升级FP — 设备运行状况监控

目录

简介

本文档介绍6.7和7.0版本中添加的新设备运行状况监控功能。

背景信息

问题:

运行状况监控系统提供对设备性能的可视性，以便进行被动调试和主动操作。

通过以下方式获得全面的可视性和分析：

- 关键指标的趋势图
- 事件重叠
- 可自定义的控制面板
- 统一运行状况监控架构 — 查看所有经理的相同数据
- 大量新指标和指标的可扩展性可增加更多指标

7.0版本中的新增功能

与FP 7.0相比有何新内容或不同之处

- 支持HA的FMC控制面板
- 超过110项新指标用于FTD
- FTD拆分大脑方案的运行状况警报
- 较新的运行状况度量的自定义运行时间间隔

好处

- 通过提供关联来自不同子系统的数据和设备上的资源的能力来帮助进行系统调试
- 各种系统性能指标的可视性
- 容量规划

6.7中的新功能

与之前版本相比，新版本或新版本（高级）：

- FMC上用于设备运行状况监控的新用户界面
- FTD设备REST API：设备度量API：增加了许多新度量
- FMC API：新API：运行状况警报、运行状况指标和部署详细信息
- 高级市场概述，实际应用
- 通过提供关联来自不同子系统的数据和设备上的资源的能力来帮助进行系统调试
- 可视性
- 容量规划

功能概述

工作原理

- FP 7.0中的设备运行状况监控
- 为FMC提供趋势图表、重叠和自定义控制面板的全新运行状况控制面板
- FTD控制面板中可用的新FTD指标
- 110多个指标，涵盖12个类别
- FTD API：使指标可供外部实体查询

在引擎盖下面，

- 使用Telegraf（开源指标收集框架）收集设备的运行状况

其他说明

运行状况监控数据可用

- 在FMC运行状况控制面板中，可从系统菜单(System > Health > Monitor)访问
- 从FMC REST API
- 当设备由FDM通过FTD设备REST API管理时

某些指标（FMC和FTD）默认处于禁用状态

- 需要启用并部署运行状况策略中的运行状况模块，才能显示某些指标。

实施FP 6.7 IFT'ers所要求的增强功能

- 默认情况下自动刷新
- 使用控制面板上的自定义时间范围进行筛选
- 在接口选择器中按用户定义的名称（以及物理接口名称）选择接口
- 从运行状况监控器“主页”(Home)页面交叉启动设备控制面板

FP 6.7中的设备运行状况监控

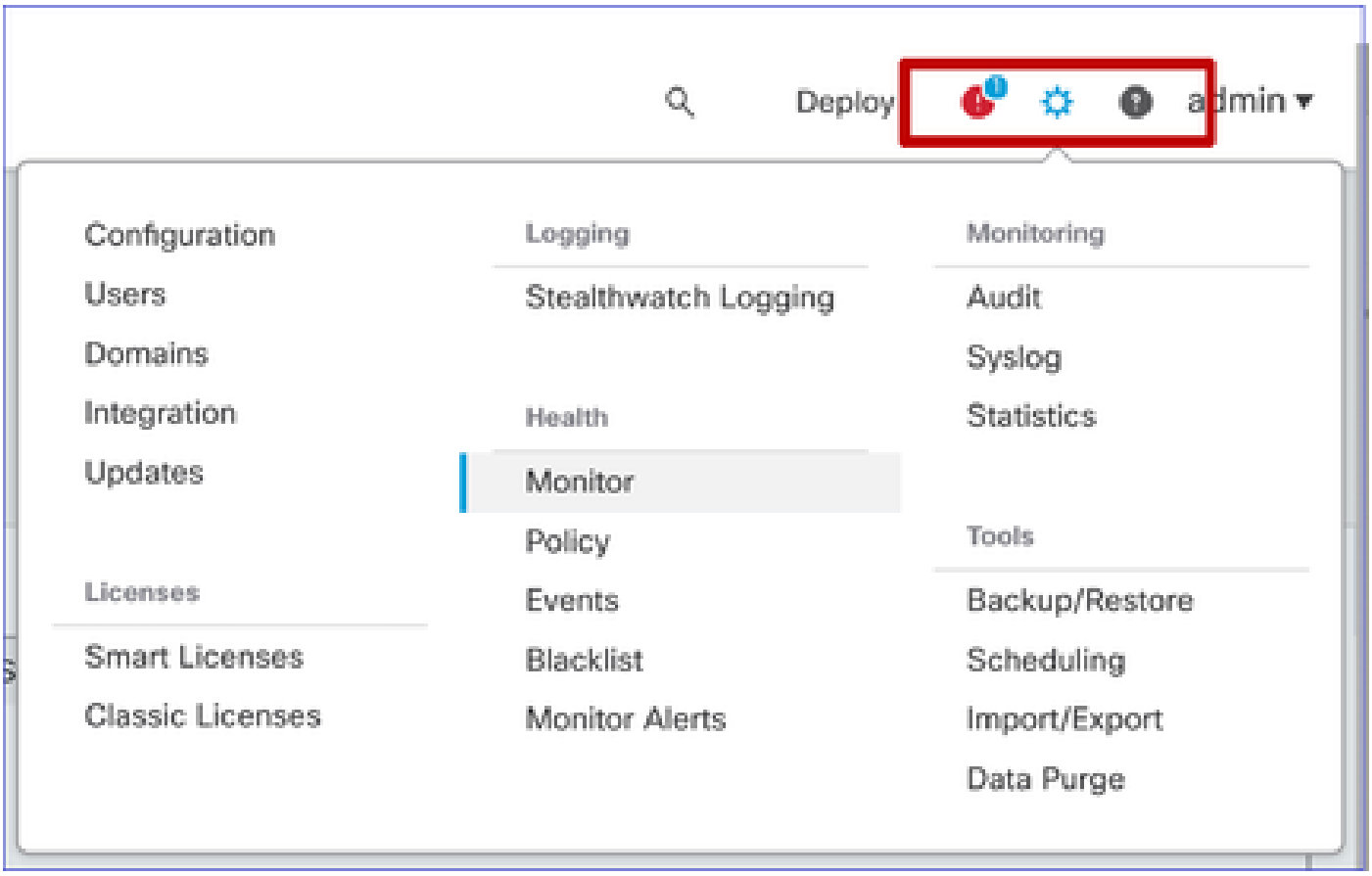
- FMC上的新UI，提供趋势图、重叠和自定义控制面板。
- FTD API：使外部实体查询的度量相同

限制摘要：

- FDM GUI或CDO不支持此功能
- 不支持在新运行状况监控UI中监控FMC本身。
- 轮询间隔不可配置。不能为不同的设备配置不同的轮询间隔。所有轮询都以固定的一分钟间隔进行。

部署示例

- 无需特定部署即可测试该功能。只需将FMC和设备升级到FP 6.7。
- 运行状况监控数据位于FMC运行状况控制面板中，可从系统选项卡访问。



必备条件和支持的平台

支持的最低软件和硬件平台

支持的管理器最低版本	受管设备	需要支持的最低受管设备版本	备注
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	仅支持FTD
FTD设备REST API	FTD 6.7	FXOS 2.9.1 FTD 6.7	仅FTD设备REST API （不是FDM或CDO

			GUI)

