Actualizar FP: supervisión del estado de los dispositivos

Contenido

Introducción Información de fondo Descripción general de características Detalles de la función 7.0 FTD: Métricas introducidas en FP 7.0 Detalles de la función 6.7

Introducción

Este documento describe la nueva función de monitoreo de estado del dispositivo que se agregó en las versiones 6.7 y 7.0.

Información de fondo

El problema:

El sistema de supervisión de estado proporciona visibilidad del rendimiento del dispositivo para la depuración reactiva y las acciones proactivas.

La visibilidad y el análisis completos se obtienen mediante:

- Gráficos de tendencias para métricas clave
- Superposición de eventos
- · Paneles personalizables
- Arquitectura de supervisión de estado unificada: vea los mismos datos para todos los gerentes
- Muchas métricas nuevas y capacidad de ampliación de métricas para añadir muchas más

Novedades de la versión 7.0

Novedades o diferencias con respecto a FP 7.0

- Panel FMC compatible con HA
- Más de 110 nuevas métricas para FTD
- Alerta de salud para el escenario de fractura cerebral del FTD
- Intervalo de tiempo de ejecución personalizado para las métricas de estado más recientes

Beneficios

- Ayuda en la depuración del sistema al proporcionar la capacidad de correlacionar datos de diferentes subsistemas y recursos en el dispositivo
- Visibilidad de las distintas métricas de rendimiento del sistema
- Planificación de capacidad

Nuevo en 6.7

Nuevo o diferente en comparación con la versión inmediatamente anterior (alto nivel):

- Nueva interfaz de usuario para la supervisión del estado de los dispositivos en FMC
- API REST de dispositivos FTD: API métrica de dispositivos: se han añadido muchas métricas nuevas
- API de FMC: nuevas API: alertas de estado, métricas de estado y detalles de implementación
- Descripción general de alto nivel del mercado, aplicaciones reales
- Ayuda en la depuración del sistema al proporcionar la capacidad de correlacionar datos de diferentes subsistemas y recursos en el dispositivo
- Visibilidad
- Planificación de capacidad

Descripción general de características

Cómo funciona

- Supervisión del estado de los dispositivos en FP 7.0
- Nuevo panel de salud para FMC que proporciona gráficos de tendencias, superposiciones y paneles personalizados
- Nuevas métricas de FTD disponibles en paneles de FTD
- Más de 110 indicadores que abarcan 12 categorías
- API de FTD: permite que entidades externas puedan consultar las métricas.

Debajo del capó,

 Recopila el estado de un dispositivo con Telegraf (un marco de recopilación de métricas de código abierto)

Notas complementarias

Se dispone de datos de supervisión de estado

- En el panel de estado de FMC, al que se puede acceder desde el menú del sistema (Sistema > Estado > Monitor)
- Desde la API REST de FMC
- Cuando FDM administra el dispositivo, mediante la API REST de dispositivo FTD

Algunos de los indicadores (tanto FMC como FTD) están desactivados de forma predeterminada

• Los módulos de estado de la política de estado deben activarse e implementarse para que

aparezcan algunas métricas.

Aplicación de las mejoras solicitadas por los responsables de FP 6.7 IFT

- · Actualización automática predeterminada
- Filtro con intervalo de tiempo personalizado en el panel
- Seleccione las interfaces por nombre definido por el usuario (así como por nombre de interfaz física) en el selector de interfaz
- Inicio cruzado del panel del dispositivo desde la página de inicio de Health Monitor

Supervisión del estado de los dispositivos en FP 6.7

- Nueva interfaz de usuario en FMC que proporciona gráficos de tendencias, superposiciones y paneles personalizados.
- API de FTD: permite que entidades externas puedan consultar las mismas métricas

Resumen de limitaciones:

- La función no es compatible con la GUI o CDO de FDM
- No se admite la supervisión del FMC en sí dentro de la nueva interfaz de usuario de supervisión de estado.
- Los intervalos de sondeo no se pueden configurar. No puede configurar diferentes intervalos de sondeo para diferentes dispositivos. Todos se sondean en intervalos fijos de un minuto.

