen metrics will be displayed as portlets in the dashboard.	0/1M 0/1M
CPU			Add Metrics	
			Cancel Add Dashboard	

FMC UI: FMC Metrics

40 metrics added across different categories (available in custom dashboard). In order enable the disabled metrics, enable the corresponding health module in the associated health policy (**System > Health > Policy**).

Metric Group Name	Enabled by default	Description
CPU	No	Monitors FMC CPU
Memory	Yes	Monitors FMC Memory
Disk	Yes	Monitors FMC Disk Usage
Interface	Yes	Monitors FMC Interface
Process	Yes	Monitors FMC processes
Event	Yes	Monitors Event Rate
MySQL	No	Monitors MySQL
RabbitMQ	No	Monitors RabbitMQ
Sybase	No	Monitors Sybase

FTD: Metrics Introduced in FP 7.0

Enabled by default: Metrics are collected by default. In order enable the disabled metrics, enable the corresponding health module in the associated health policy (System > Health > Policy).

Metric Group Name	Enabled by default	Description	Platform		
Chassis Status	Yes	Monitors different Chassis parameters like Fan speed, and temperature.	Applicable to only FPR2100 and FPR1000 platforms		
Flow offload Yes S		Monitors hardware flow offload statistics	Applicable to FPR9300 and FPR4100 platforms		
ASP drops	Yes	Monitors Lina side packet drops	All		
Hit counts No		Monitors hit counts for Access Control Policy Rules	All		
AMP Threat Grid Status	Yes	Monitors connectivity to AMP ThreatGrid	All		
AMP Connectivity Status No		Monitors AMP cloud connectivity from the FTD	All		
SSE connector status No		Monitors SSE cloud connectivity from the FTD	All		
NTP Status No		Monitors NTP clock synchronization parameters on the FTD	All		
VPN statistics	Yes	Monitors S2S and RA VPN Tunnel statistics	All		
Route statistics	Yes	Monitors Lina side packet drops	All		
Snort 3 perf stats Yes		Monitors certain Snort3 performance statistics (perfstats)	All		
xTLS counters	No	Monitors xTLS/SSL flows,	All		

	memory and cache effectiveness	
--	--------------------------------	--

REST APIs, Syslog, SNMP

No new FMC or FTD Device REST APIs have been introduced in 7.0. The existing REST APIs support new metrics added in 7.0.

Syslog and SNMP

Syslog

• No change in syslog for health monitor

SNMP

• Separate TOI for "SNMP Device Health Monitoring"

SAL/CTR/3rd Party product integration

- Separate TOI for 'Azure Application Insights' support
- No specific change done to support integrating 'Health Monitoring' with SAL/CTR/SecureX
- REST API can be leveraged for 3rd party integration

Software Technology

Feature Details 6.7

New NGFW Health Monitoring for FTD Health and Performance

Helps users with

- Reactive debugging, like root cause analysis the problem after it has happened
- Proactive actions such as monitoring usage and saturation levels to identify potential capacity issues and thereby helping users to do capacity enhancements or refactoring.

Highlights

- **Trend charts**: Trend charts make it very easy to detect anomalies and determine a root cause of issues. With visual inspection trends can be spotted and correlations can be plotted between different metrics to find causal relation between them.
- **Event overlays**: Event overlays show important information, such as config deployment and SRU updates on trend charts to indicate causal relationships.
- **Customizable dashboards**: Users can make their own dashboards to group metrics they wish to see together on one page.
- Unified Health monitoring architecture: Single point of collection and export for metrics irrespective of which manager is "interested" in the metrics. FTD APIs as well as the FMC use data from the same metrics collector.
- **Extensibility of metrics**: One of the goals of the architecture for the platform was to be able to easily add new metrics. This is achieved by using Open Source metrics collection and storage tools and with customizable dashboards.

FMC GUI

FMC UI: Navigate to Health Status

On FMC, click on the **System** icon > **Health** > **Monitor** to navigate to the **Health Status** page.



FMC UI: New Health Status Page

The Health Status page is designed to show a health overview of all the devices that the FMC manages, including the health of the FMC.

- Devices are grouped as per their group/ha/cluster.
- A dot to the left of the device indicates its health
- Green no alarms
- Orange at least one health warning
- Red at least one critical health alarm
- Health summary is shown when hovering at the hexagon that represents the device health.
- Thresholds for warningand critical can be configured in health policy, in the same way it was done pre-FP 6.7.