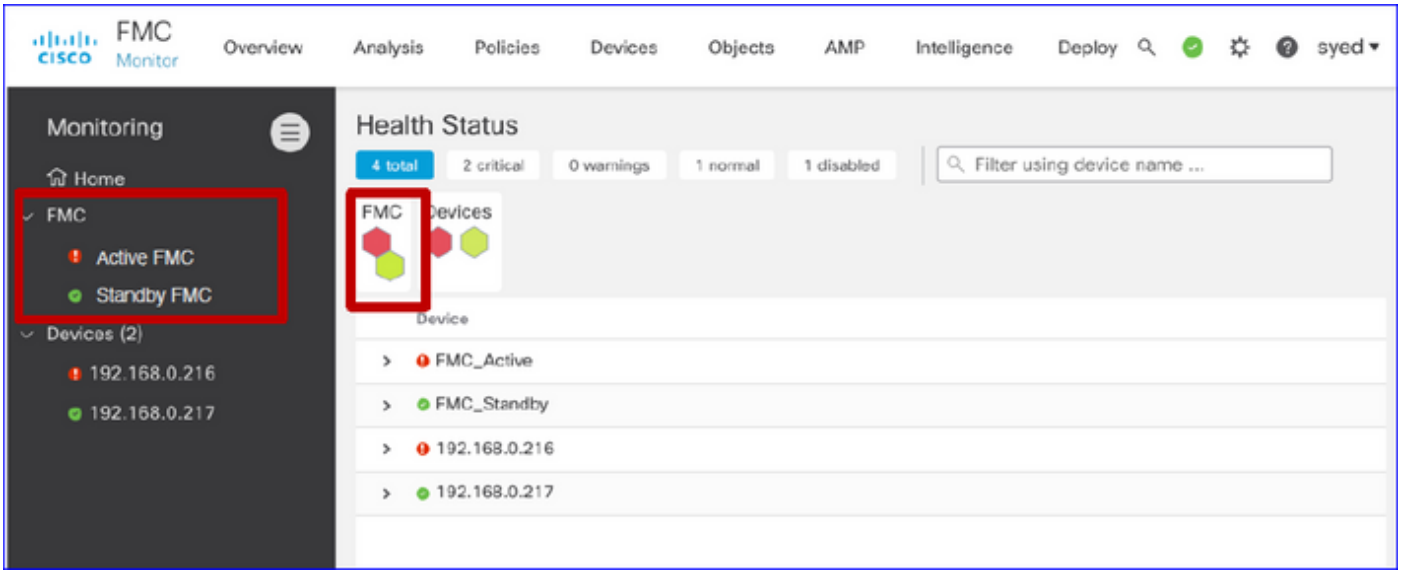
互操作性

互操作性无特定要求。

功能详细信息7.0

FMC UI：独立和高可用性支持

运行状况监控页面导航



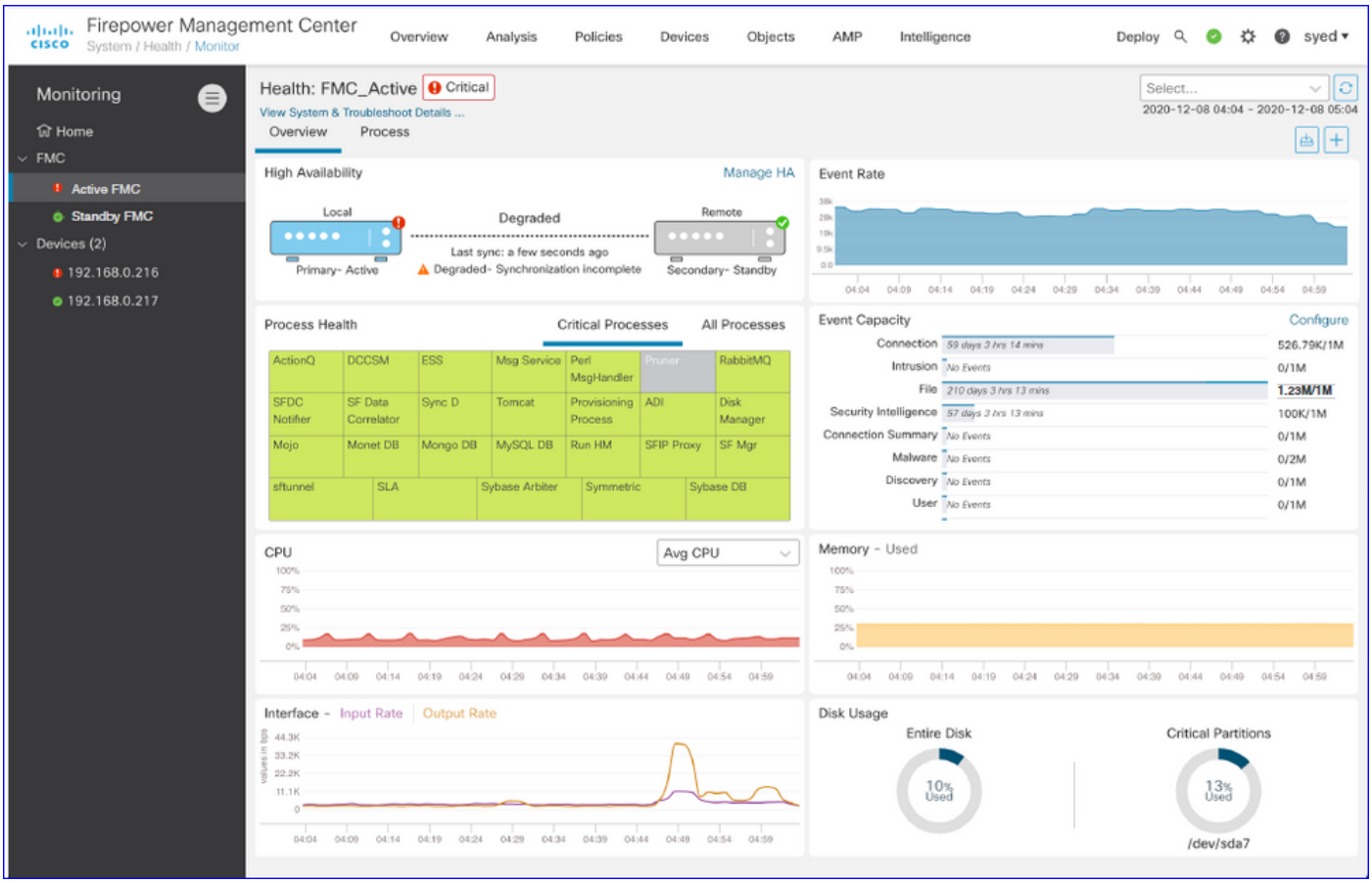
- 独立FMC显示为单个节点
- FMC HA显示为一对节点
- 显示每个FMC的运行状况