Ejemplos de implementación

- No se necesita una implementación específica para probar la función. Simplemente actualice FMC y el dispositivo a FP 6.7.
- Los datos de supervisión de estado están disponibles en el panel de estado de FMC, al que se puede acceder desde la ficha del sistema.

	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
l		

Requisitos previos y plataformas admitidas

Plataformas de hardware y software admitidas mínimas

Versión mínima del administrador admitido	Dispositivos gestionados	Versión mínima de dispositivos administrados admitidos requerida	Notas
CSP 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	Sólo se admite en FTD
API REST de dispositivo FTD	FTD 6.7	FXOS 2.9.1 FTD 6.7	Sólo API REST de dispositivo FTD (no son GUI de FDM o CDO)

Interoperabilidad

No existen requisitos específicos de interoperabilidad.

Detalles de la función 7.0

FMC UI: independiente y compatibilidad con HA

Navegación por la página Supervisión de estado

CISCO FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	0	۵	Ø sye	d 🕶
Monitoring 10 Home FMC Active FMC Standby FMC Devices (2) 192.168.0.216 9 192.168.0.217		Health S	Ac_Active 2.168.0.217	0 warnings	1 normal	1 disabled	Q Filter u	sing device	: nam	0			

- FMC independiente se muestra como un nodo único
- · FMC HA se muestra como un par de nodos
- Cada CSP se muestra con el estado de mantenimiento

Estado de salud

- FMC HA se muestra en hexágono doble.
- Los dispositivos FMC activos y en espera también se enumeran en la tabla de alertas.

Panel de FMC

Panel de supervisión de estado de FMC en 7.0

Firepower Manage System / Health / Monitor	ement Cer	nter ov	erview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	० 📀 🌣	Ø syed▼
Monitoring (重) 얇 Home	Health: F View System Overview	MC_Activ & Troubleshoo Process	e 🔒 Critica t Details	al						Sele 2020	ect -12-08 04:04 -	2020-12-08 05:04
V FMC	High Availa	ability					Manage HA	Event Rate	9			
 Active FMC Standby FMC Devices (2) 192.168.0.216 192.168.0.217 	Primar	y- Active	Last s	Degraded tync: a few sec d- Synchroniza	onds ago tion incomplete	e Second	ary- Standby	38k 28k 18k 9.5k 0.0 04:04	04:09 04:14 04:19 04:24	04:29 04:34 04:39	04:14 04:19	04:54 04:59
e formonie fr	Process H	ealth		(Critical Proce	esses A	II Processes	Event Cap	acity			Configure
	ActionQ	DCCSM	ESS	Msg Service	Peri MsgHandler	Pruner	RabbitMQ	(Connection 59 days 3 hrs 14 mins Intrusion No Events			526.79K/1M 0/1M
	SFDC Notifier	SF Data Correlator	Sync D	Torncat	Provisioning Process	ADI	Disk Manager	Security I	ntelligence 57 days 3 hrs 13 mins			100K/1M
	Mojo	Monet DB	Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Connection	Malware No Events			0/1M 0/2M
	sftunnel	SLA		Sybase Arbiter	Symmetric	s Syb	ase DB		Discovery No Events User No Events			0/1M 0/1M
	CPU 100% 75% 50% 25% 0% 04:04	04:09 04:14	04:19 04:24	0129 013	4 04:39 04:	Avg CF	U ~	Memory - 100% 50% 25% 0% 0%	Used	04.29 04.34 04.39	04:44 04:49	04:54 04:59
	Interface - 644.3K 1133.2K 11.1K 0 04:04	Input Rate	Output Ra	ate	4 04:39 04:	44 D4:49	De:54 04:59	Disk Usag	e Entire Disk		Critical Partition	ns

Vista de resumen de:

- Alta disponibilidad
- · Capacidad y velocidad de eventos
- Estado del proceso
- CPU
- Memoria
- Interfaz
- Disco

Este panel está disponible tanto para los CSP activos como en espera. El usuario puede crear paneles personalizados para supervisar las métricas que elija.

