

# 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

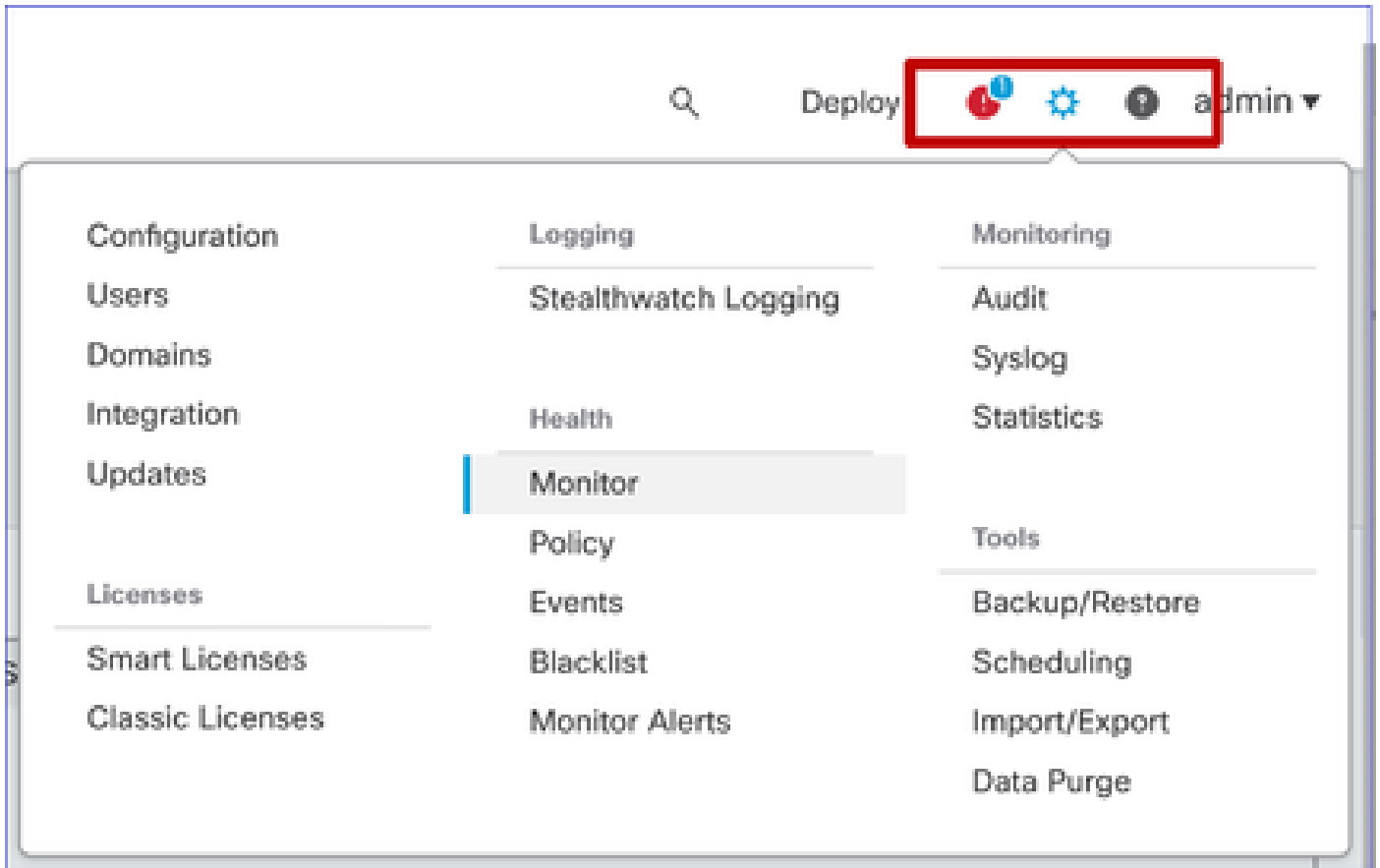
- Nueva interfaz de usuario en FMC que proporciona gráficos de tendencias, superposiciones y paneles personalizados.
- API de FTD: permite que entidades externas puedan consultar las mismas métricas

#### 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.



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)