运行状况

- FMC HA以双六边形显示。
- FMC主用和备用设备也在警报表中列出。

FMC控制面板

7.0中的FMC运行状况监控仪表板



以下内容的摘要视图：

- 高可用性
- 事件速率和容量
- 进程运行状况
- CPU
- 内存
- 接口
- 磁盘

此控制面板可用于活动和备用FMC。用户可以创建自定义控制面板以监控他们选择的指标。

FMC控制面板：FMC HA面板

高可用性面板显示

- 当前高可用性状态
- 主用与备用
- 上次同步时间
- 设备运行状况

FMC控制面板：事件速率和容量

事件速率

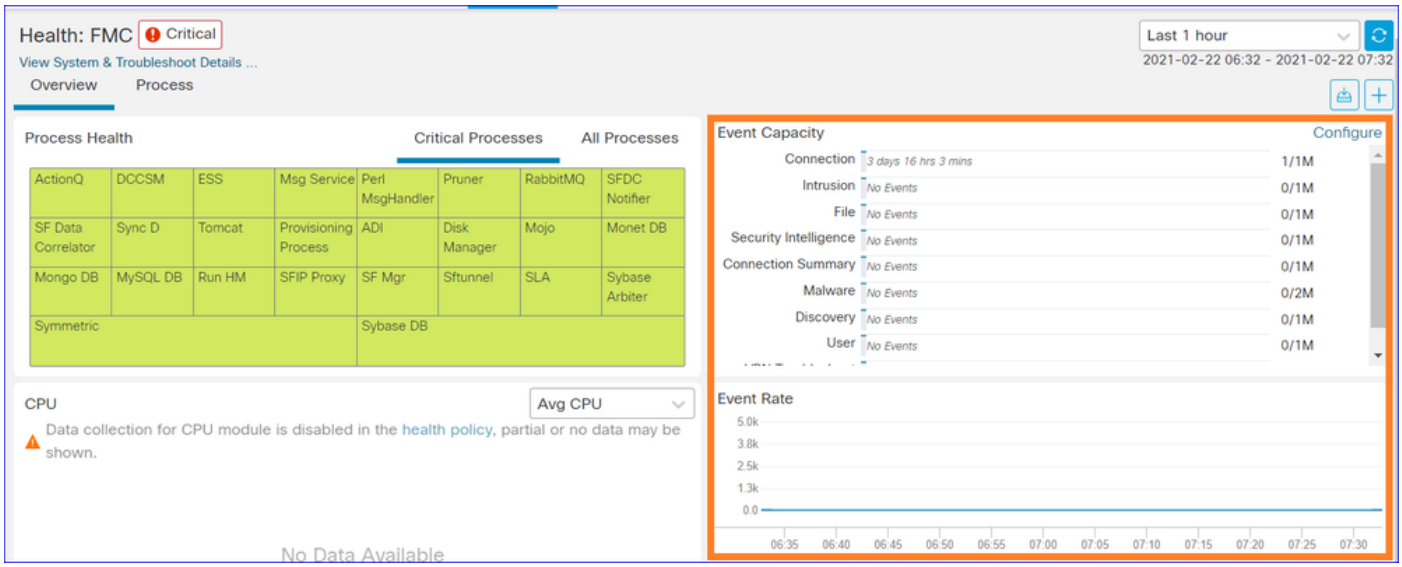
- 最大事件速率作为基准行
- FMC接收的总事件速率

事件容量

- 按事件类别划分的当前消耗量
- 事件的保留时间
- 当前与最大值

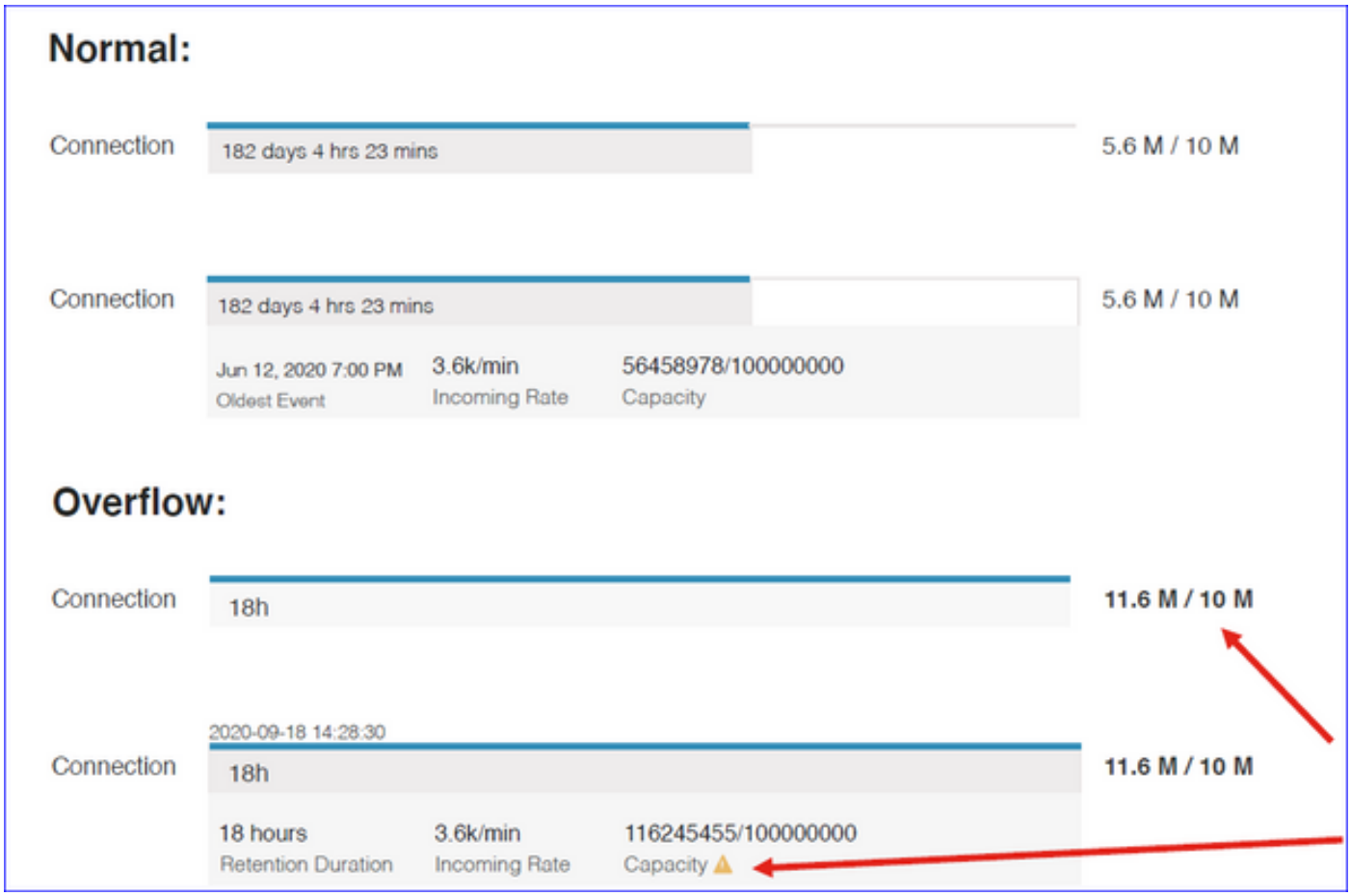
事件容量

- 容量溢出标记



FMC控制面板：事件容量

正常事件容量消耗状态



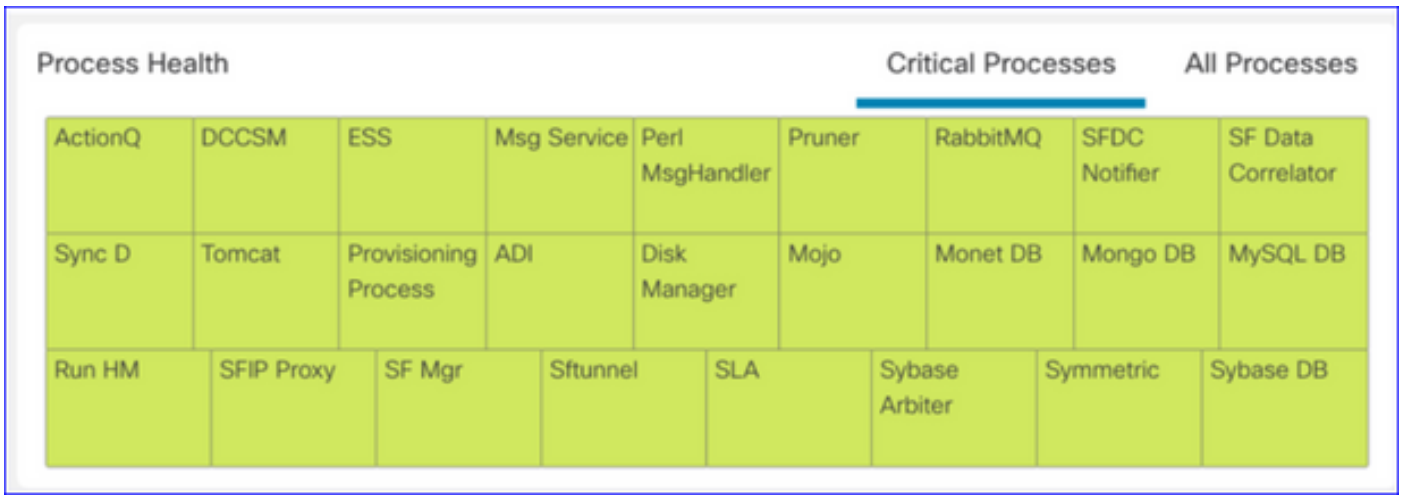
溢出情况，事件存储超出配置的最大容量。

- 粗体文本表示溢出
- 警告图标突出显示容量溢出

FMC控制面板：FMC流程面板

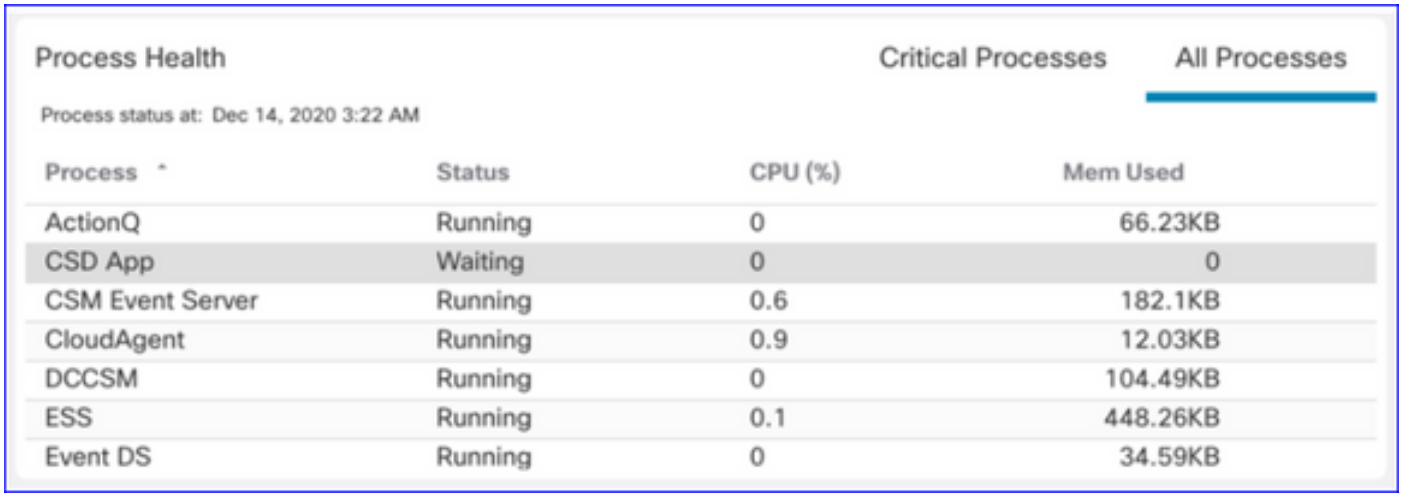
“关键进程”面板显示

- 进程当前状态
- 进程重新启动计数



进程面板显示所有“pmconfig”进程的以下度量：

- 当前状态
- CPU 使用情况
- 内存使用情况



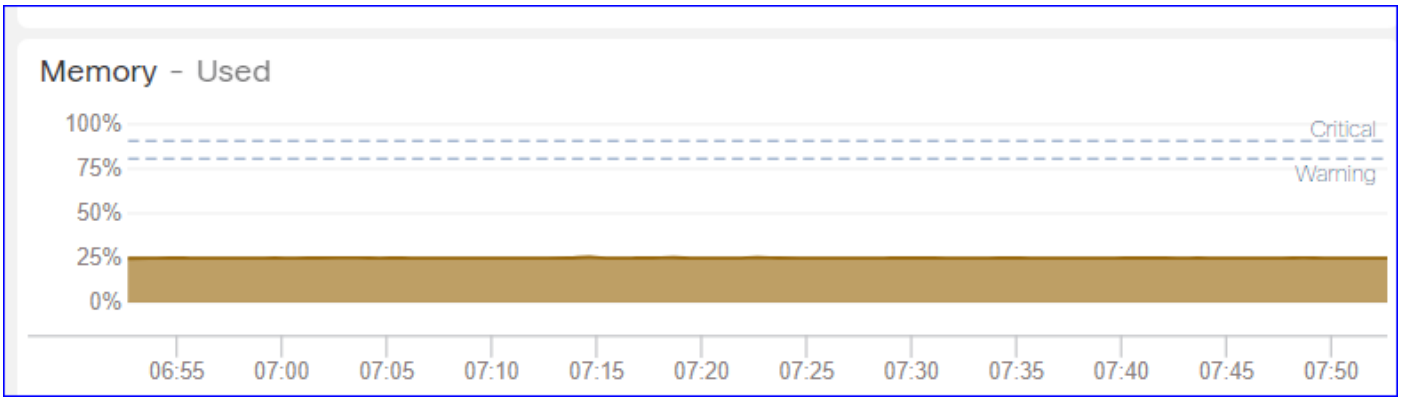
FMC控制面板：FMC CPU

CPU面板显示

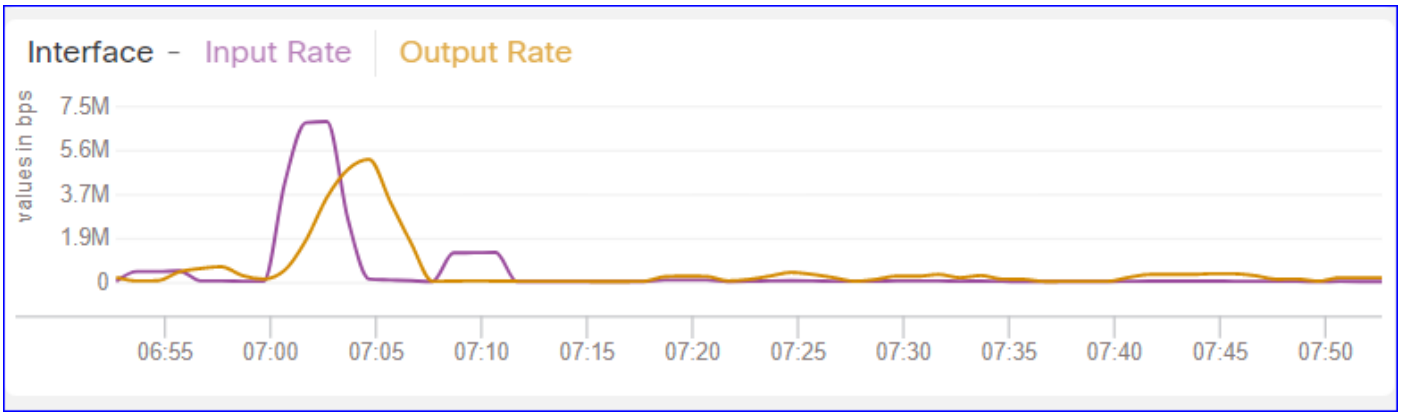
- 平均CPU（默认）
- 所有内核