Panel de FMC: panel de HA de FMC

High Availability		Configure
Primary- Active	Degraded Last sync: a few seconds ago Degraded- Synchronization incomplete	Remote Secondary- Standby FMC_Standby - Critical Alerts: 2

El panel HA muestra

- Estado actual de HA
- Activo frente a En espera
- Hora de la última sincronización
- · Estado del dispositivo

Panel de FMC: velocidad y capacidad del evento

Tasa de eventos

- · Velocidad máxima de eventos como línea base
- Tasa global de eventos que recibe el CSP

Capacidad del evento

- · Consumo actual por categorías de eventos
- Tiempo de retención de eventos
- · Actual vs. Máxima

capacidad del evento

· Marcador de desbordamiento de capacidad

He Viev O	alth: FN v System & verview	MC Orit Troubleshoo Process	tical ot Details s											Last 2021	1 hour	r 06:32 - 2	2021-02	-22 07:32
Pro	ocess He	alth			Crit	tical Proce	sses A	II Processes	Event Capacity	-							Co	nfigure
	1.100	DOODL	500	Mar Cardina	Deal	Develop	Destable	0500	Connection	3 days 16 hrs 3 m	ins						1/1M	Ê
A	ctionQ	DCCSM	655	Msg Service	MsgHandler	Pruner	RabbitMQ	Notifier	Intrusion	No Events						(0/1M	
	C Data	0.000	Townsh	Descisioning	ADI	Disk	Main	Marat DD	File	No Events							0/1M	
C	errelator	Sync D	Tomcat	Process	ADI	Manager	MOJO	Monet DB	Security Intelligence	No Events						(0/1M	
		14.001.00	Durality	0510.0	05.14-2	Othersel	01.4	C. hund	Connection Summary	No Events							0/1M	
~	iongo DB	MySQL DB	KUN HM	SHIP Proxy	SH Mgr	Situnnei	SLA	Arbiter	Malware	No Events							0/2M	
s	ymmetric		1		Sybase DB			1	Discovery	No Events							0/1M	
									User	No Events							0/1M	-
_										-								
CE	U						Avg CPI	u ~	Event Rate									
0.	Data coll	lection for C	PLLmodul	e is disabled	in the healt	h policy p	artial or no	data may be	5.0k									
▲	shown.		or or module	6 15 01500160	in the near	in policy, p		data may be	3.8k									
	01101111								2.5k									
									1.3k									_
									0.0									
				No Data	Available	9			06:35 06:40	06:45 06:50	06:55	07:00	07:05	07:10	07:15	07:20	07:25	07:30

Panel de FMC: Capacidad del evento

Estado de consumo de capacidad de evento normal

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	56458978/100000000 Capacity	
Overflow	v:			
Connection	18h			11.6 M / 10 M
Oracativa	2020-09-18 14:28:30			
Connection	18h			11.6 M / 10 M
	18 hours Retention Duration	3.6k/min Incoming Rate	116245455/10000000 Capacity 🔺 🚽	

Escenario de desbordamiento, cuando los eventos se almacenan más allá de la capacidad máxima configurada.

- El texto en negrita indica desbordamiento
- Un icono de advertencia resalta el desbordamiento de capacidad

Panel de FMC: Panel de procesos de FMC

El panel Procesos críticos muestra

- Procesar estado actual
- Recuento de reinicio del proceso

rocess He	ealth					Critic	cal Proc	esses A	All Processe
ActionQ	DCCSM ESS		Msg Service	Perl MsgHandler	Pruner	F	RabbitMQ	SFDC Notifier	SF Data Correlator
Sync D	Tomcat Provisioning Process		ADI Disk Manager		Mojo	Mojo Monet [Mongo DB	MySQL DB
Run HM	SFIP Prox	y SF Mgr	Sftunne	SLA		Sybas Arbite	ie ir	Symmetric	Sybase DB

El panel de procesos muestra estas métricas para todos los procesos "pmconfig":

- Estado actual
- Uso de CPU
- Uso de memoria

Process Health		Critica	al Processes	All Processes
Process status at: Dec 14, 2020 3:22	2 AM			
Process *	Status	CPU (%)	Mem Us	sed
ActionQ	Running	0	66	.23KB
CSD App	Waiting	0		0
CSM Event Server	Running	0.6	18	2.1KB
CloudAgent	Running	0.9	12	.03KB
DCCSM	Running	0	104	.49KB
ESS	Running	0.1	448	.26KB
Event DS	Running	0	34	.59KB