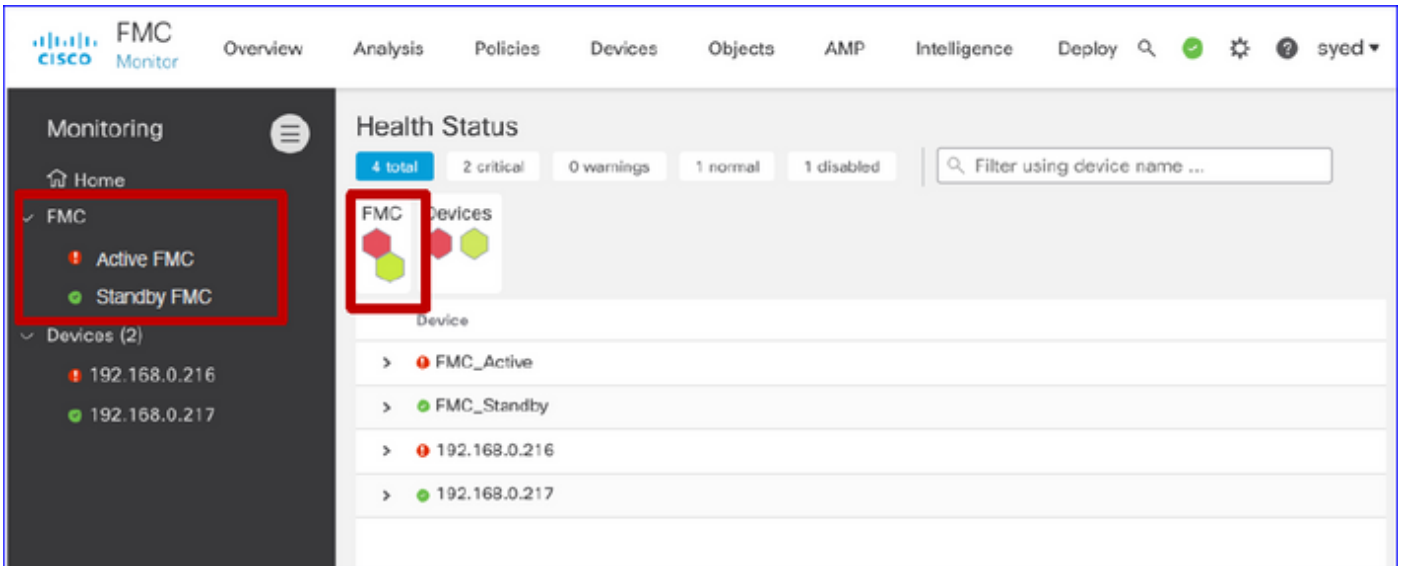
Interoperabilidad

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



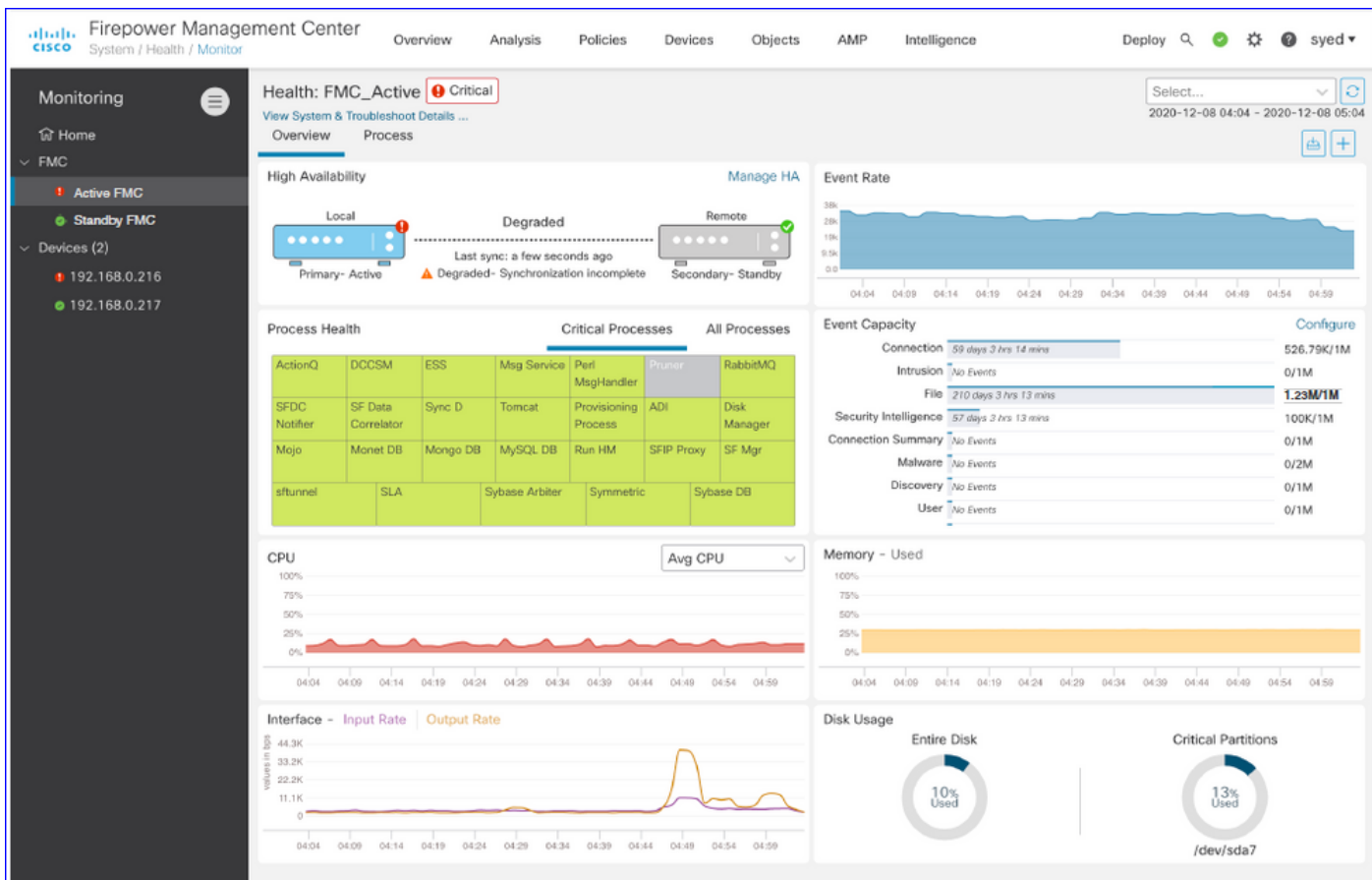
- FMC independiente se muestra como un nodo único
- FMC HA se muestra como un par de nodos
- Cada CSP se muestra con el estado de mantenimiento

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

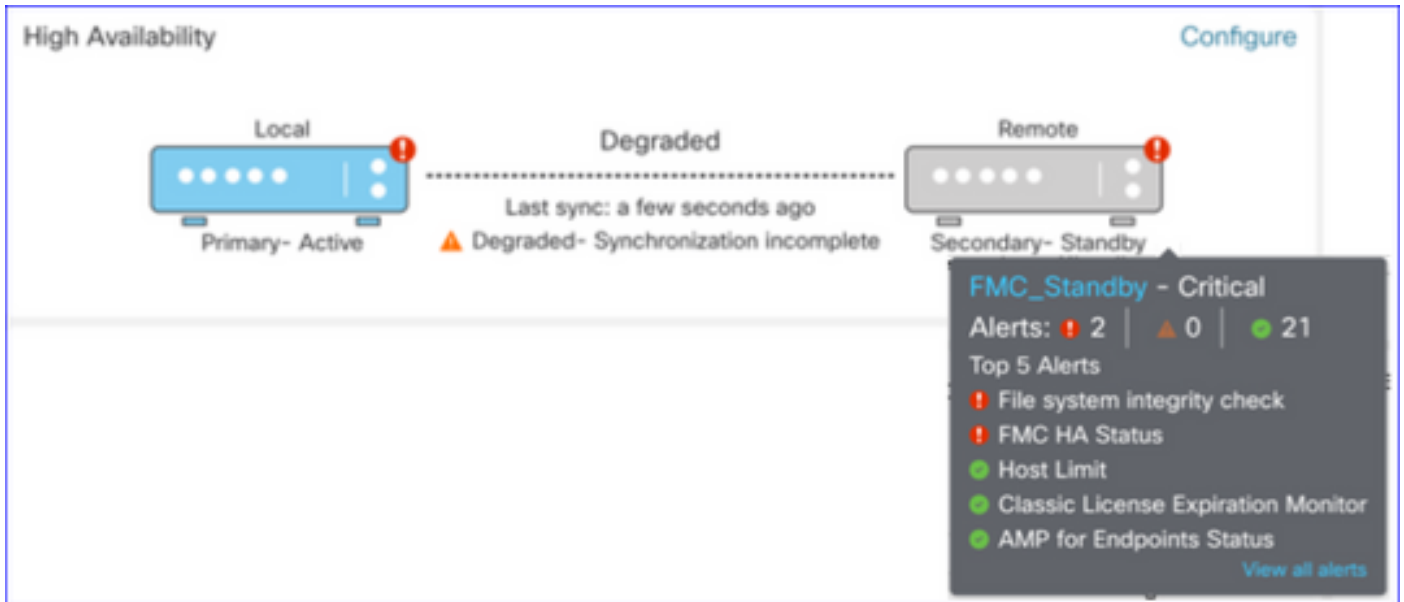


Vista de resumen de:

- 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



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

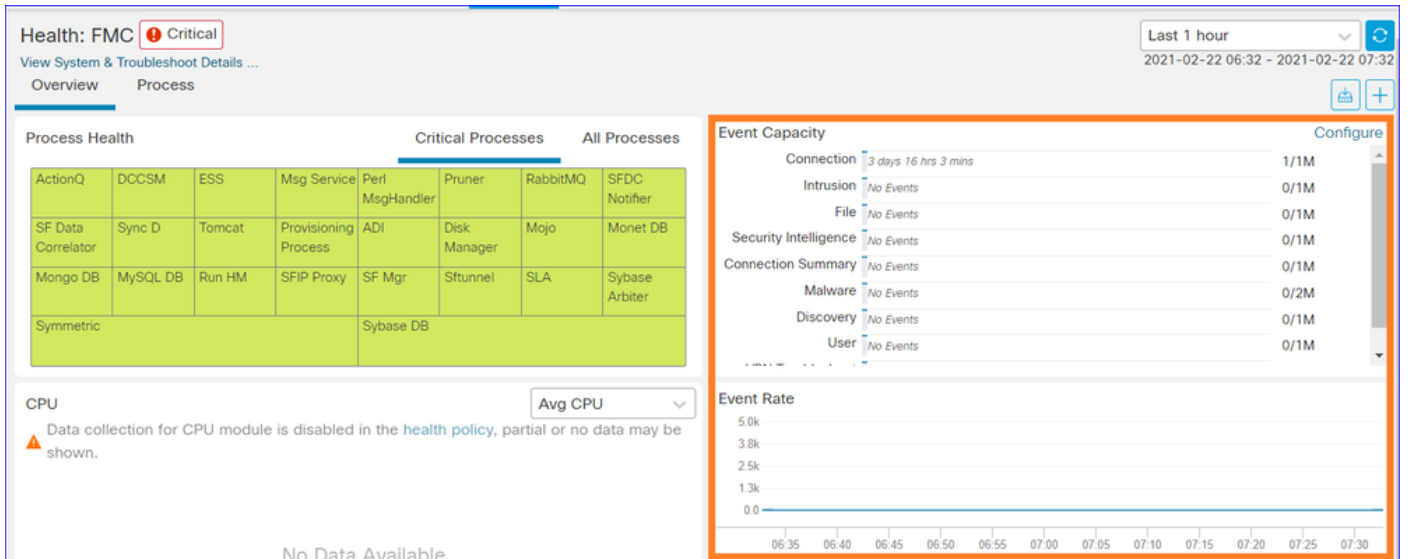
- Velocidad máxima de eventos como línea base
- Tasa global de eventos que recibe el CSP