FMC控制面板：其他面板

Memory面板显示FMC上的整体内存使用情况



接口面板显示所有接口的平均输入/输出速率

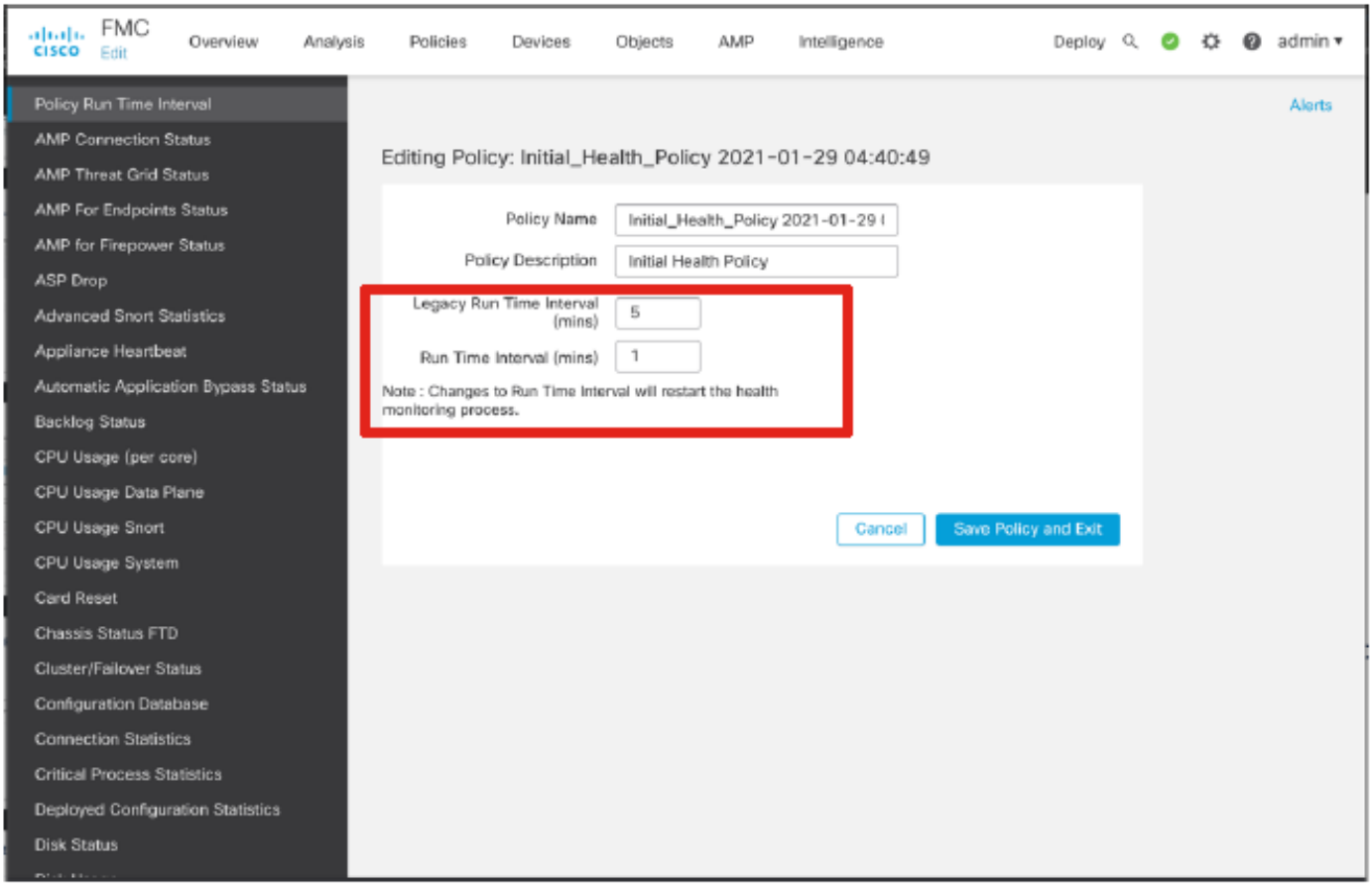


磁盘面板显示

- 整个磁盘容量
- 存储FMC数据的关键分区容量

运行时间间隔

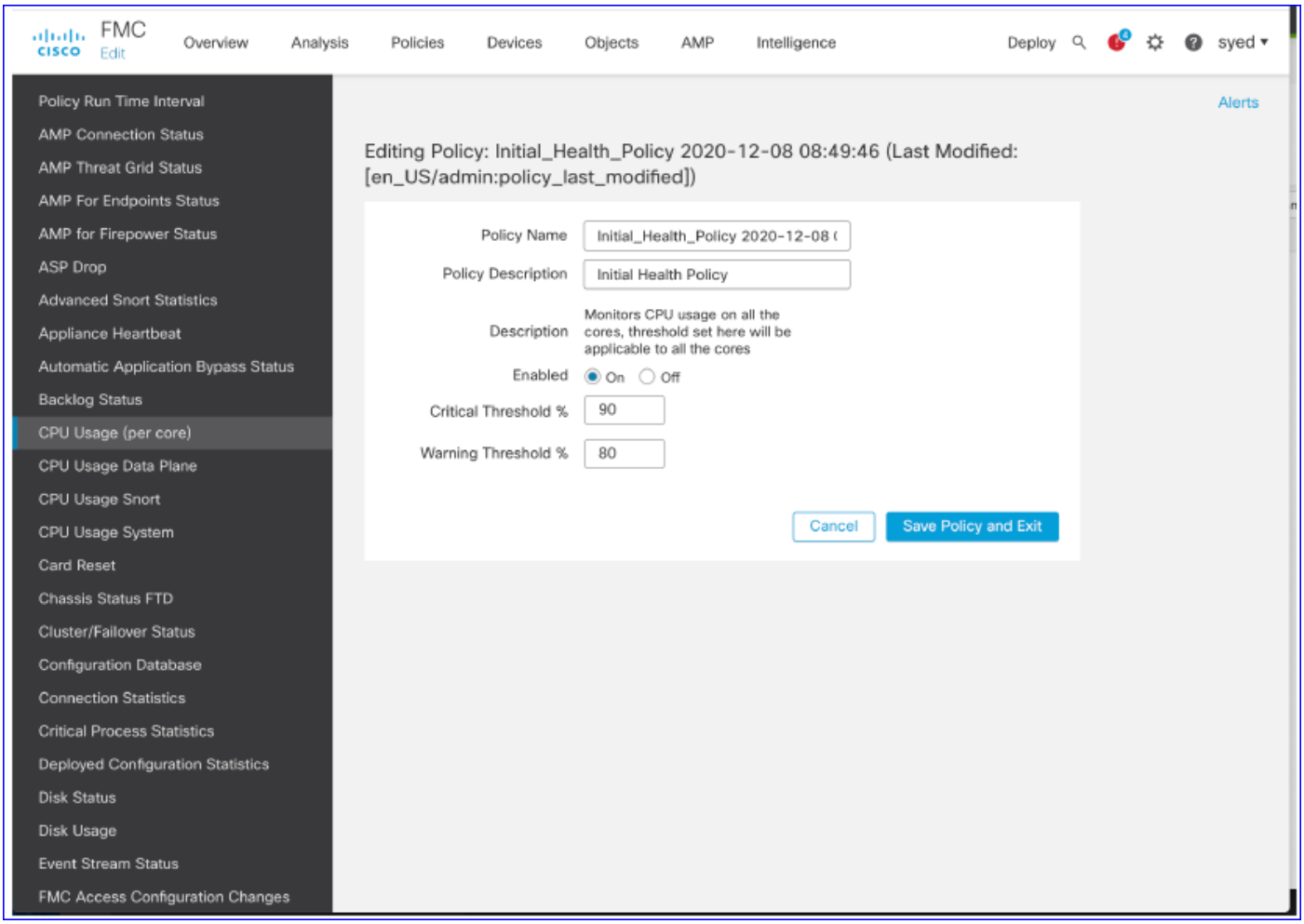
- 旧运行状况模块的运行时间间隔重命名为“旧运行时间间隔”(Legacy Run Time Interval)
- “Run Time Interval”（运行时间间隔）以新的基于电话的运行状况模块为目标
- 全局设置，影响所有设备



可用指标

可用于自定义控制面板的度量

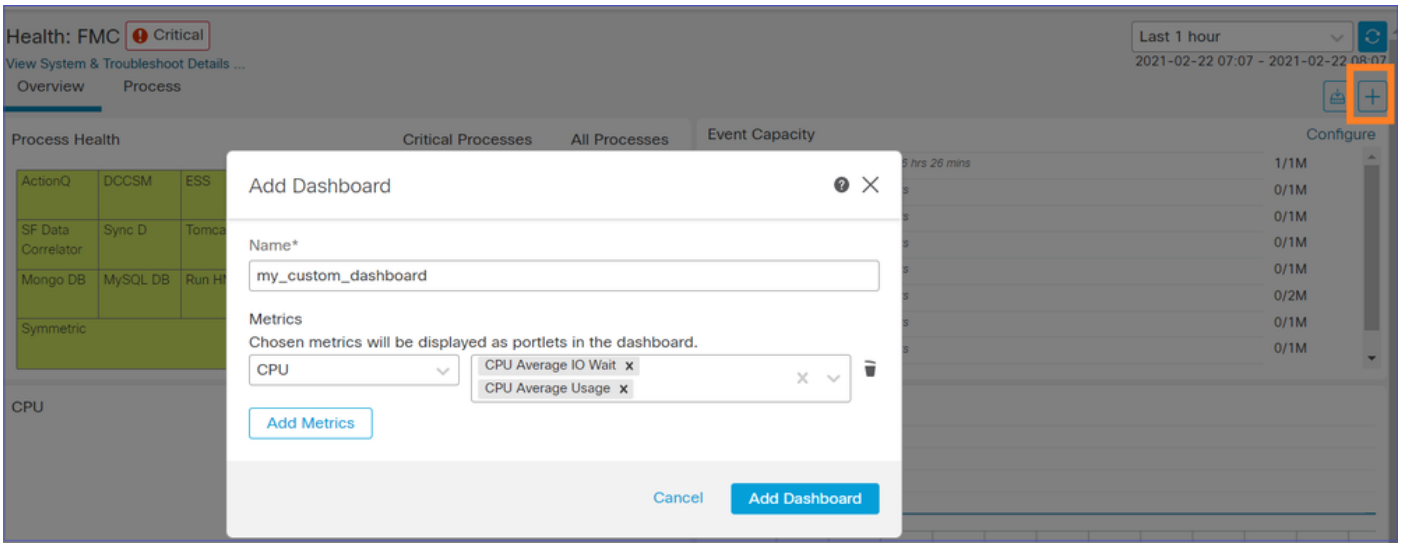
- 如果用户想要制作自定义控制面板，则这些幻灯片是可用指标的指南。
- 某些指标必须在运行状况策略中启用，才能在自定义运行状况控制面板中使用



FMC UI:FMC自定义控制面板

7.0中新增的FMC监控指标类别

- CPU
- 内存
- 接口
- 磁盘
- Event
- Process
- RabbitMQ
- Sybase
- MySQL



FMC UI:FMC指标

跨不同类别添加了40个指标（在自定义控制面板中提供）。要启用已禁用的度量，请在关联的运行状况策略(System > Health > Policy)中启用相应的运行状况模块。

指标组名称	默认启用	描述
CPU	无	监控FMC CPU
内存	Yes	监控FMC内存
磁盘	Yes	监控FMC磁盘使用情况
接口	Yes	监控FMC接口
Process	Yes	监控FMC进程
Event	Yes	监控事件速率
MySQL	无	监视MySQL
RabbitMQ	无	监控器RabbitMQ
Sybase	无	监控Sybase