Panel de FMC: CPU de FMC

El panel CPU muestra

- CPU media (predeterminado)
- Todos los núcleos





Panel de control de FMC: Otros paneles

El panel Memoria muestra el uso general de la memoria en FMC



El panel Interfaz muestra la velocidad de entrada/salida de la media de todas las interfaces



El panel Disco muestra

- · Capacidad de disco completa
- · Capacidad de partición crítica donde se almacenan los datos de FMC

Disk Usage	
Entire Disk	Critical Partitions
9% Used	12% Used
	/dev/sda7

Intervalo de tiempo de ejecución

- El intervalo de tiempo de ejecución para el módulo de mantenimiento antiguo cambia a "Intervalo de tiempo de ejecución heredado".
- El 'Intervalo de tiempo de ejecución' se dirige a los nuevos módulos de salud basados en Telegraf
- · Configuración global, afecta a todos los dispositivos

CISCO Edit Overview Analy	vsis Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	0	ø	0	admin 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Poli	icy: Initial_H	ealth_Polic	y 2021-	01-29 04:40:49	9					Alerts
AMP For Endpoints Status AMP for Firepower Status ASP Drop	Po	Policy Name licy Description	Initial_Hea	alth_Policy	2021-01-291						
Advanced Snort Statistics Appliance Heartbeat	Legacy Ru Run Time	un Time Interva (mins) e Interval (mins)	5								
Automatic Application bypass Status Backlog Status CPU Usage (per core)	Note : Changes monitoring pro-	s to Run Time Int cess.	ierval will restar	t the health							
CPU Usage Data Plane CPU Usage Snort CPU Usage System					Gancel	Save Policy and Exit	1				
Card Reset Chassis Status FTD Cluster/Feilower Status											
Configuration Database Connection Statistics											
Critical Process Statistics Deployed Configuration Statistics Disk Status											

Métricas Disponibles

Métricas disponibles para paneles personalizados

• Si un usuario desea crear un panel personalizado, estas diapositivas son una guía de las

métricas disponibles.

• Algunas métricas deben estar habilitadas en la política de estado antes de que se puedan utilizar en un panel de estado personalizado

cisco Edit Overview Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	(Q	¢	≎	0	syed •
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Polic [en_US/adn	cy: Initial_H nin:policy_I	ealth_Polic ast_modifie	y 2020- ed])	12-08 08:49:4	6 (Last Modified:					Alerts
AMP for Englower Status AMP for Firepower Status ASP Drop	Poli	Policy Name cy Description	Initial_Hea	alth_Policy	2020-12-08 (
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status		Description	Monitors CP cores, thresh applicable to	U usage on hold set here all the core	all the e will be ⊧s						
Backlog Status	Critica	Enabled al Threshold %	90	Dff							
CPU Usage (per core) CPU Usage Data Plane	Warnin	g Threshold %	80								
CPU Usage Snort CPU Usage System					Cancel	Save Policy and Exit					
Chassis Status FTD											
Configuration Database											
Critical Process Statistics											
Deployed Configuration Statistics Disk Status											
Disk Usage Event Stream Status FMC Access Configuration Changes											

Interfaz de usuario de FMC: panel personalizado de FMC

Nuevas categorías de métrica de supervisión de CSP en 7.0

- CPU
- Memoria
- Interfaz
- Disco
- Evento
- Proceso
- RabbitMQ
- Sybase
- MySQL

Health: FN View System 8 Overview	Crit Troubleshoo Process	ical 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 ^
SF Data Correlator	Sync D	Tomca	Name*	0/1M 0/1M
Mongo DB	MySQL DB	Run H	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	

Interfaz de usuario de FMC: métricas de FMC

40 métricas agregadas en diferentes categorías (disponibles en el panel personalizado). Para activar las métricas desactivadas, active el módulo de estado correspondiente en la política de estado asociada (Sistema > Estado > Política).