Capacidad del evento

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

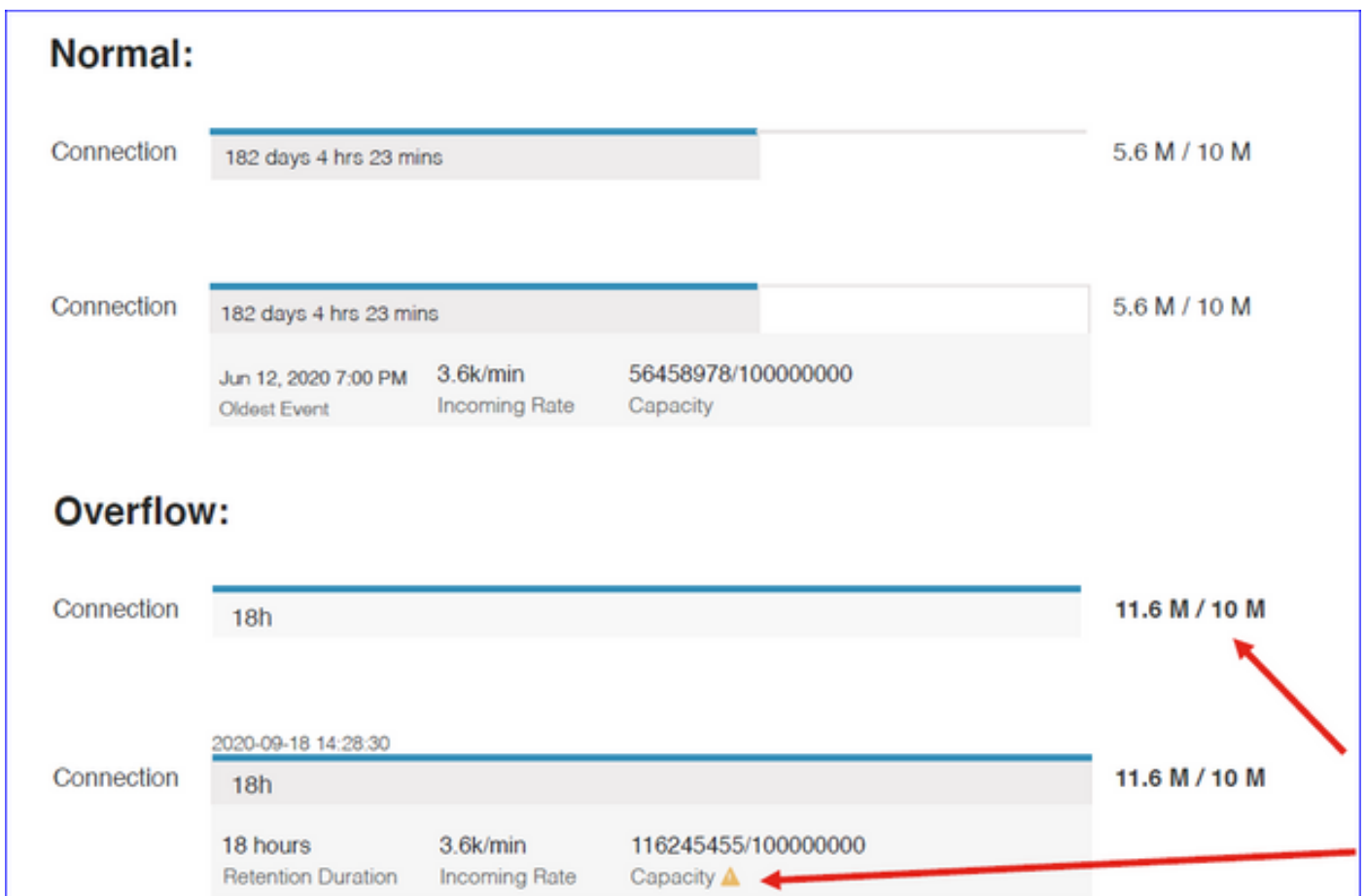
capacidad del evento

- Marcador de desbordamiento de capacidad



Panel de FMC: Capacidad del evento

Estado de consumo de capacidad de evento normal



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

Process Health				Critical Processes				All Processes
ActionQ	DCCSM	ESS	Msg Service	Perl MsgHandler	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 Proxy	SF Mgr	Sftunnel	SLA	Sybase Arbiter	Symmetric	Sybase DB	

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

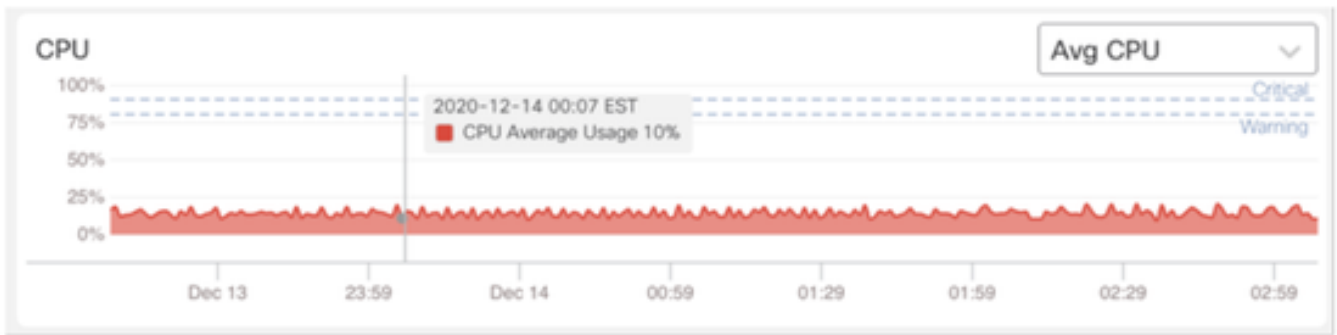
- Estado actual
- Uso de CPU
- Uso de memoria

Process Health		Critical Processes		All Processes
Process status at: Dec 14, 2020 3:22 AM				
Process *	Status	CPU (%)	Mem Used	
ActionQ	Running	0	66.23KB	
CSD App	Waiting	0	0	
CSM Event Server	Running	0.6	182.1KB	
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