FTD:FP 7.0中引入的指标

默认启用：默认情况下收集度量。要启用已禁用的度量，请在关联的运行状况策略(System > Health > Policy)中启用相应的运行状况模块。

指标组名称	默认启用	描述	Platform
机箱状态	Yes	监控不同的机箱参数，如风扇速度和温度。	仅适用于FPR2100和FPR1000平台
流分流	Yes	监控硬件流卸载统计信息	适用于FPR9300 和FPR4100平台
ASP丢包	Yes	监控Lina侧数据包丢弃	all
命中计数	无	监控访问控制策略规则的命中计数	all
AMP Threat Grid状态	Yes	监控与AMP的连接 Threatgrid	all
AMP连接状态	无	从FTD监控AMP云连接	all
SSE连接器状态	无	从FTD监控SSE云连接	all
NTP状态	无	监视NTP时钟同步参数 FTD	all
VPN 统计信息	Yes	监控S2S和RA VPN隧道统计信息	all
路由统计信息	Yes	监控Lina侧数据包丢弃	all
Snort 3性能统计信息	Yes	监控某些Snort3性能统计信息(perfstats)	all

xTLS计数器	无	监控xTLS/SSL流、内存和缓存的有效性	all

REST API、系统日志、SNMP

7.0中未引入新的FMC或FTD设备REST API。现有REST API支持7.0中添加的新指标。

系统日志和SNMP

系统日志

- 运行状况监控器的系统日志无更改

SNMP

- 用于“SNMP设备运行状况监控”的独立TOI

SAL/CTR/第三方产品集成

- 针对“Azure Application Insights”支持的独立TOI
- 未做具体更改以支持将“运行状况监控”与SAL/CTR/SecureX集成
- REST API可用于第三方集成

软件技术

功能详细信息6.7

针对FTD运行状况和性能的全新NGFW运行状况监控

帮助用户

- 被动调试，如发生问题后的根本原因分析
- 主动操作，如监控使用情况和饱和级别，以确定潜在的容量问题，从而帮助用户执行容量增强或重构。

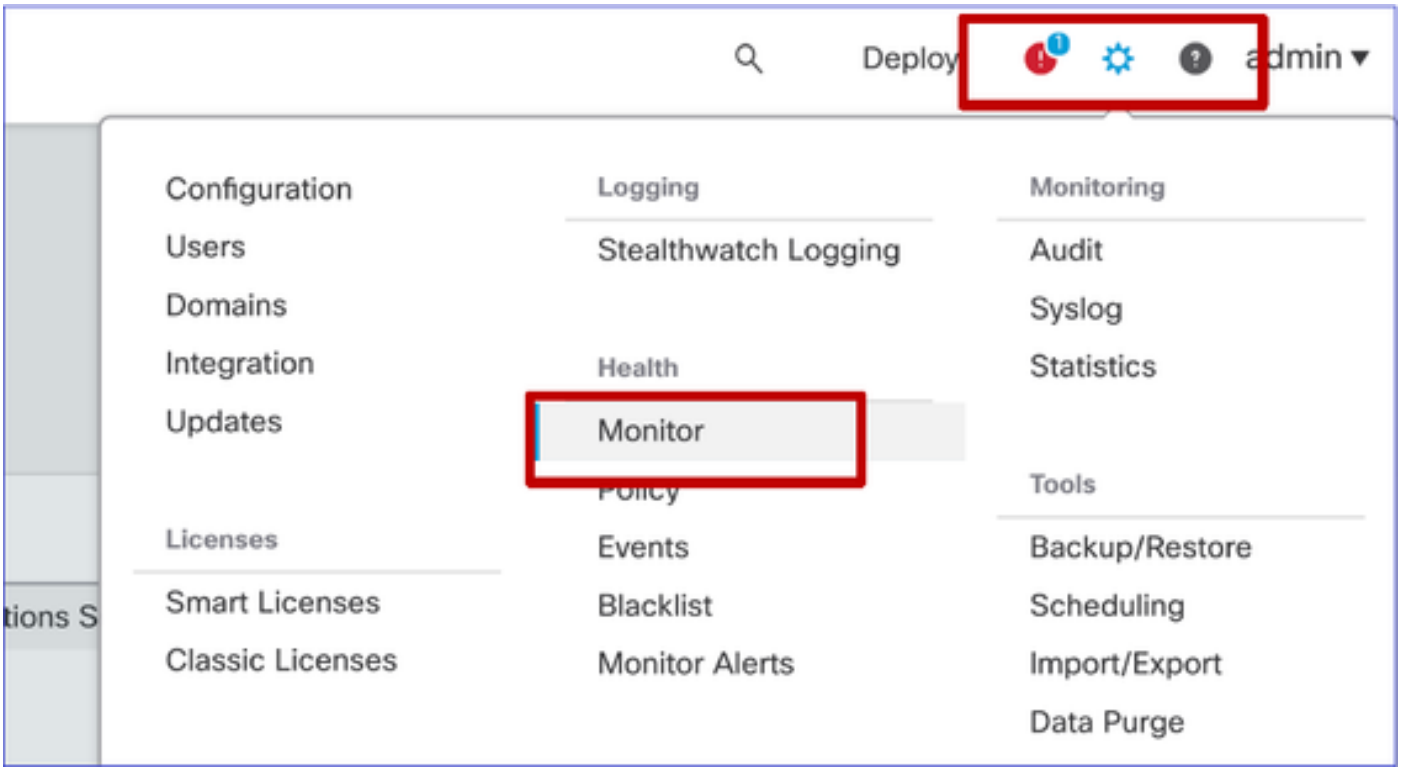
亮点

- 趋势图：趋势图可以非常轻松地检测异常并确定问题的根本原因。利用视觉检测技术可以发现检测趋势，并绘制不同度量之间的相关度以找出它们之间的因果关系。
- 事件重叠：事件重叠显示重要信息，例如趋势图上的配置部署和SRU更新，以指示因果关系。
- 可定制的控制面板：用户可创建自己的控制面板，将希望一起查看的指标分组到一个页面上。
- 统一运行状况监控架构：指标的单个收集和导出点，无论哪个经理对指标“感兴趣”。FTD API和FMC使用来自同一指标收集器的数据。
- 指标的可扩展性：该平台架构的目标之一是能够轻松添加新指标。这是通过使用开源指标收集和存储工具以及可自定义的控制面板来实现的。

FMC GUI

FMC UI：导航至运行状况

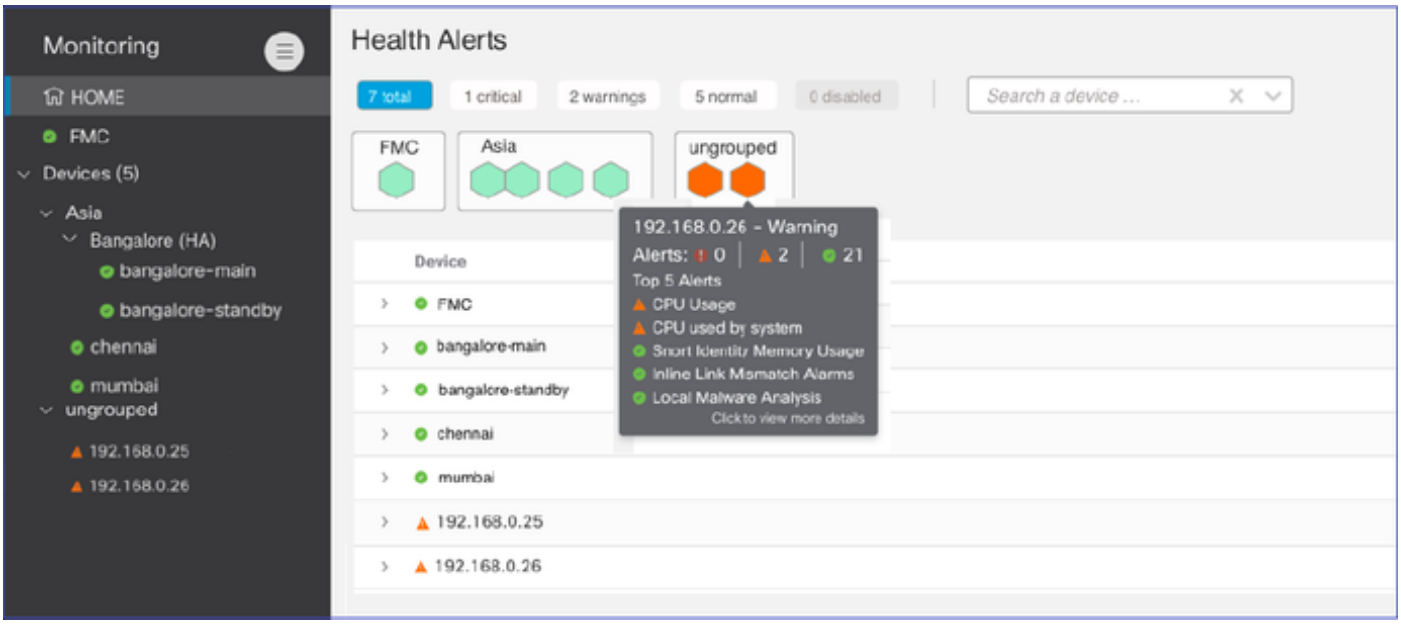
在FMC上，点击System图标> Health > Monitor以导航到Health Status页面。



FMC UI：新建运行状况状态页面

Health Status页面用于显示FMC管理的所有设备的运行状况概述，包括FMC的运行状况。

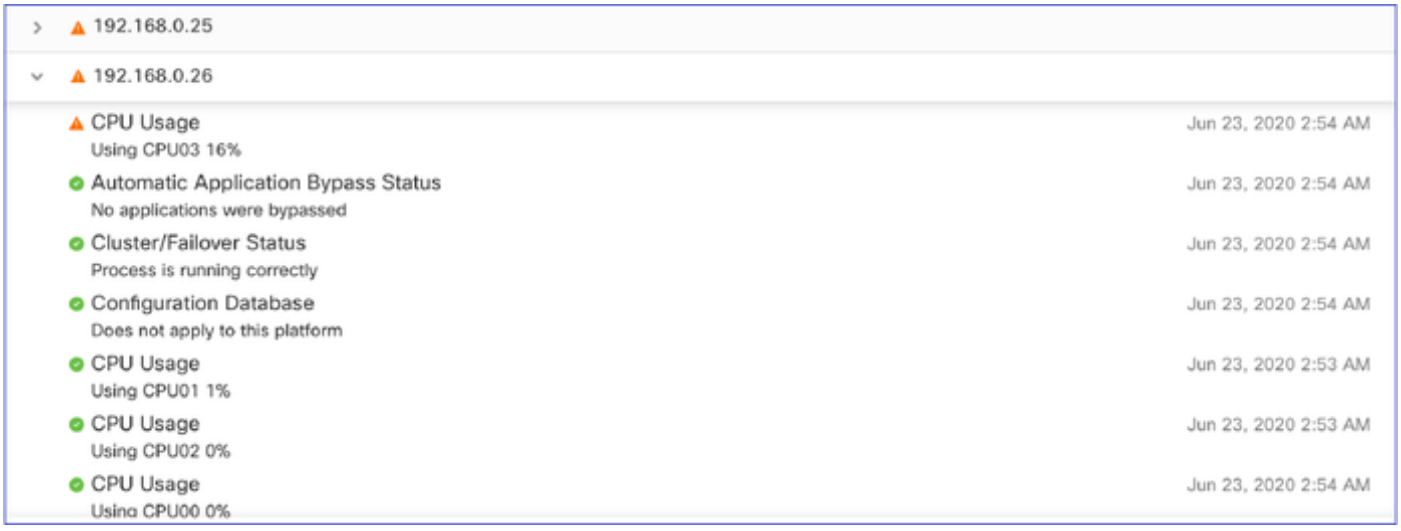
- 设备按其组/ha/集群分组。
- 设备左侧的点表示其运行状况
- 绿色 — 无警报
- 橙色 — 至少一个健康警告
- 红色 — 至少一个严重运行状况警报
- 将鼠标悬停在表示设备运行状况的六边形上时会显示运行状况摘要。
- 可以在运行状况策略中配置警告和严重阈值，与FP 6.7之前的配置方式相同。