Nombre del grupo de métricas	Habilitado de forma predeterminada	Descripción
CPU	No	Supervisa la CPU de FMC
Memoria	Yes	Supervisa la memoria FMC
Disco	Yes	Supervisa el uso del disco FMC
Interfaz	Yes	Supervisa la interfaz FMC
Proceso	Yes	Supervisa los procesos de FMC
Evento	Yes	Supervisa La Tasa De Eventos
MySQL	No	Supervisa MySQL
RabbitMQ	No	Supervisa RabbitMQ

Sybase	No	Supervisa Sybase
- ,	-	

FTD: Métricas introducidas en FP 7.0

Habilitado de forma predeterminada: las métricas se recopilan de forma predeterminada. Para activar las métricas desactivadas, active el módulo de estado correspondiente en la política de estado asociada (Sistema > Estado > Política).

Nombre del grupo de métricas	Habilitado de forma predeterminada	Descripción	Platform
Estado del chasis	Yes	Supervisa diferentes parámetros del chasis, como la velocidad del ventilador y la temperatura.	Aplicable únicamente a las plataformas FPR2100 y FPR1000
Descarga de flujo	Yes	Supervisa las estadísticas de descarga de flujo de hardware	Aplicable a FPR9300 y plataformas FPR4100
caídas ASP	Yes	Supervisa las caídas de paquetes laterales Lina	Todos
Número de visitas	No	Supervisa los recuentos de visitas para las reglas de directiva de control de acceso	Todos
Estado de AMP Threat Grid	Yes	Supervisa la conectividad con AMP ThreatGrid	Todos
Estado de conectividad de AMP	No	Supervisa la conectividad de la nube de AMP desde el FTD	Todos
estado del conector SSE	No	Supervisa la conectividad de nube SSE desde el FTD	Todos

Estado de NTP	No	Supervisa los parámetros de sincronización del reloj NTP en el FTD	Todos
estadísticas de VPN	Yes	Supervisa las estadísticas del túnel S2S y VPN RA	Todos
Estadísticas de ruta	Yes	Supervisa las caídas de paquetes laterales Lina	Todos
Estadísticas de rendimiento de Snort 3	Yes	Supervisa determinadas estadísticas de rendimiento de Snort3 (perfstats)	Todos
contadores xTLS	No	Supervisa los flujos de xTLS/SSL y la eficacia de la memoria y la caché	Todos

API REST, Syslog, SNMP

No se han introducido nuevas API REST de FMC o FTD Device en 7.0. Las API REST existentes admiten nuevas métricas añadidas en 7.0.

Syslog y SNMP

Syslog

• No hay cambios en syslog para el monitor de estado

SNMP (Protocolo de administración de red simple)

• TOI independiente para "Supervisión del estado de los dispositivos SNMP"

Integración de productos SAL/CTR/de terceros

- TOI independiente para la compatibilidad con 'Azure Application Insights'
- No se ha realizado ningún cambio específico para permitir la integración de la "supervisión de estado" con SAL/CTR/SecureX
- La API REST se puede aprovechar para la integración de terceros

Tecnología de software

Detalles de la función 6.7

Nueva supervisión del estado de NGFW para el estado y el rendimiento de FTD

Ayuda a los usuarios con

- Depuración reactiva, como el análisis de la causa raíz, el problema después de que haya ocurrido
- Acciones proactivas como la supervisión de los niveles de uso y saturación para identificar posibles problemas de capacidad y, por tanto, ayudar a los usuarios a realizar mejoras de capacidad o refactorización.

Aspectos destacados

- Gráficos de tendencias: los gráficos de tendencias facilitan la detección de anomalías y la determinación de la causa principal de los problemas. Con la inspección visual se pueden detectar tendencias y trazar correlaciones entre diferentes métricas para encontrar una relación causal entre ellas.
- Superposiciones de eventos: las superposiciones de eventos muestran información importante, como la implementación de configuraciones y las actualizaciones de SRU en los gráficos de tendencias para indicar las relaciones causales.
- Paneles personalizables: los usuarios pueden crear sus propios paneles para agrupar las métricas que deseen ver juntos en una página.
- Arquitectura de supervisión de Unified Health: punto único de recopilación y exportación de métricas, independientemente del gestor que esté "interesado" en las métricas. Las API de FTD, así como el FMC, utilizan datos del mismo recopilador de métricas.
- Extensibilidad de las métricas: uno de los objetivos de la arquitectura para la plataforma era poder añadir nuevas métricas fácilmente. Esto se logra mediante el uso de herramientas de recopilación y almacenamiento de métricas de código abierto y con paneles personalizables.