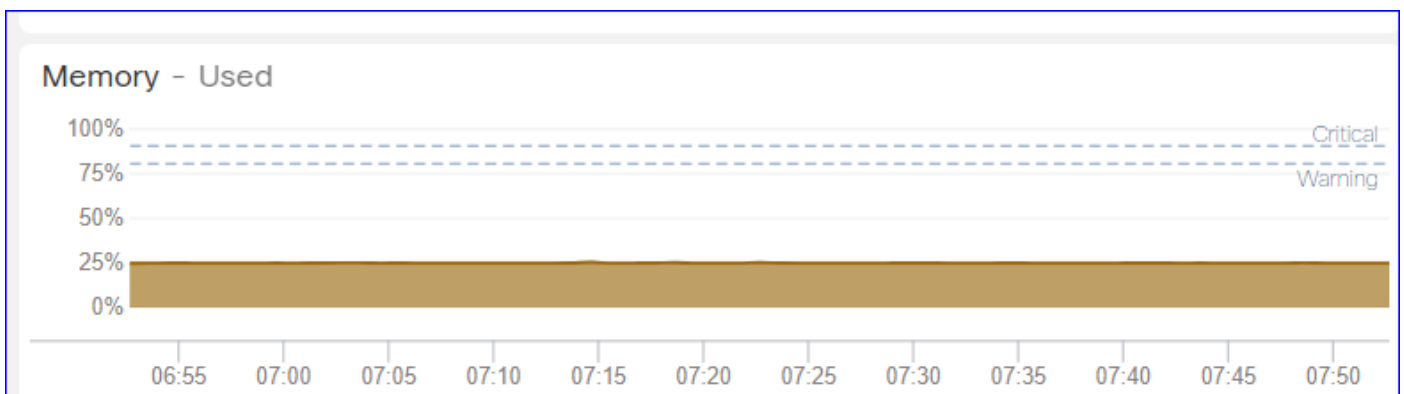
El panel CPU muestra

- CPU media (predeterminado)
- Todos los núcleos

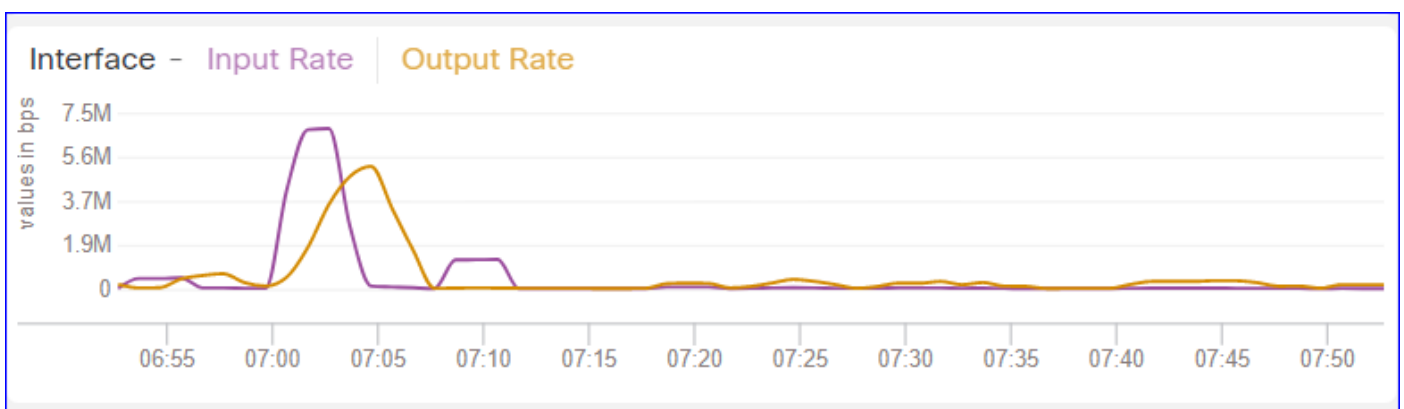


Panel de control de FMC: Otros paneles

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

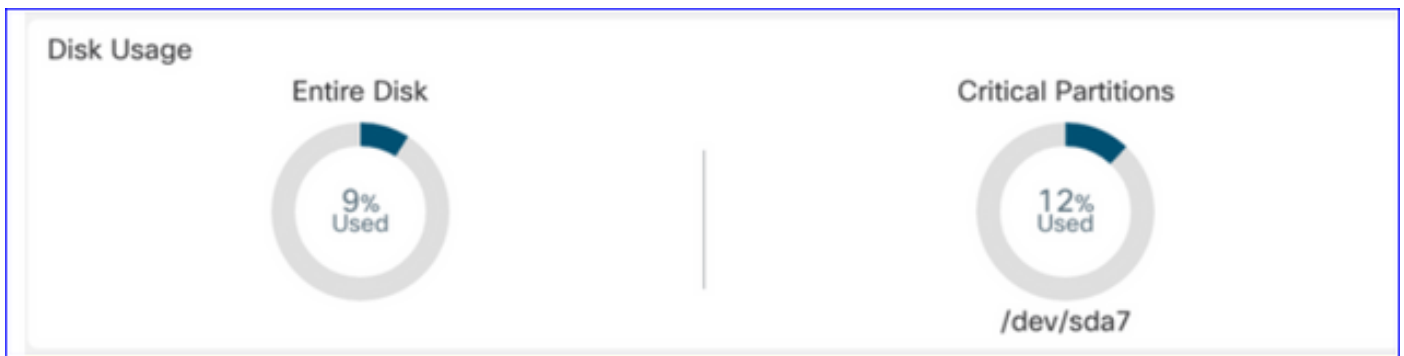


El panel Interfaz muestra la velocidad de entrada/salida de la media de todas las interfaces



El panel Disco muestra

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



### 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

The screenshot shows the Cisco FMC interface for editing a policy. The left sidebar lists various metrics, with 'Policy Run Time Interval' selected. The main area is titled 'Editing Policy: Initial\_Health\_Policy 2021-01-29 04:40:49'. It contains two input fields: 'Policy Name' (Initial\_Health\_Policy 2021-01-29) and 'Policy Description' (Initial Health Policy). Below these, a red box highlights the 'Legacy Run Time Interval (mins)' field set to 5 and the 'Run Time Interval (mins)' field set to 1. A note below the fields states: 'Note : Changes to Run Time Interval will restart the health monitoring process.' At the bottom right, there are 'Cancel' and 'Save Policy and Exit' buttons.

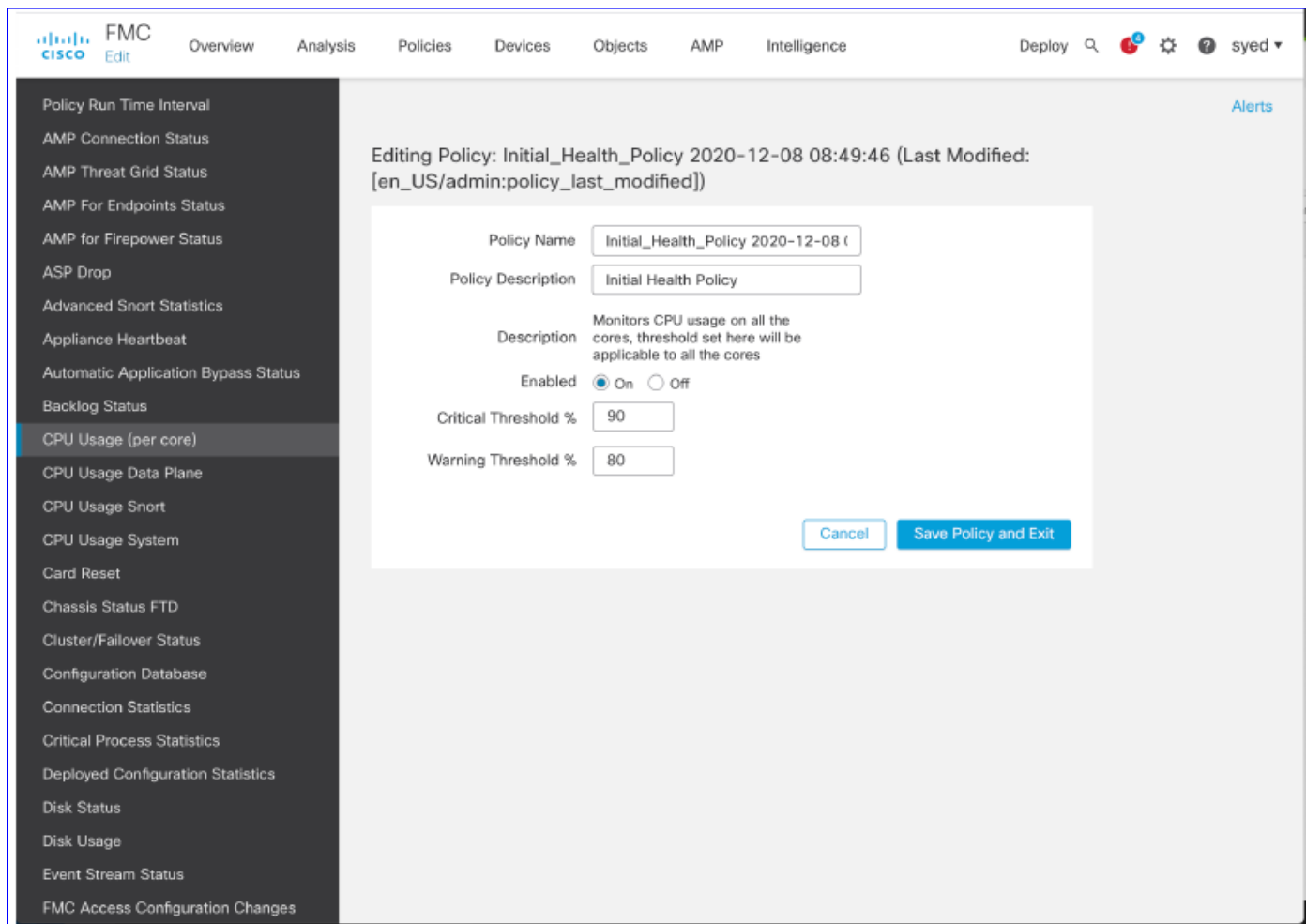
### Métricas Disponibles

#### Métricas disponibles para paneles personalizados

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

métricas disponibles.