FMC UI：设备运行状况事件

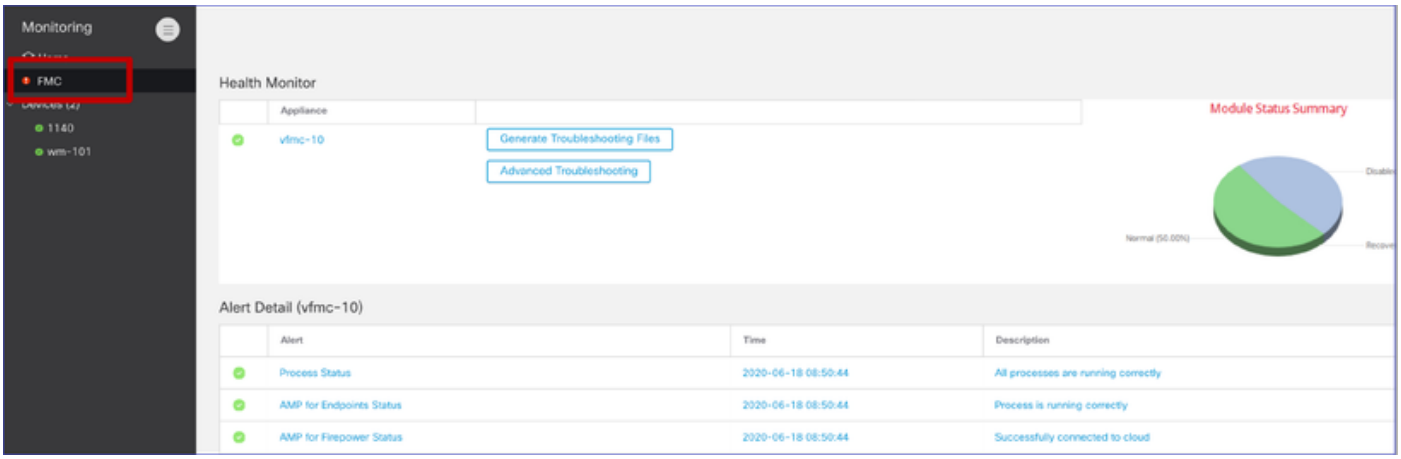
单击底部面板中的设备，显示与设备相关的运行状况事件。警报按其运行状况状态（严重性）排序。

运行状况监控页面



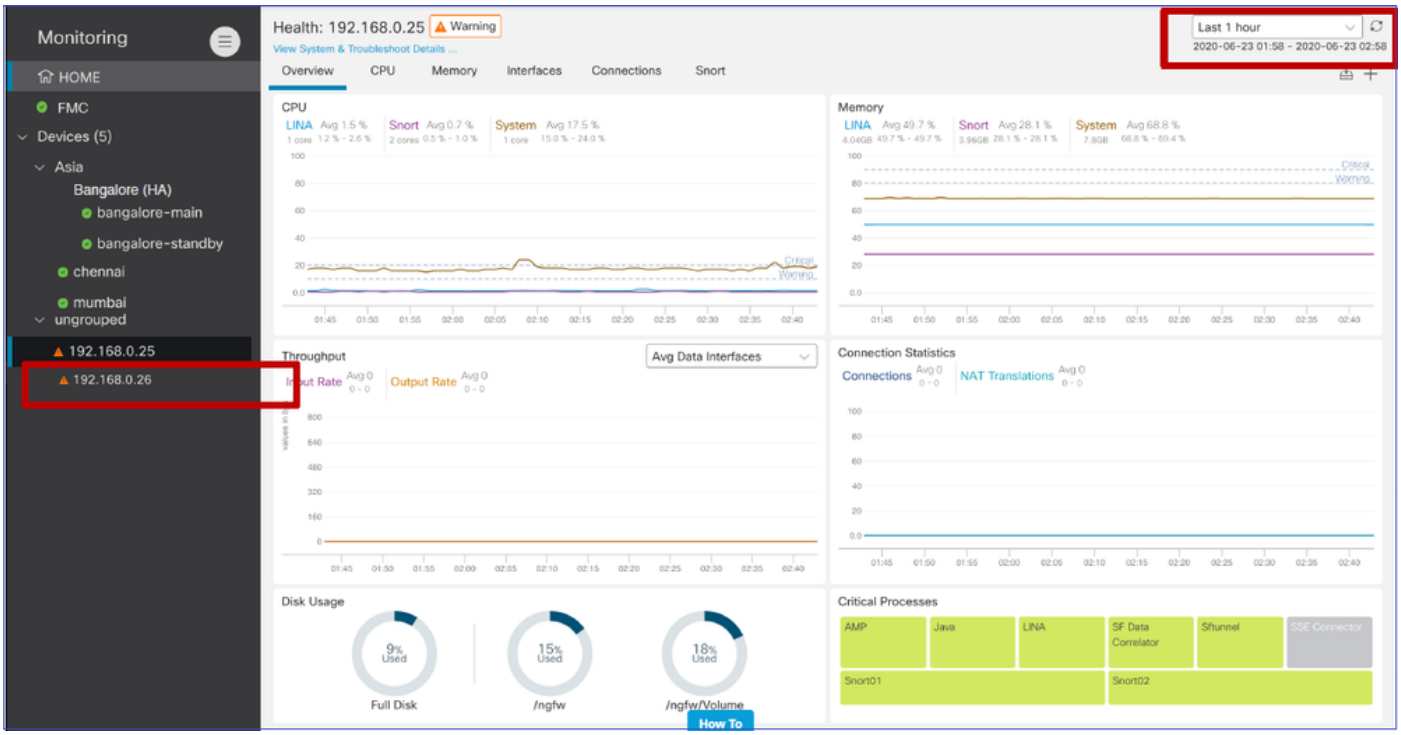
FMC UI:FMC运行状况监控未更改

FMC运行状况页面仍是旧页面。新用户界面仅支持带6.7+的FTD



FMC UI：新！设备控制面板

- 点击左侧窗格中的设备名称可进入设备的运行状况概述页面。
- 运行状况概述包含所有关键运行状况指标趋势图。
- 可使用各种时间范围（默认为过去1小时）
- 自动刷新以重新加载图表