Monitoring 😑	Health Alerts
ល់ HOME	7 total 1 critical 2 warnings 5 normal 0 disabled Search a device X V
 FMC Devices (5) Asia Responses (UA) 	FMC Asia ungrouped 192.168.0.26 - Warning
 Bangalore (HA) bangalore-main 	Device Alerts: 3.0 A 2 0 21
bangalore-standby	FNC A CPU used by sustain
chennai	o bangalore-main O Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalore-standby budget of the Link Momarch Alarms Local Malware Analysis
A 192.168.0.25	Clickto view more details
A 192.168.0.26	> 📀 mumbai
	> 🔺 192.168.0.25
	> 🔺 192.168.0.26

FMC UI: Device Health Events

Click the device in the bottom panel to display the health events associated with the device Alerts are sorted by their health status (severity).

Health monitoring page

>	▲ 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
	O CPU Usage Using CPU01 1%	Jun 23, 2020 2:53 AM
	O CPU Usage Using CPU02 0%	Jun 23, 2020 2:53 AM
	CPU Usage Using CPU00 0%	Jun 23, 2020 2:54 AM

FMC UI: FMC Health Monitoring is Unchanged

The FMC health page is still the legacy page. The new UI is supported only for FTD with 6.7+

Monitoring	Health	Monitor Applance vimc-10	Generate Troubleshooting Files Advanced Troubleshooting		Nermal (55.05%) -	Module Status Summary Cluster Recover
	Alert D	etail (vfmc-10)				
		Alert		Time	Description	
	•	Process Status		2020-06-18 08:50:44	All processes are running correctly	
	0	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 UI: New! Device Dashboards

- Click the device name in the left pane to get to the device's health overview page.
- The health overview has all the key health metrics trend charts.
- Various time ranges are available (default to last 1 hour)
- Auto-refresh to reload the graph

Monitoring 📄	Health: 192.168.0.25 Warning View System & Troubleshoot Details	Last 1 hour S 2020-06-23 01:58 - 2020-06-23 02:58
ନ୍ତି HOME	Overview CPU Memory Interfaces Connections Snort	± +
 FMC Devices (5) 	CPU LINA Avg 1.5 % Snort Avg 0.7 % System Avg 17.5 % 1 core 12 % - 2.6 % 2 cores 0.5 % - 1.0 % 1 core 15.0 % - 24.0 %	Memory Snort Avg 28.1% System Avg 68.8% 2,9608 80.8% 2,9608 68.8% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 69.4% 2,9608 2,9608 2,9608
 Asia Bangalore (HA) bangalore-main 		60 Cotest
 bangalore-standby chennai 	20Creat	20
 e mumbai ✓ ungrouped 	0.0 91.45 01:50 01:55 02:00 02:05 02:15 02:20 02:25 02:30 02:35 02:40	0.0 01:45 01:50 01:55 02:00 02:05 02:10 02:15 02:20 02:25 02:00 02:25 02:40
A 192.168.0.25	Throughput Avg Data Interfaces V	Connection Statistics
▲ 192.168.0.26	In put Rate Avg 0 0-0 Output Rate Avg 0 0-0	Connections Avg 0 0 - 0
	800 400 300 100 0 0 145 0150 0155 0200 0255 0210 0215 0220 0225 0230 0235 0240	100 80 40 20 8.0 01/45 01.55 01.55 02.05 02.15 02.15 02.25 02.25 02.25 02.49
	Disk Usage	AMP Java LINA SF Data Correlator Shunnel SSE Connector Snort01 Snort02 <
	How To	

FMC UI: Deployment data overlay

Click the deployment icon to show deployment overlay details on the graph w.r.t selected time range

- Icon indicates the number of deployments during the selected time-range
- Band appears to indicate deployment start and end time.
- In case of multiple deployments, multiple bands/lines appear
- Click the icon on top of the dotted line to show the details