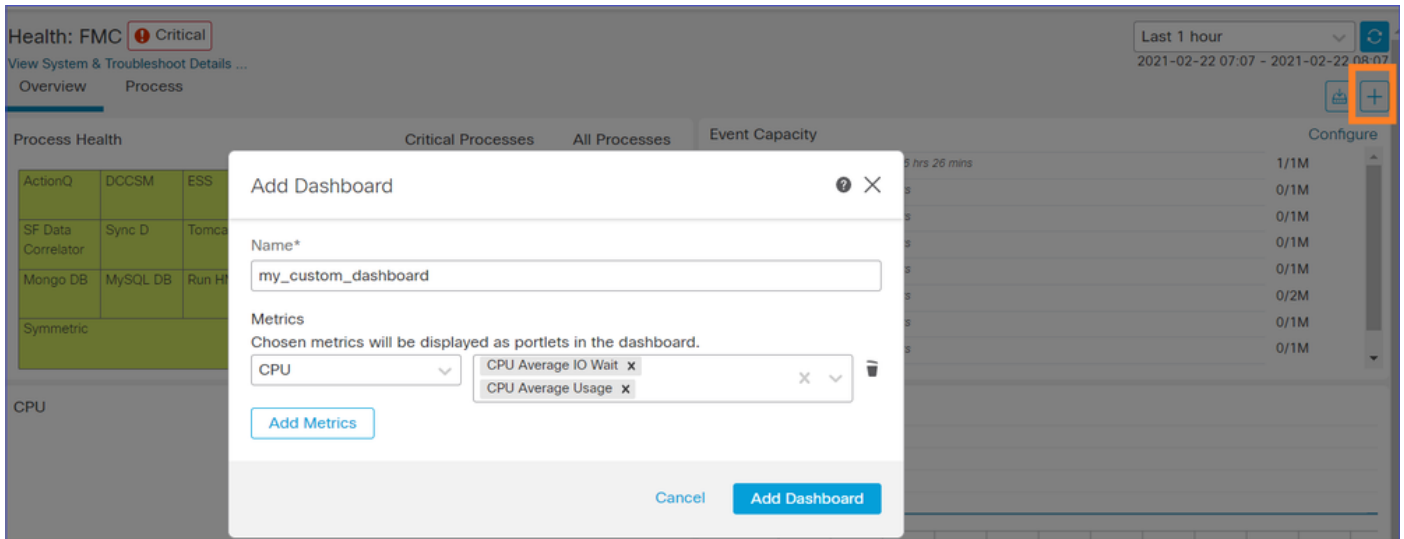
- Algunas métricas deben estar habilitadas en la política de estado antes de que se puedan utilizar en un panel de estado personalizado



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



## 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

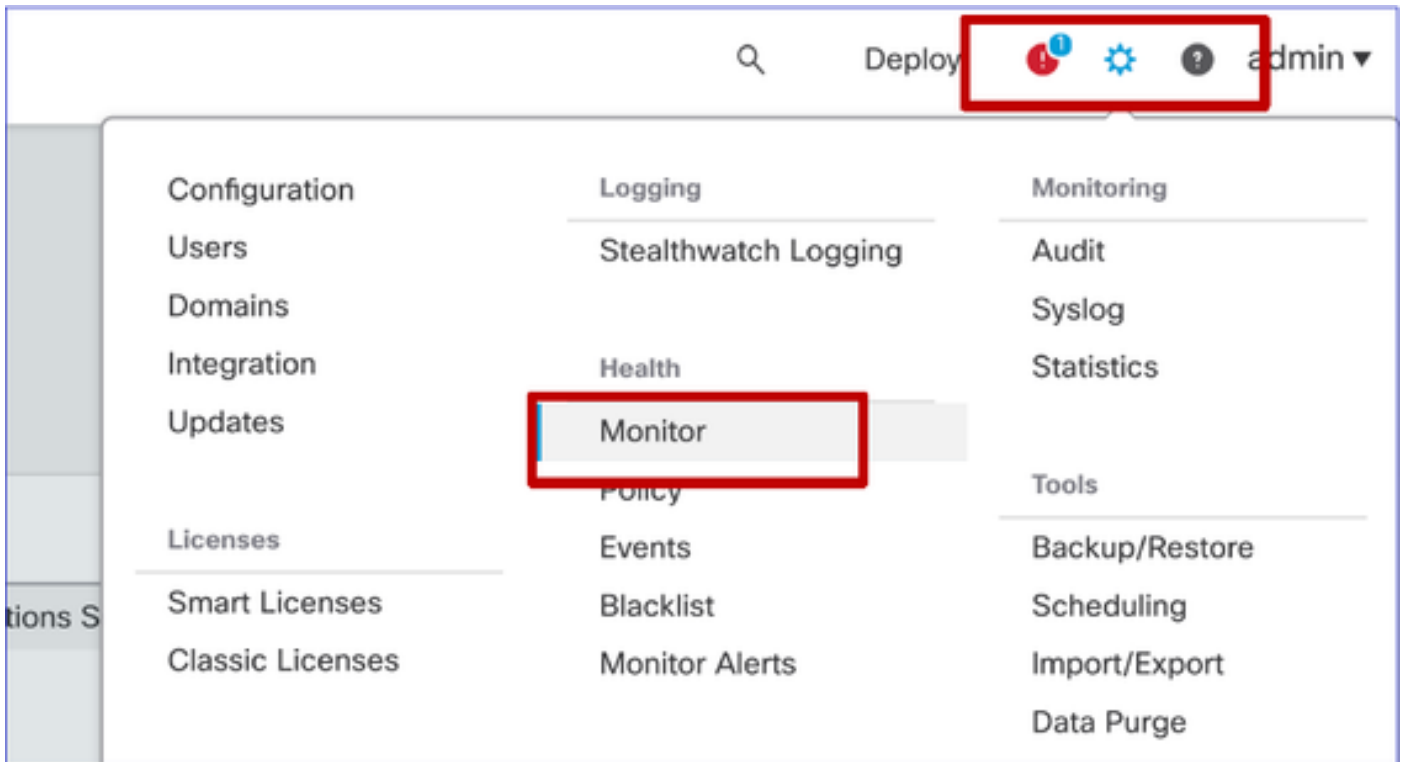
- Gráficos de tendencias: los gráficos de tendencias facilitan la detección de anomalías y la determinación de la causa principal de los problemas. Con la inspección visual se pueden detectar tendencias y trazar correlaciones entre diferentes métricas para encontrar una relación causal entre ellas.
- 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.

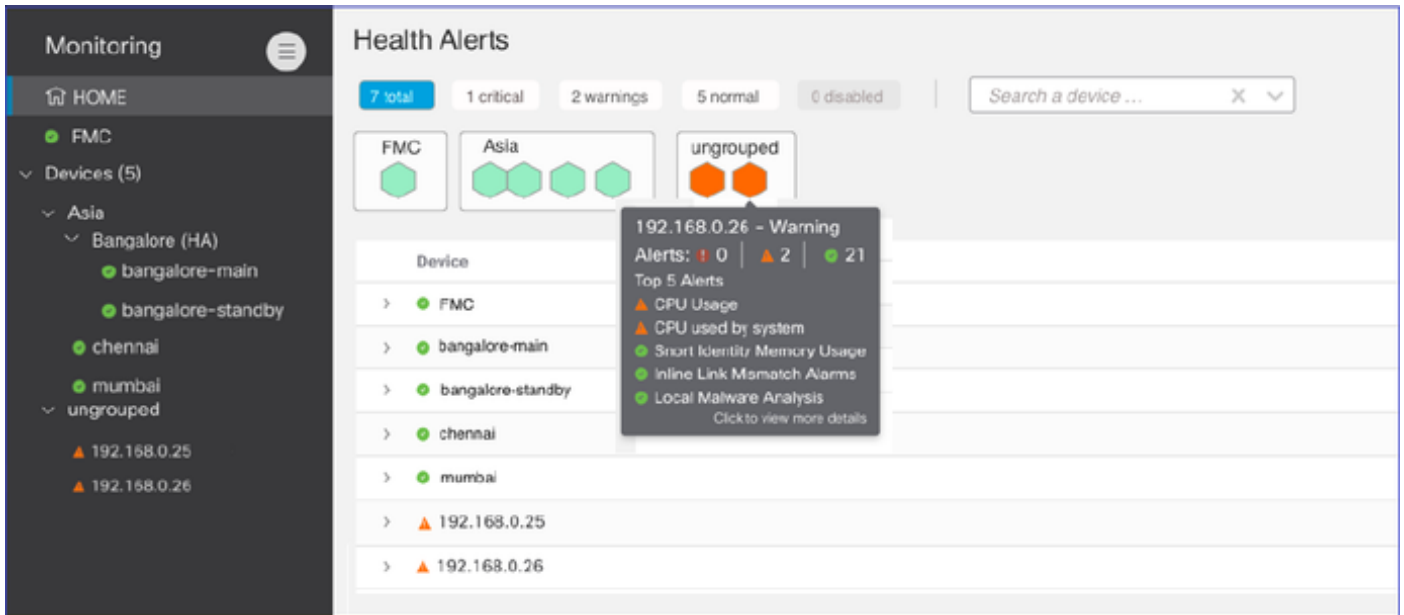




Interfaz de usuario de FMC: Página Nuevo estado de mantenimiento

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.