GUI de FMC

Interfaz de usuario de FMC: Navegar hasta Estado de mantenimiento

En FMC, haga clic en el icono System > Health > Monitor para navegar a la página Health Status.



Interfaz de usuario de FMC: Página Nuevo estado de mantenimiento

La página Estado de salud está diseñada para mostrar una descripción general del estado de todos los dispositivos que gestiona el FMC, incluido el estado del FMC.

- · Los dispositivos se agrupan según su grupo/ha/clúster.
- Un punto a la izquierda del dispositivo indica su estado
- Verde: sin alarmas
- Naranja: al menos una advertencia médica
- Rojo: al menos una alarma de estado crítico
- El resumen de estado se muestra al situar el cursor en el hexágono que representa el estado del dispositivo.
- Los umbrales de advertencia y crítico se pueden configurar en la política de salud, de la misma manera que se hizo antes de FP 6.7.

Monitoring 😑	Health Alerts
ିର HOME	7 total 1 critical 2 warnings 5 normal 0 disabled Search a device X V
 FMC Devices (5) Asia 	FMC Asia ungrouped 192.168.0.26 - Warning
 Bangalore (HA) bangalore-main 	Device Alerts: 9 0 A 2 0 21
ø bangalore-standby	FMC CPU Usage CPU usage
chennai	bangalore-main Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalore-standby linine Link Mismatch Alarms Local Malware Analysis Columnation
A 192.168.0.25	> Clickeo view more datais
A 192.168.0.26	> 🔷 mumbai
	> 192.168.0.25
	> 192.168.0.26

Interfaz de usuario de FMC: eventos de estado del dispositivo

Haga clic en el dispositivo en el panel inferior para mostrar los eventos de estado asociados al dispositivo. Las alertas se ordenan por su estado (gravedad).

Página Supervisión de estado

>	A 192.168.0.25	
~	▲ 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

Interfaz de usuario de FMC: la supervisión de estado de FMC no ha cambiado

La página de estado de FMC sigue siendo la página heredada. La nueva interfaz de usuario solo es compatible con FTD con 6.7+

Monitoring							
FMC	Health	Monitor					
· Devices (4)		Appliance				Module Status Summary	
0 1140	•	vime-10	Generate Troubleshooting Files				
			Advanced Troubleshooting		Normal (56.0	Coulde Could	
	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		

Interfaz de usuario de FMC: Nuevo Paneles de dispositivos

- Haga clic en el nombre del dispositivo en el panel izquierdo para acceder a la página de descripción general del estado del dispositivo.
- La descripción general de estado contiene todos los gráficos de tendencias de métricas de estado clave.
- Hay disponibles varios intervalos de tiempo (el valor predeterminado es la última hora)
- Actualización automática para volver a cargar el gráfico

Monitoring 😑	Health: 192.168.0.25 A Warning View System & Troubleshoot Details	Last 1 hour V 0 2020-06-23 01:58 - 2020-06-23 02:58					
ଜି HOME	Overview CPU Memory Interfaces Connections Snort	± +					
FMC	CPU	Memory					
 Devices (5) 	LINA Avg 1.5 % Snort Avg 0.7 % System Avg 17.5 % 1 core 1.2 % - 2.6 % 2 cores 0.5 % - 1.0 % 1 core 15.0 % - 24.0 %	LINA Avg 49.7 % Snort Avg 28.1 % System Avg 68.8 % 4.0468 49.7 % - 49.7 % 3.6668 28.1 % - 28.1 % 7.608 68.8 % - 69.4 %					
✓ Asia	100	100 Cilicol					
Bangalore (HA)	80	80					
bangalore-main	00	60					
bangalore-standby	40	40					
chennai	20	20					
o mumbai ∽ ungrouped	0.0 91.45 01.50 01.55 02.99 02.05 02.10 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					
▲ 192.168.0.25	Throughput Avg Data Interfaces V	Connection Statistics					
A 192.168.0.26	Input Rate Avg 0 0-0 Output Rate Avg 0 0-0	Connections Avg 0 0 - 0 NAT Translations Avg 0 0 - 0					
	g sco	100					
	§ 640	80					
	480	60					
	320	40					
	160	20					
	C	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	01145 01.50 01.55 02:00 02:05 02:10 02:15 02:20 02:25 02:30 02:35 02:40					
	Disk Usage	Critical Processes					
		AMP Java LINA SF Data Sfturnel SSE Connector					
	9% 15% 18% Used Used Used	Contraintor					
		Short01 Short02					
	Full Disk /ngfw /ngfw/Volume						