	Health: 192 View System & Tr Overview	.168.0.21 ON oubleshoot Details CPU Mem	ormal ory Interfaces	Connections	Snort	Last 1 hour 2020-06-23 02:26 - 2020-06-23 03:26 +	
	CPU LINA Avg 0.6 1 core 0.5 % - 1.6 100 	8 Snort Avg 0.9 9 cores 0.0 % - 8	% System Avg 11 5 % 1 core 13.0 % -	6.0 % -75.0 %	03.00	Critical Warning Warning 03.05 03:10 03:15 03:20 03:25	
CPU LINA Avg 2.7 % Snort 1 core 0.5 % - 7.8 % 2 cores 0 100 80 	Avg 3.7 % System 0 % - 10.5 % 1 core	n Avg 19.1 % 14.0 % - 30.0 %		Cristen Warning Jun 2	CPU LINA A 1 core 01 100 	Vig 2.7 % 3 t - 62 ts Snort Avg 4.3 % 2 cores 0.0 % - 15.5 % System Avg 20.5 % 1 core 1 core 14.0 % - 78.0 % Vig Deployed Policies Interface Policy Access Control Policy Preditive Policy Interface Policy Interface Policy Interface Policy Deployed Policies Interface Policy BGP Routing Policy BV Downs BV Interface Routing Policy BV Downs BV Multicast Boundary Filter Policy Multicast Routing Policy Advanced Settings OSPF Routing Policy Virtual Routor Virtual Routor	0059 Werno 2020 Jun 2 :rfaces

FMC UI: Device Pre-Built Dashboards

- There are pre-built health dashboards present in the FMC UI.
- These pre-built dashboards come with related metrics grouped together.
- The interface dashboard has trend chart for all interface-related metrics such as input/output bytes, packets, and average packet size for different interfaces.

He	Health: wm-101 📀 Normal						
View	/ System & T	roubleshoot D	etails				
٥v	verview	CPU	Memory	Interfaces	Connections	Snort	
_							
Int	erface - In	put Bytes, O	Output Bytes				
Bps	1.6K						
es ir							
valu	1.2K						
	800						
	400						
	0						
-							
		07:45		07:50	07	:55	08:00
Int	erface - In	put Packets	, Output Pack	ets, Drop Pack	ets		
1	00						
	80						

FTD Snort Memory - From where does it originate?

Firepower Manage CISCO System / Health / Monitor	ement Cente	Overviev	w Analy	rsis Poli	cies De	evices (Objects	AMP Ir	telligence		Dep	loy Q	6 ⁰⁰ ¢	Global \ mzafeiro ¥
Monitoring	Health: mza View System & Tr	feiro_FTD1 oubleshoot Deta	150-1 (Act)	ve) 🖉 Norma	al							La 202	st 1 week 21-10-05 10:	2021-10-12 10:59
යි Home	Overview	CPU M	/lemory	Interfaces	Connectio	ons Sno	ort ASP	drops						MA
FMC		_												
 Devices (8) 	Memory - Ma	iximum Data P	lane, Data Pl	ane										
√ cisco	5.7 GB													
mzafeiro_FP4100_8	4.1 GB													
	3.3 GB													
A 10.62.148.228	2.5 G8													
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
KSEC-FPR4145-1-2	Memory - Ma	ximum Snort	Snort											
✓ mzafeiro_FP1150-HA	20.2 GB	ixintani onort,	onore					2021-	10-08 22:15 059	T				
e mzafeiro_FTD1150-1 Ac	10.3 GB							Ma So	ximum Snort 20.2 srt 4.7	GB GB				
mzafeiro_FTD1150-2 s	12.5 GB													
mzafeiro_FTD4115-2	8.6 GB													
Sami_10.62.148.194	4.7 GB							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 - Sv	stem Lised. To	tal											
	31.4 GB	510m 0000, 10	001											
	25.8 GB													
	20.2 GB													
	14.6.GR													•

FMC UI: Custom Dashboards Can Be Created

Users can create their own Custom dashboard

- In addition to pre-built dashboards, a user can also create custom dashboards.
- In custom dashboard, any number of metrics can be added.
- Typically, a custom dashboard would be created if metrics from different metric groups could be correlated to arrive at the root cause of a problem.
- In case of high Lina CPU, one is able to see incoming Connection Per Second (CPS), interface stats (and so on) which can cause the CPU to go high.



FMC UI: Create a Custom Dashboard

Correlate Metrics Dialog

- When a user clicks "+" to create a custom dashboard, the Correlate Metrics window opens.
- A user can add different metrics which the user wants to monitor together.