Interfaz de usuario de FMC: eventos de estado del dispositivo

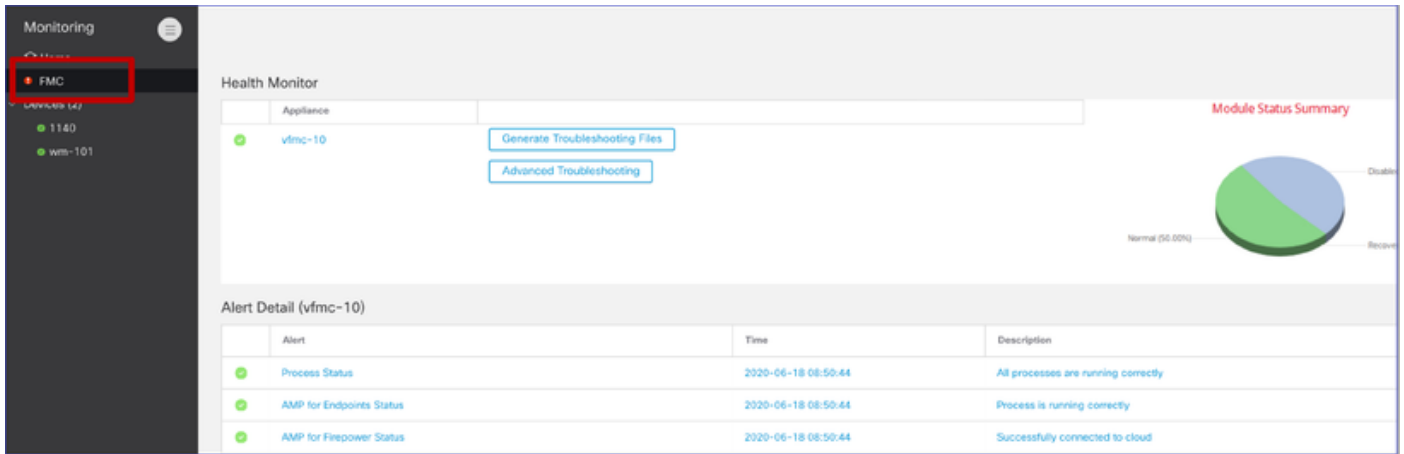
Haga clic en el dispositivo en el panel inferior para mostrar los eventos de estado asociados al dispositivo. Las alertas se ordenan por su estado (gravedad).

Página Supervisión de estado

>	▲ 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

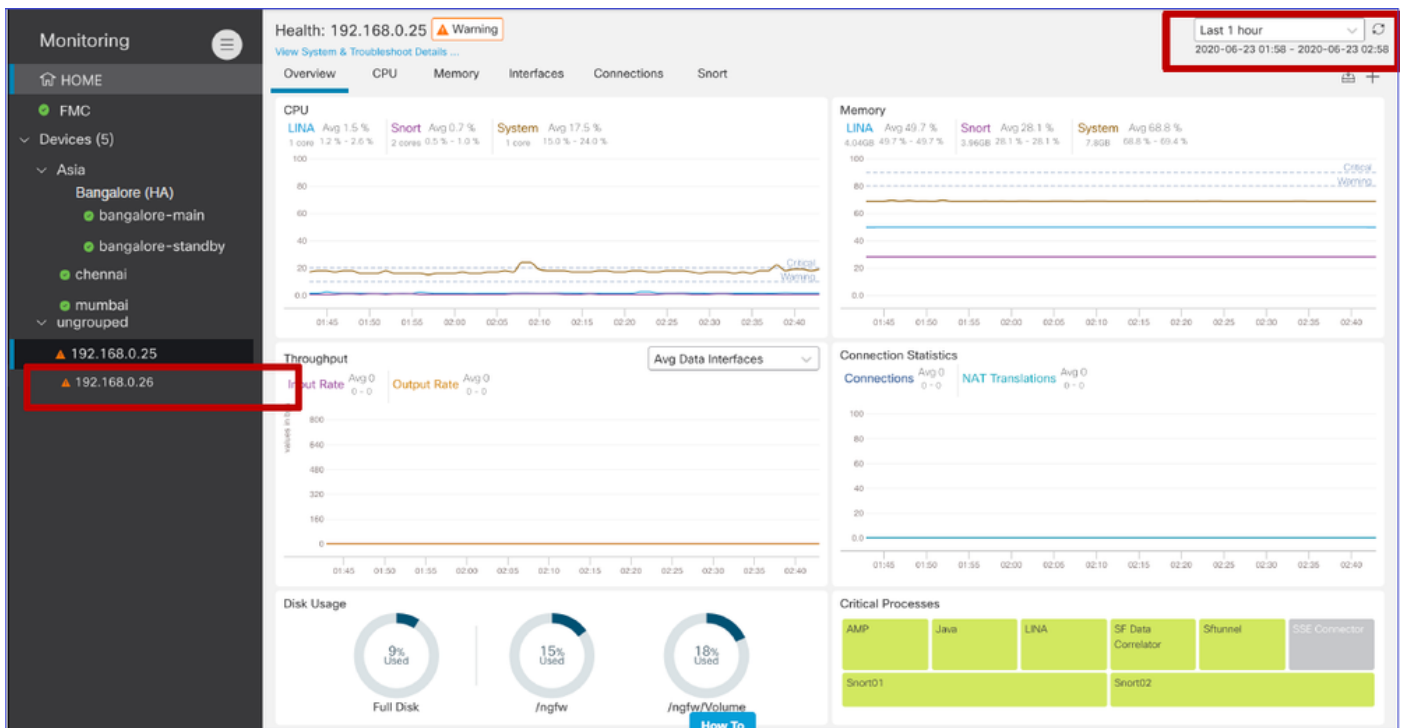
Interfaz de usuario de FMC: la supervisión de estado de FMC no ha cambiado