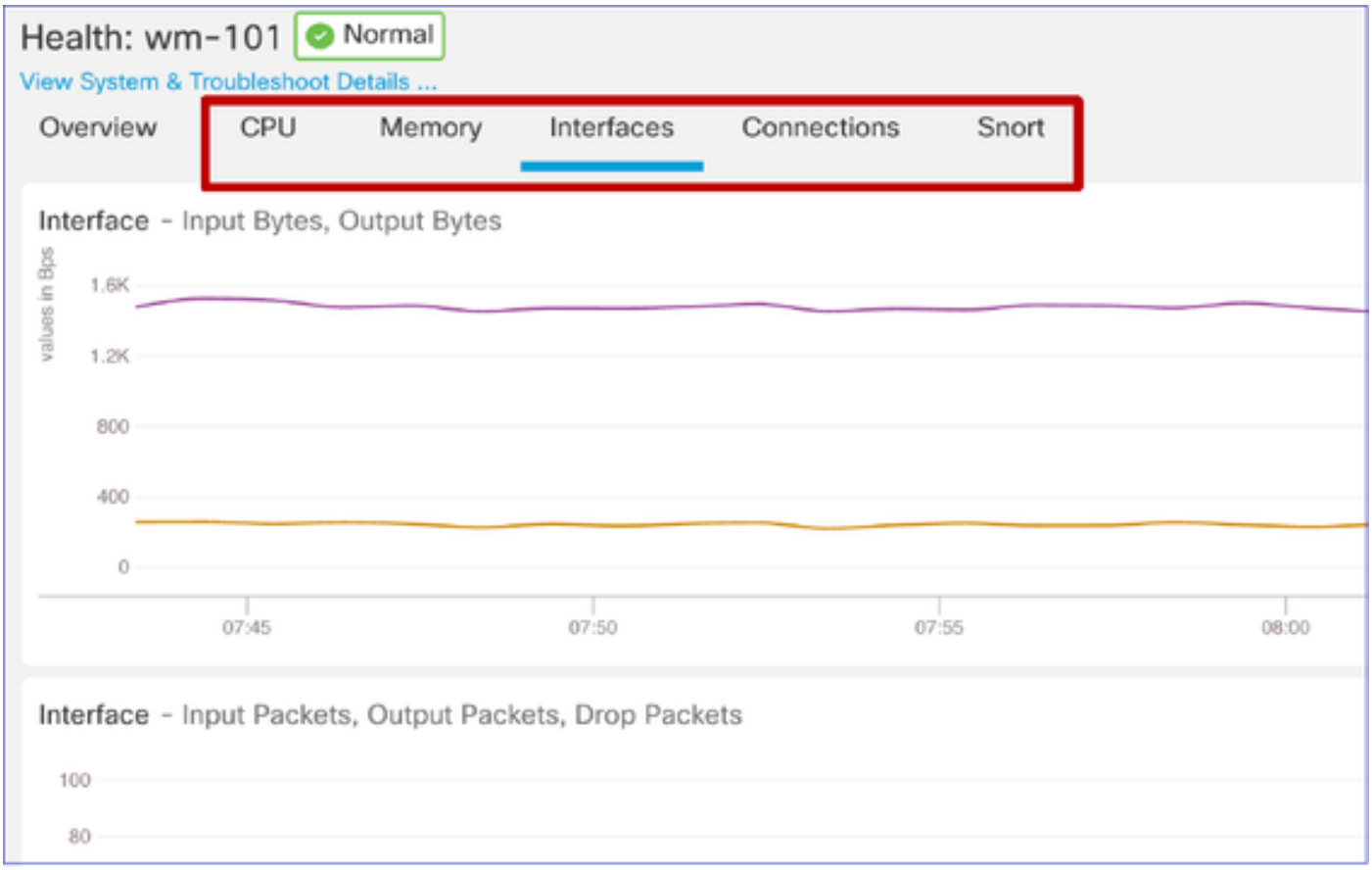
FMC UI：部署数据重叠

点击部署图标，在图上显示所选时间范围的部署覆盖详细信息

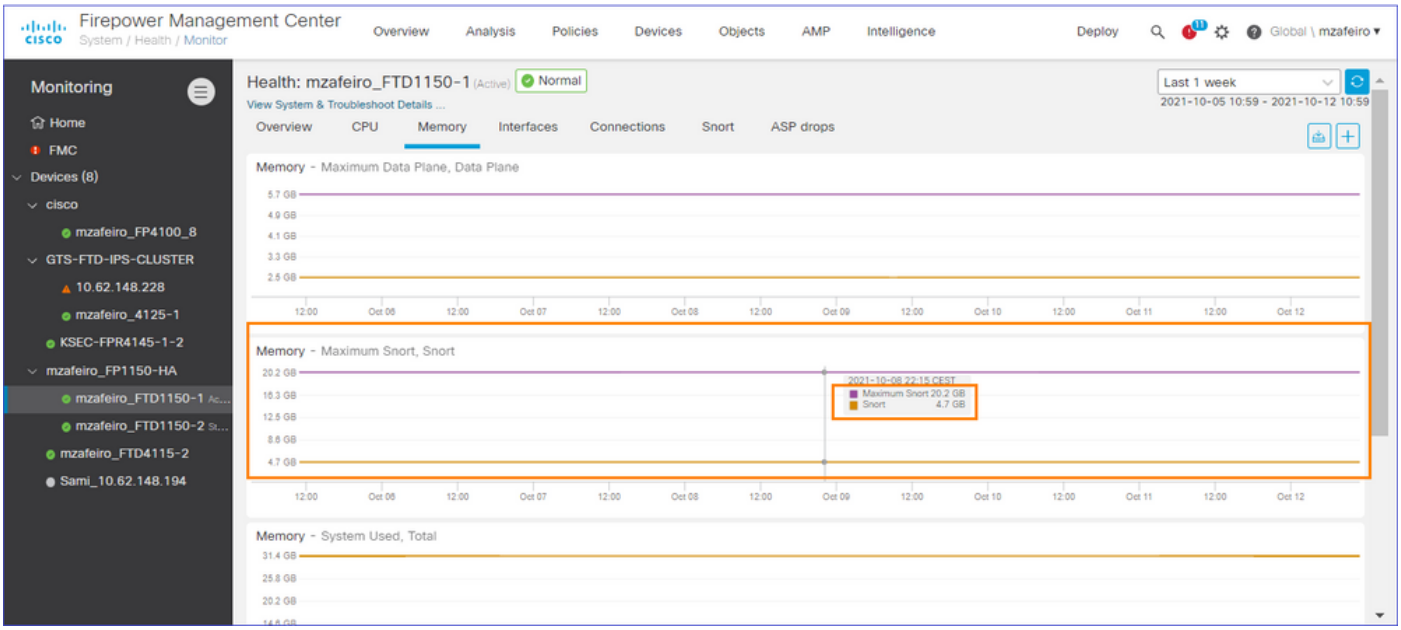
- 图标表示所选时间范围内的部署数量
- 显示频段，指示部署开始和结束时间。
- 如果部署较多，则会出现多个频段/线路
- 单击虚线顶部的图标以显示详细信息

FMC UI：设备预构建控制面板

- FMC UI中存在预构建的运行状况控制面板。
- 这些预构建的控制面板将相关的指标组合在一起。
- 接口控制面板具有所有接口相关度量的趋势图，例如输入/输出字节、数据包以及不同接口的平均数据包大小。



FTD Snort内存 — 源自哪里？

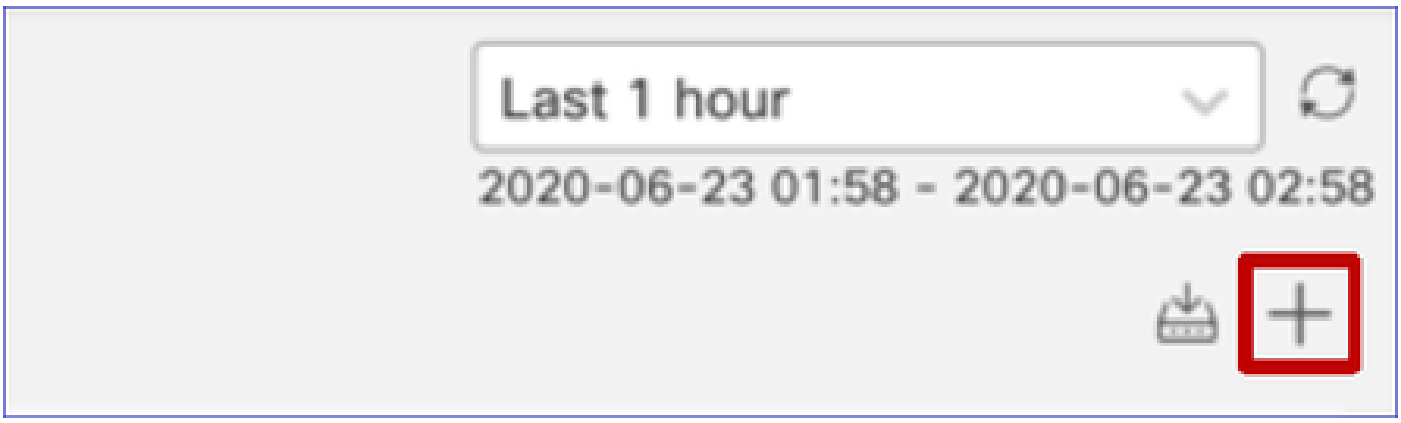


FMC UI：可以创建自定义控制面板

用户可以创建自己的自定义控制面板

- 除了预构建的控制面板之外，用户还可以创建自定义的控制面板。
- 在自定义控制面板中，可以添加任意数量的指标。

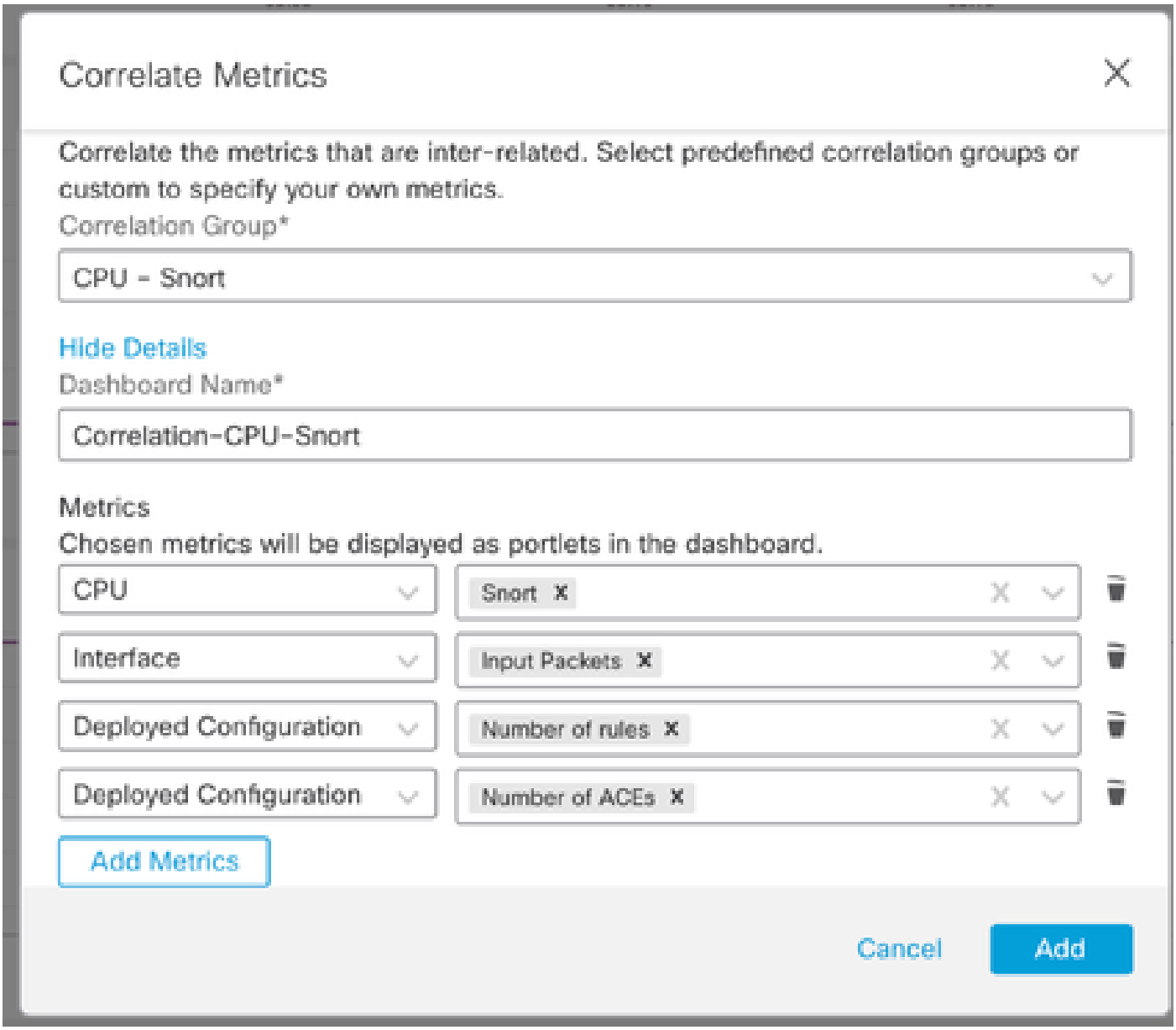
- 通常，如果来自不同度量组的度量可以关联起来以找到问题的根本原因，则会创建自定义控制面板。
- 如果Lina CPU使用率较高，可以看到每秒传入连接(CPS)、接口统计信息（等等），这会导致CPU使用率较高。