Correlate Metrics		×
Correlate the metrics that are in custom to specify your own me Correlation Group*	ter-related. Select predefined correlation trics.	ation groups or
CPU - Snort		\sim
Hide Details Dashboard Name*		
Correlation-CPU-Snort		
Metrics Chosen metrics will be displaye CPU \checkmark	d as portlets in the dashboard.	X V T
Interface \lor	Input Packets X	× ~ T
Deployed Configuration \lor	Number of rules X	× ~ T
Deployed Configuration \lor	Number of ACEs X	× ~ T
Add Metrics		
	Car	ncel Add

Gathering Data from (device) - GUI

Data for a Time Range Showing in GUI

T

When the Health Monitor does not have data for the selected time range, GUI shows 'No Data Available' in the dashboard panel:

Event Rate	
	No Data Available

In case of data available, graph appears like this:



Use the Browser's Console and Network Tabs

Browser Console log and Network call log

- In this example, the Chrome browser developer console is shown
- In case of error, exception details are shown in the console log

Gisco System / Health / Monitor	nent Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy 9, 🥏 🔅 🚳 syed 🔻
Monitoring	Overview CPU Memory Interfaces Connections Short ASP drops
	CPU Memory
€ Home	Data Plane Avg 0% Snort Avg 1% System Avg 15% Data Plane Avg 76% Snort Avg 21% System Avg 45% Data Plane Avg 0% Data Plane Avg 76% Data Plane Avg 76% Snort Avg 21% System Avg 45%
V FMC	100% 100% 100%
FMC - Active	73% 73%
FMC - Standby	50%50%
 Devices (2) 	
192.168.0.219	0%
✓ FTD-HA	Dec 13 Dec 14 00:59 01:59 01:59 02:59 02:59 03:29 Dec 13 Dec 14 00:59 01:59 02:59 02:59 03:29
192.168.0.216	Throughput Avg - all interfaces Connection Statistics
4 192.168.0.217	Input Rate Avg 1.34Kbps Output Rate Avg 2.03Kbps Connections Avg 4 NAT Translations Avg 0 0 0 0
	433hps - 2.24Kbps 803hps - 2.37Khps 10
	1 2x 7.5 1.3x 668 2.5
*	0 0.0
	Dec 13 Dec 14 00:59 01:59 02:59 02:59 03:29 Dec 13 Dec 14 00:59 01:29 01:59 02:59 03:59
	s Network Pendimiande Memory Application Security Lighthouse Hedux is Components is Promer vs = 3b4 vs : A
in Radein lat Root <u>/index.ist30</u>) in Suspense lat Root <u>/index.ist30</u> in Root (at application.jst37) in MessageProvider (at TrastProv in ToastProvider (at Provider.jst37) in MessageProvider lat Provi in Router lat Provider.jst34) in InputModerProvider lat Provi in ThemeProvider lat Provide in IntegrationProvider lat Provide in IntegrationProvider lat Provide in ConnectFunction (at Provider. in ConnectFunction (at Provider. in ConnectFunction (at Provider. in Provider (at LocaleProvid in LocaleProvider (at LocaleProvid in ReactQueryCacheProvider (at Q in QueryCacheProvider (at Provider. in StrictMode (at application.jst3 in StrictMode (at application.jst3)	Imm Decade errors j) ider, js:80) i36) der, js:33) r, js:33) der, js:32) nectFunction) js:31) js:11) er, js:29) nnectFunction) js:31) er, js:28) er, js:21) er, js:28) er, js:21)
<pre></pre>	index.jsil

Browser Console Log Example

Console Tab Exception det	tails	
Elements Console Sources Network Performance Memory Application	Security Lighthouse Redux » 📀 3 🗛 1 🔅 🕻 🗙	
🕩 🚫 top 🔻 🥑 Filter Defailt levels 🔻	\$	
v Validation using FMC HA State schema failed with 2 error(s) validator.js:75		
<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>		
<pre>>> bata.remote.status[3] = null should be string,number (per #/definitions/Status/properties/status/items/type)</pre>		
▲ >Details > {data: {}, error: {}, schema: {}}	react devtools backend.js:2430	
S ►► {message: "validation failed", errors: Array(2), validation: true, ajv: true} react devtools backend.js:2430		
BaseLineChart - Render BaseLineChart.js:376		
Baseline chart props changed BaseLineChart.js:163		
undefined 0 100 undefined ▶ [{}] "area" undefined ▶ (2) [{}, {}] ▶ {type: "UTC_TIME", range: e} "percent" undefined BaseLineChart.js:164		
and the second sec	- · · · · · · · ·	

References

FMC Health Monitoring - 6.7