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



### 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

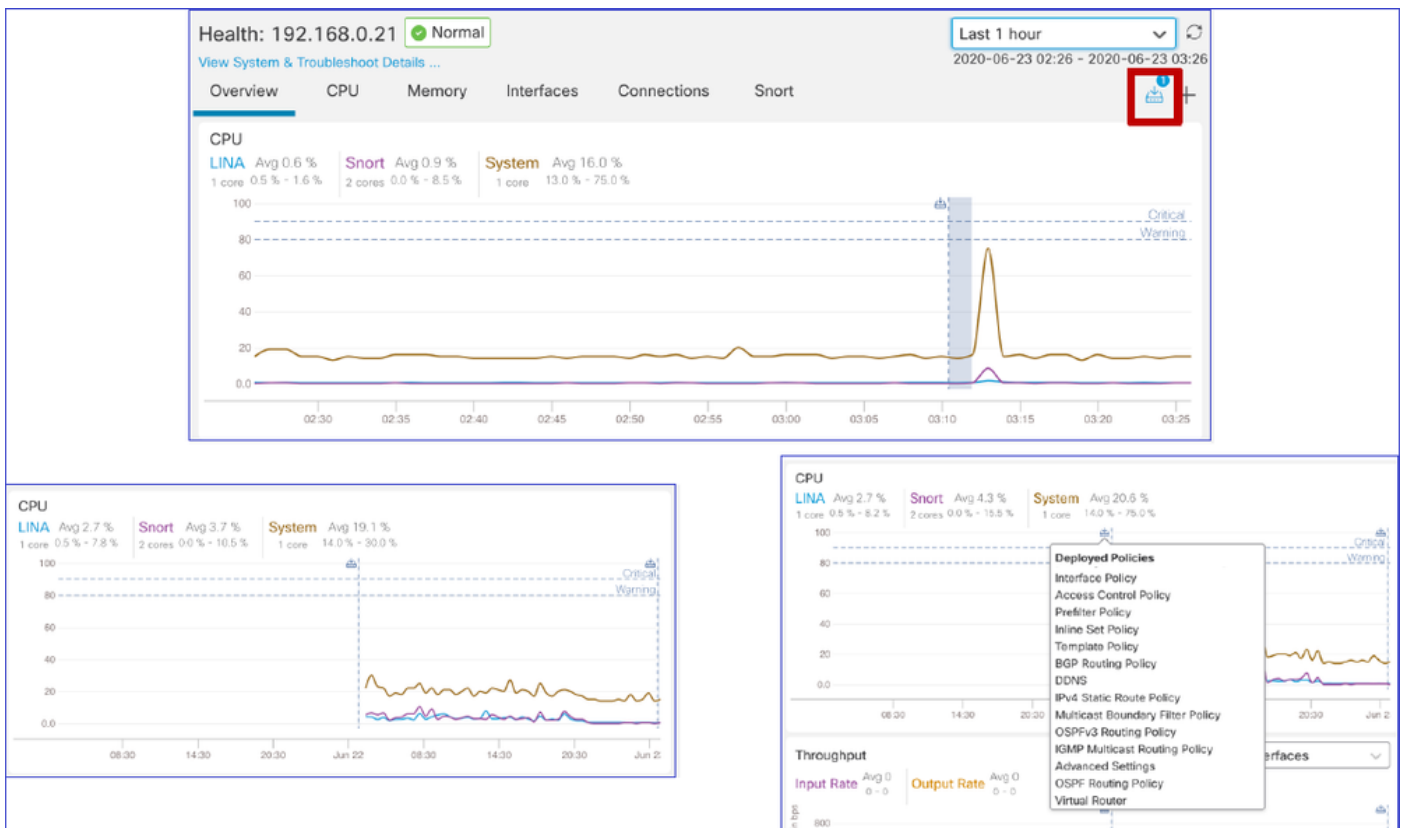


### Interfaz de usuario de FMC: superposición de datos de implementación

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

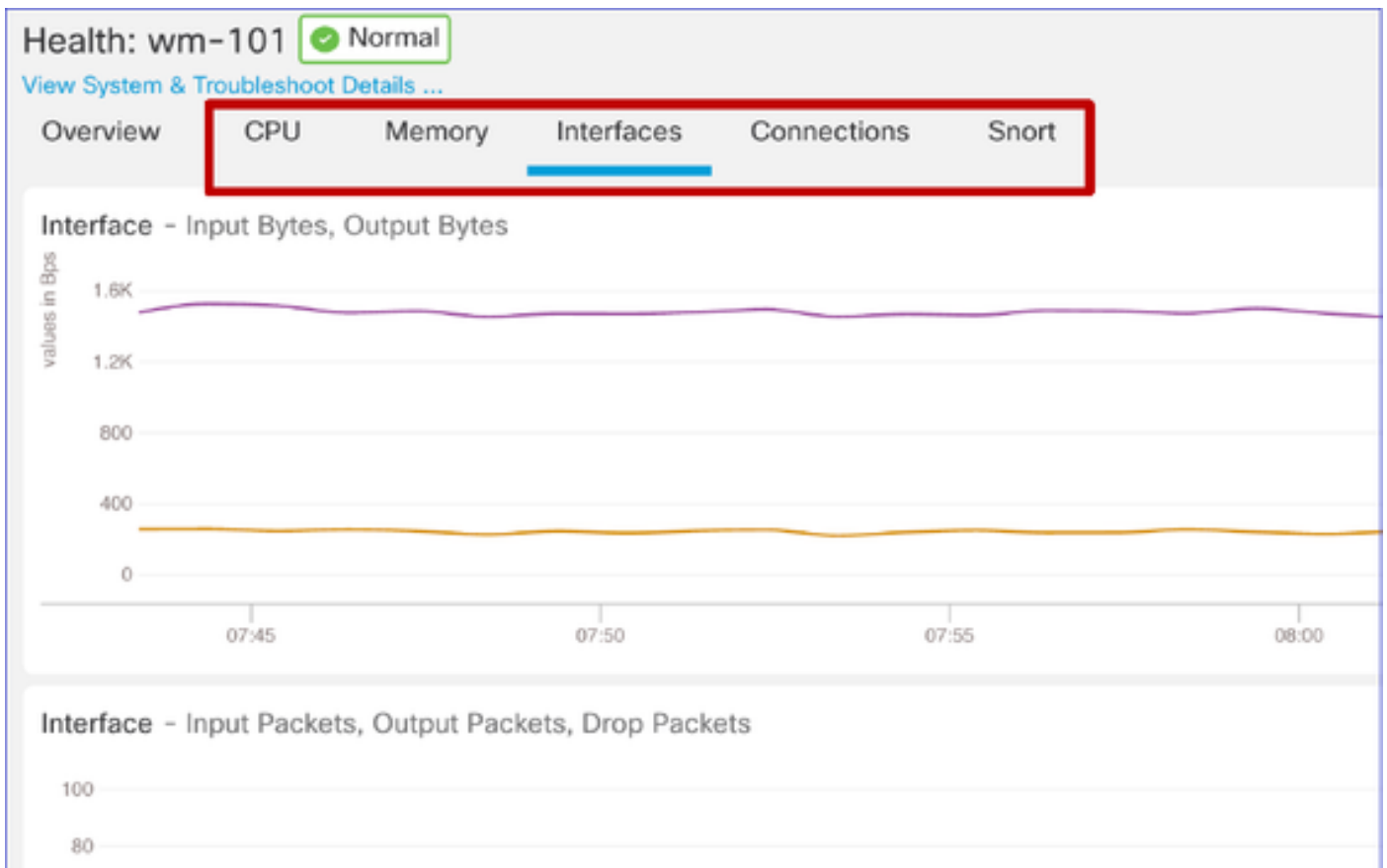
- El icono indica el número de implementaciones durante el rango de tiempo seleccionado
- La banda aparece para indicar la hora de inicio y finalización de la implementación.
- En caso de varias implementaciones, aparecen varias bandas/líneas
- Haga clic en el icono situado en la parte superior de la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

## detalles

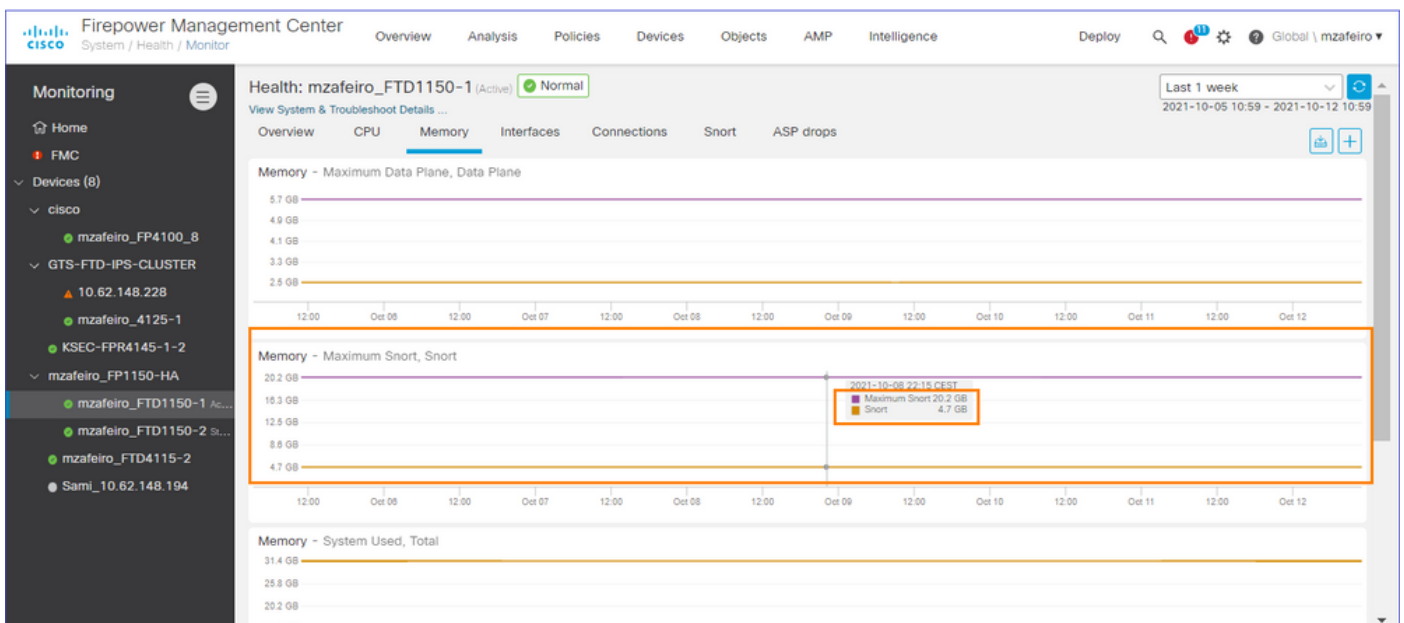


Interfaz de usuario de FMC: paneles prediseñados para dispositivos

- 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.