Interfaz de usuario de FMC: superposición de datos de implementación

Haga clic en el icono de despliegue para mostrar los detalles de la superposición de despliegue en el gráfico con el rango de tiempo seleccionado

- El icono indica el número de implementaciones durante el rango de tiempo seleccionado
- La banda aparece para indicar la hora de inicio y finalización de la implementación.
- En caso de varias implementaciones, aparecen varias bandas/líneas
- Haga clic en el icono situado en la parte superior de la línea de puntos para mostrar los

detalles

	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 Snort	
	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 0 0 0 0 0 0 80 0 0 0 0 0 0 0 0.0 02.30 02.35 02.40 02.45 02.50 02.55		
CPU LINA Avg 2.7 % Snort 1 core 0.5 % - 7.8 % 2 cores 0 100 60 40 20 0.0 08.30	Aug 3.7 % System Aug 19.1 % 1 core 14.0 % - 30.0 %	CPU System Avg 20.5 % 1 core 0.5 % + 2.5 % 2 cores 0.0 % + 15.5 % 100 1 core 1 core 1 core 80 1 core 1 core 1 core 90 1 c	Jun 2

Interfaz de usuario de FMC: paneles prediseñados para dispositivos

- Hay paneles de salud prediseñados presentes en la interfaz de usuario de FMC.
- Estos paneles prediseñados incluyen métricas relacionadas agrupadas.
- El panel de interfaz tiene un gráfico de tendencias para todas las métricas relacionadas con la interfaz, como bytes de entrada/salida, paquetes y tamaño promedio de paquete para diferentes interfaces.

Health: wm-101 Normal View System & Troubleshoot Details									
Ov	erview	CPU	Memory	Interfaces	Connections	Snort			
Int	erface -	Input Bytes,	Output Bytes						
es in Bp	1.6K								
value	1.2K								
	800								
	400								
	0								
		07:45		07:50	07	55	08:00		
Int	erface -	Input Packet:	s, Output Pack	ets, Drop Pack	ets				
10	00								
4	80								

FTD Snort Memory - ¿De dónde se origina?

Firepower Manage CISCO System / Health / Monitor	ement Cente	er _{Overview}	Analysis	Policie	s Devic	es Obj	ects Al	MP Int	elligence		Deplo	iy Q	6 ¢	Global \ mzafeiro •
Monitoring	Health: mz	afeiro_FTD11	50-1 (Active)	Normal								La:	st 1 week 1-10-05 10	✓ ○ * 59 - 2021-10-12 10:59
G Home	Overview	CPU M	emory Int	erfaces	Connections	Snort	ASP dr	ops						
FMC														
✓ Devices (8)	Memory - N	taximum Data Pi	ane, Data Plane)										
√ cisco	5.7 G8													
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 - N	taximum Snort S	Sport											
v mzafeiro_FP1150-HA	20.2 GB	laximam onort, c						2021-1	00 00 15 0007	_				
mzafeiro_FTD1150-1 Ac	16.3 GB							Maxi	mum Snort 20.2 G t 4.7 G	8				
mzafeiro_FTD1150-2 s	12.5 GB							-						
mzafeiro_FTD4115-2	8.8 GB													
Sami_10.62.148.194	1.1 00							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 - S	ystem Used, Tot	al											
	31.4 GB													
	25.8 GB													
	20.2 GB													-

Interfaz de usuario de FMC: se pueden crear paneles personalizados

Los usuarios pueden crear su propio panel personalizado

• Además de los paneles predefinidos, el usuario también puede crear paneles personalizados.

- En el panel personalizado, se puede agregar cualquier cantidad de métricas.
- Normalmente, se crearía un panel personalizado si las métricas de diferentes grupos de métricas pudieran correlacionarse para llegar a la causa raíz de un problema.
- En el caso de una CPU de línea alta, se puede ver la conexión entrante por segundo (CPS), las estadísticas de la interfaz (y así sucesivamente) que pueden hacer que la CPU se eleve.