FMC UI：创建自定义控制面板

关联指标对话框

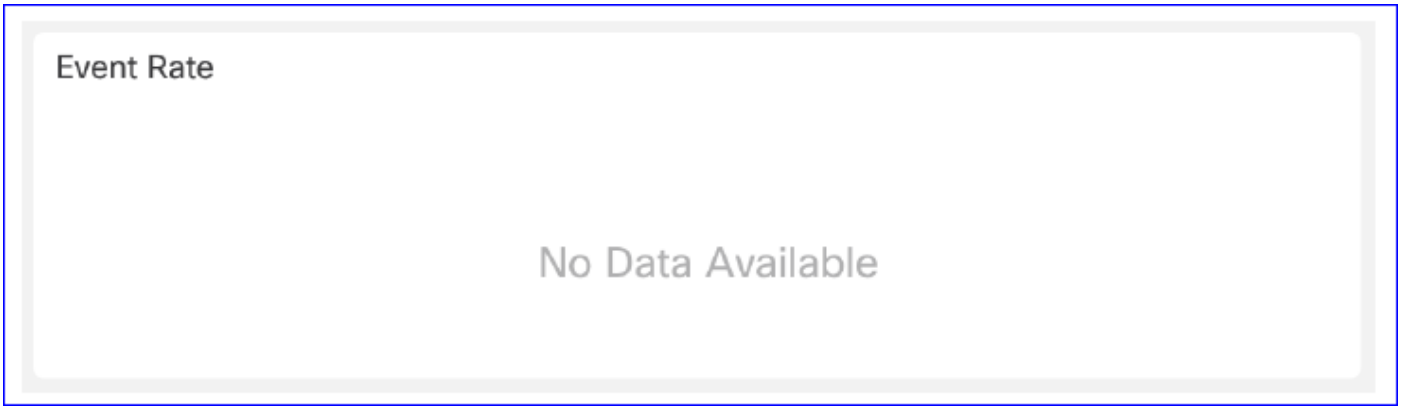
- 当用户点击“+”创建自定义控制面板时，将打开“关联度量”窗口。
- 用户可以添加用户想要一起监控的不同度量。



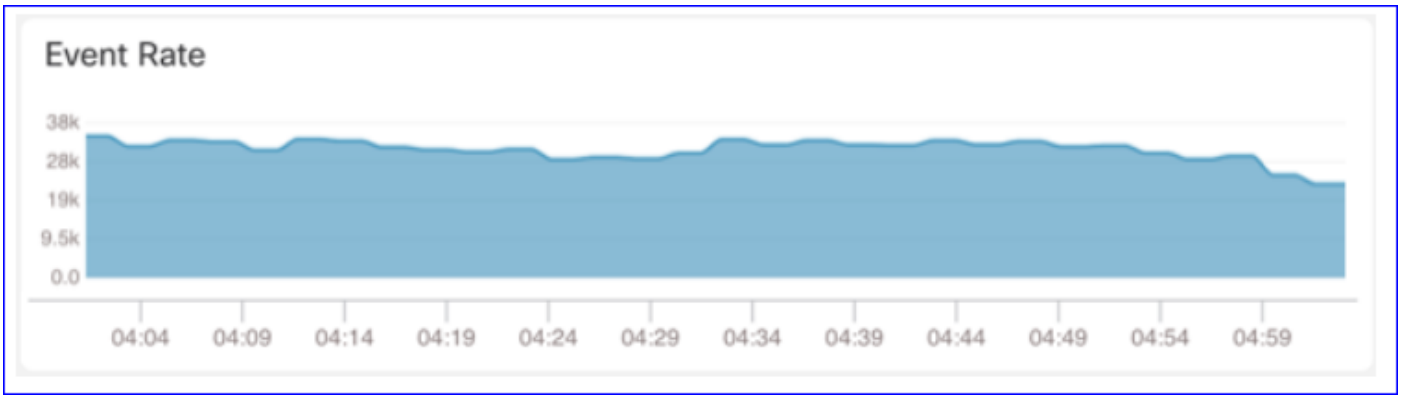
从（设备）收集数据 — GUI

GUI中显示的时间范围数据

如果运行状况监控器没有选定时间范围内的数据，则GUI在控制面板中显示“无可用数据”(No Data Available):



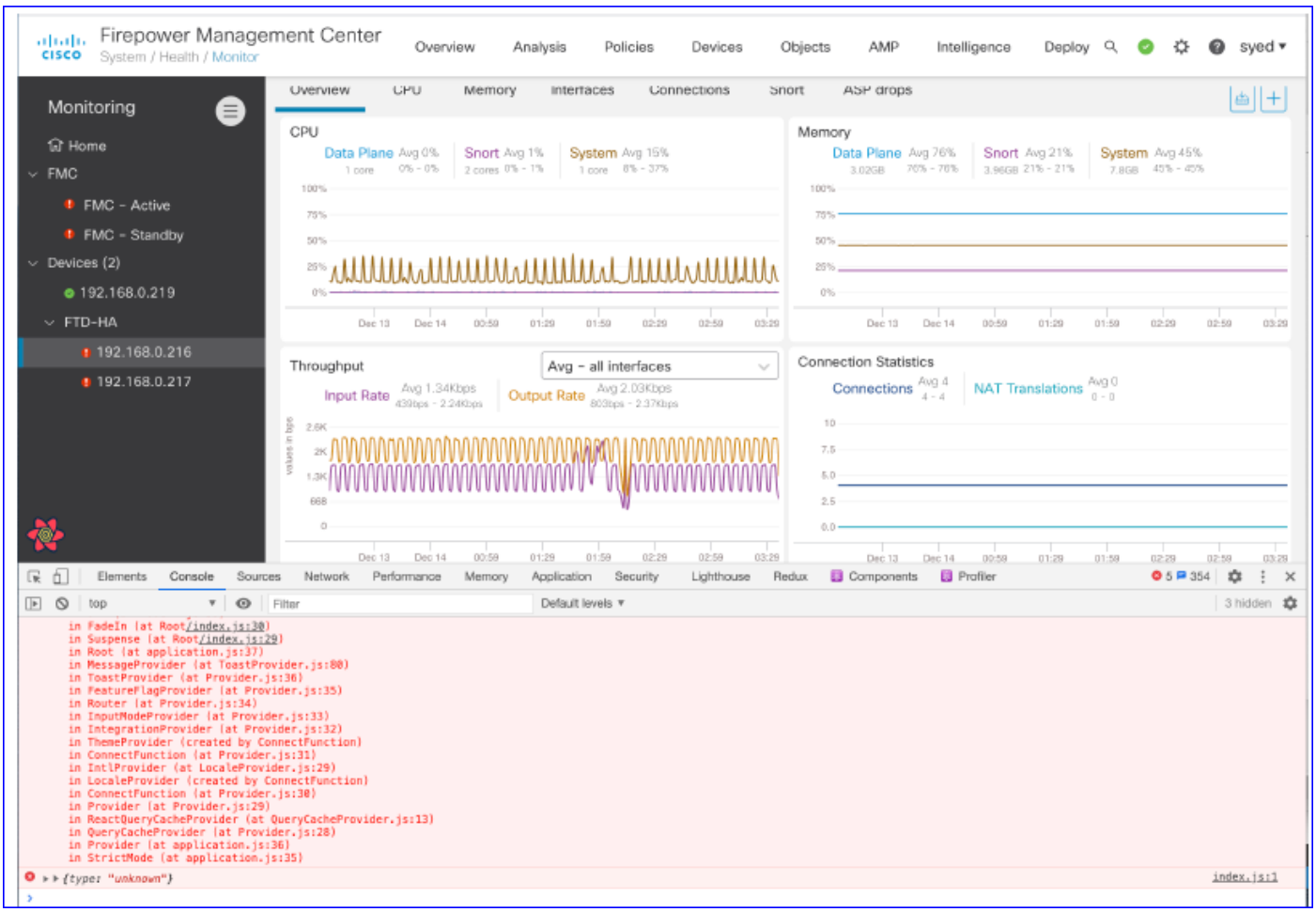
如果数据可用，图形显示如下：



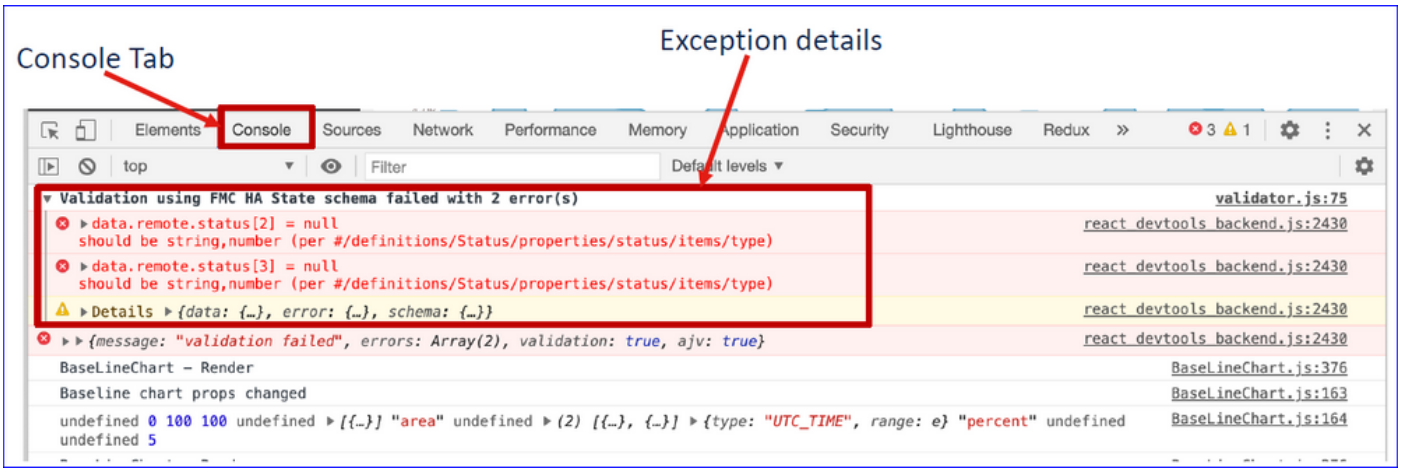
使用浏览器的控制台和网络选项卡

浏览器控制台日志和网络呼叫日志

- 在本示例中，显示Chrome浏览器开发者控制台
- 如果发生错误，异常详细信息将显示在控制台日志中



浏览器控制台日志示例



参考

[FMC运行状况监控 — 6.7]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。