FTD Snort Memory - ¿De dónde se origina?

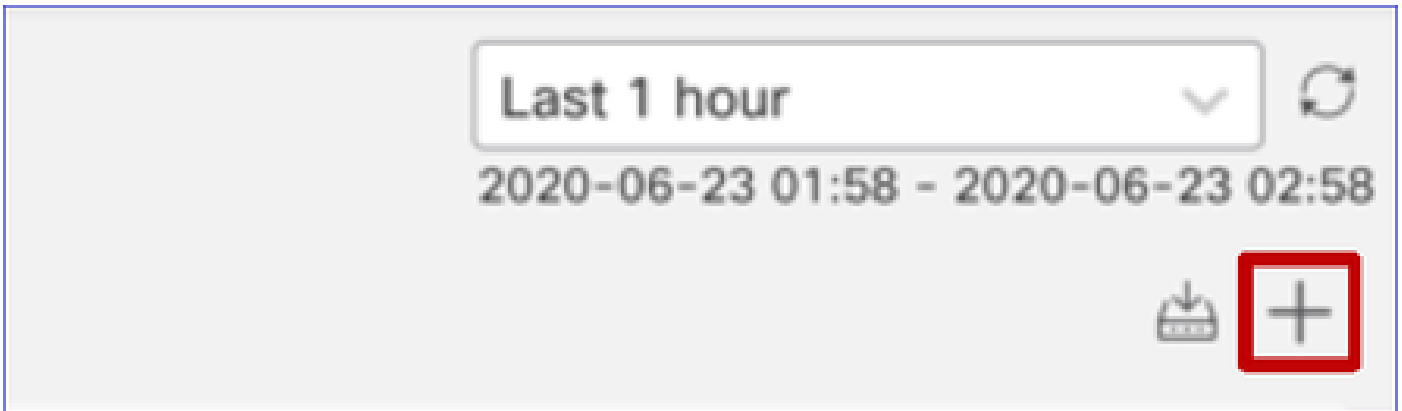


Interfaz de usuario de FMC: se pueden crear paneles personalizados

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 inter-related. Select predefined correlation groups or custom to specify your own metrics.

Correlation Group\*

CPU - Snort ▼

[Hide Details](#)

Dashboard Name\*

Correlation-CPU-Snort

**Metrics**

Chosen metrics will be displayed as portlets in the dashboard.

CPU <span style="float: right;">▼</span>	Snort <span style="float: right;">✕</span>	<span style="float: right;">✕</span> <span style="float: right;">▼</span>	<span style="float: right;">🗑</span>
Interface <span style="float: right;">▼</span>	Input Packets <span style="float: right;">✕</span>	<span style="float: right;">✕</span> <span style="float: right;">▼</span>	<span style="float: right;">🗑</span>
Deployed Configuration <span style="float: right;">▼</span>	Number of rules <span style="float: right;">✕</span>	<span style="float: right;">✕</span> <span style="float: right;">▼</span>	<span style="float: right;">🗑</span>
Deployed Configuration <span style="float: right;">▼</span>	Number of ACEs <span style="float: right;">✕</span>	<span style="float: right;">✕</span> <span style="float: right;">▼</span>	<span style="float: right;">🗑</span>

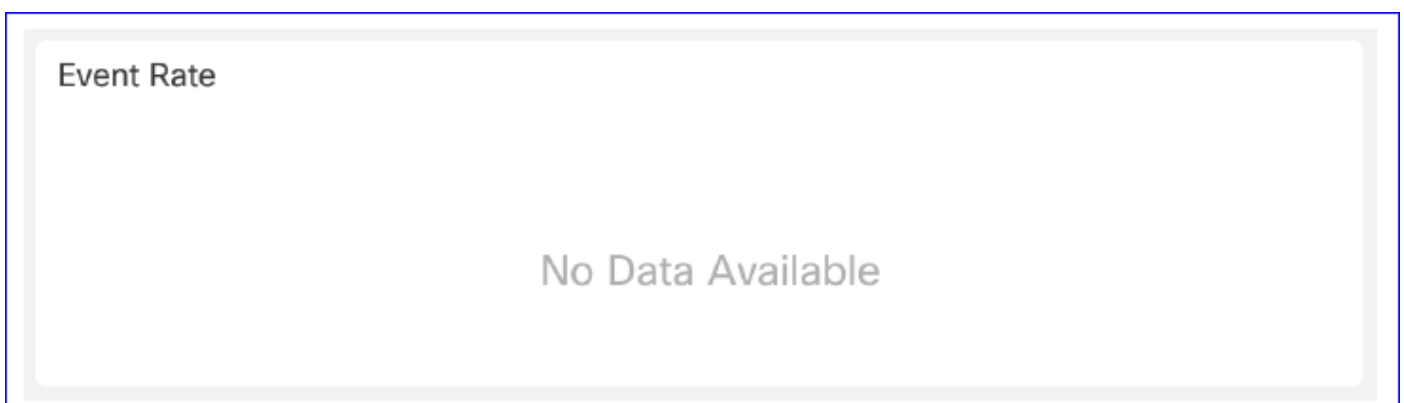
[Add Metrics](#)

[Cancel](#) [Add](#)

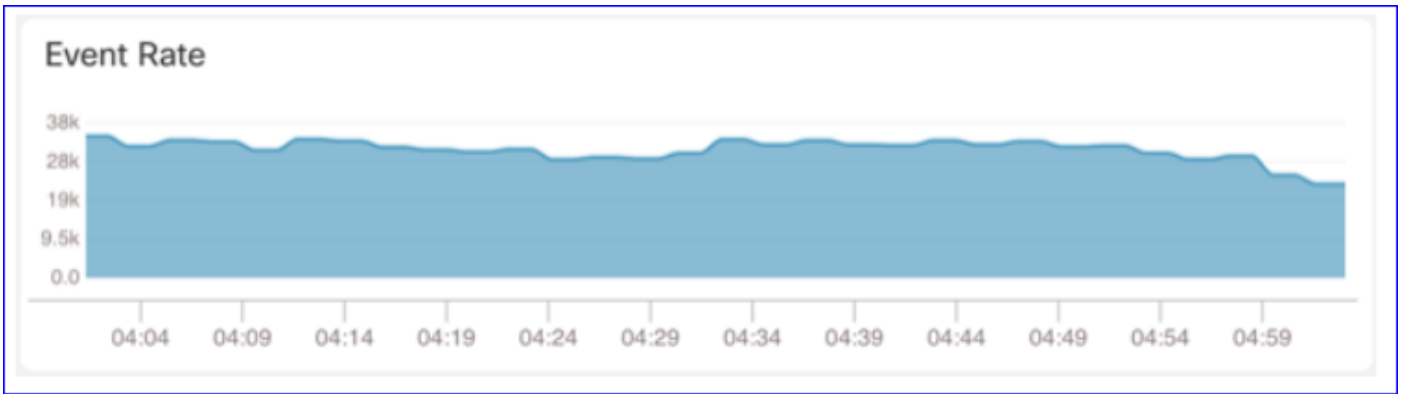
Recopilación de datos desde (dispositivo): GUI

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:



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

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a user profile 'syed'. The main content area is divided into several monitoring dashboards: CPU (Data Plane, Snort, System), Memory (Data Plane, Snort, System), Throughput (Input Rate, Output Rate), and Connection Statistics (Connections, NAT Translations). Below these dashboards is the Chrome DevTools console, which displays a stack trace for an error in 'index.js:11'. The stack trace includes frames for 'FadeIn', 'Suspense', 'Root', 'MessageProvider', 'ToastProvider', 'FeatureFlagProvider', 'Router', 'InputModeProvider', 'IntegrationProvider', 'ThemeProvider', 'ConnectFunction', 'IntlProvider', 'LocaleProvider', 'ConnectFunction', 'Provider', 'ReactQueryCacheProvider', 'QueryCacheProvider', 'Provider', and 'StrictMode'.

Ejemplo de registro de consola del explorador



Console Tab

Exception details



## 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).