Interfaz de usuario de FMC: creación de un panel personalizado

Diálogo Correlacionar Métricas

- Cuando un usuario hace clic en "+" para crear un panel personalizado, se abre la ventana Correlacionar métricas.
- Un usuario puede agregar diferentes métricas que desea supervisar conjuntamente.

Correlate Metrics		×
Correlate the metrics that are custom to specify your own r Correlation Group*	inter-related. Select predefined correlation group netrics.	ps or
CPU - Snort		\sim
Hide Details Dashboard Name*		
Correlation-CPU-Snort		
Metrics Chosen metrics will be displa	yed as portlets in the dashboard.	~ ₹
Interface v	/ Input Packets X X	~
Deployed Configuration v	Number of rules X X	~ 7
Deployed Configuration v	Number of ACEs X X	~
Add Metrics		
	Cancel	Add

Recopilación de datos desde (dispositivo): GUI

Datos para un rango de tiempo que se muestran en la GUI

Si el monitor de estado no tiene datos para el intervalo de tiempo seleccionado, la GUI muestra "No hay datos disponibles" en el panel de control:

Event Rate		
	No Data Available	

En caso de que haya datos disponibles, el gráfico se muestra de la siguiente manera:



Uso de las pestañas Consola y Red del explorador

Registro de la consola del explorador y registro de llamadas de red

- En este ejemplo, se muestra la consola del desarrollador del navegador Chrome
- En caso de error, los detalles de la excepción se muestran en el registro de la consola

Gisco System / Health / Monitor	ment Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy Q 🥝	🔅 🕜 syed 🕶
Monitoring	Overview CPU Memory Interfaces Connections Snort ASP drops	曲 +
 ₩onitoring If Home FMC FMC - Active FMC - Standby Devices (2) 192.168.0.219 	CPU Data Plane Aug 0%. Snort Aug 1%. System Aug 15%. Data Plane Aug 76%. Snort Aug 21%. System Aug 16%. 100% 1 core 0% - 0%. 2 cores 0% - 1%. 1 core 0% - 0%. 3.96G8 21% - 21%. 7.868 451 100% 50%	g 45% b - 475
V FTD-HA	Dae 13 Dae 14 00:59 01:29 01:59 02:29 02:59 03:29 Dae 13 Dae 14 00:59 01:29 01:59 02:2	29 02:59 03:29
192.168.0.217 192.168.0.217 K	Throughput Avg - all interfaces Connection Statistics Input Rate Avg 1.34kbps 439tps - 2.34kbps Output Rate Avg 2.03kbps 803tps - 2.37kbps Connection Statistics 2.5K	29 02.59 03.28 5 ₽ 354 ✿ : ×
Imp v v v v v v v v v v v v v v v v v v v	Filter Default levels * 2) vider, js:80) s:36) ider, js:33) rr, js:33) ider, js:32) onnectFunction) , js:39)	3 hidden 🏚
<pre>>> {type: "unknown"}</pre>		index.js:1

Ejemplo de registro de consola del explorador

Console Tab Exception details	S			
Elements Console Sources Network Performance Memory Application Security	ity Lighthouse Redux » 🛛 3 🗛 1 🗱 🗄 🗙			
🕩 🛇 top 🔻 🧿 Filter Default levels 🔻	\$			
v Validation using FMC HA State schema failed with 2 error(s) validator.js:75				
♥ ►data.remote.status[2] = null should be string,number (per #/definitions/Status/properties/status/items/type)				
♥ ► data.remote.status[3] = null should be string,number (per #/definitions/Status/properties/status/items/type)				
▲ > Details > {data: {}, error: {}, schema: {}}				
S ► ► {message: "validation failed", errors: Array(2), validation: true, ajv: true}				
BaseLineChart - Render BaseLineChart.js:376				
Baseline chart props changed BaseLineChart.js:163				
undefined 0 100 100 undefined ▶ [{_}] "area" undefined ▶ (2) [{_}, {_}] ▶ {type: "UTC_TIME", range: e} "percent" undefined BaseLineChart.js:164				
	- · · · · · · · · ·			

Referencias

Seguimiento del estado de FMC - 6,7

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).