升級FP — 裝置運行狀況監控

目錄

簡介

本文檔介紹6.7和7.0版本中新增的新裝置運行狀況監控功能。

背景資訊

問題：

運行狀況監控系統提供裝置效能的可視性，以便進行被動調試和主動操作。

綜合可視性和分析通過以下方式獲得：

- 關鍵度量的趨勢圖
- 事件覆蓋
- 可自定義的控制面板
- 統一運行狀況監控架構 — 為所有管理人員檢視相同的資料
- 大量新指標以及指標的可擴充性，從而增加更多

7.0版本中的新增功能

與FP 7.0相比有何新異之處

- 支援HA的FMC控制面板
- 110多項新指標用於FTD
- FTD分割大腦情形的運行狀況警報
- 較新的運行狀況度量的自定義運行時間間隔

優勢

- 通過提供將來自不同子系統的資料和裝置上的資源關聯的能力，幫助進行系統調試
- 各種系統效能指標的可視性
- 容量規劃

6.7中的新功能

與上一版本（高級版本）相比的新版本或不同版本：

- 用於在FMC上監視裝置運行狀況的新使用者介面
- FTD裝置REST API：裝置度量API：增加了許多新度量
- FMC API：新API：運行狀況警報、運行狀況指標和部署詳細資訊
- 高級市場概述，真實世界應用
- 通過提供將來自不同子系統的資料和裝置上的資源關聯的能力，幫助進行系統調試
- 可視性
- 容量規劃

功能概述

工作方式

- FP 7.0中的裝置運行狀況監控
- FMC的新運行狀況儀表板，提供趨勢圖、重疊和自定義儀表板
- FTD控制面板中可用的新FTD指標
- 涵蓋12個類別的110多項指標
- FTD API：使度量可供外部實體查詢

在引擎蓋下面，

- 使用Telegraf（開源度量收集框架）收集裝置的運行狀況

附加說明

運行狀況監控資料可用

- 在FMC運行狀況控制面板中，可從系統選單(System > Health > Monitor)訪問
- 從FMC REST API
- 當裝置由FDM管理時，通過FTD裝置REST API

某些指標（FMC和FTD）預設會停用

- 需要啟用並部署運行狀況策略中的運行狀況模組，才能顯示某些度量。

實施FP 6.7 IFT使用者要求的增強功能

- 預設情況下自動刷新
- 儀表板上具有自定義時間範圍的篩選器
- 在介面選擇器中按使用者定義的名稱（以及物理介面名稱）選擇介面
- 從運行狀況監視器「首頁」頁面交叉啟動裝置儀表板

FP 6.7中的裝置運行狀況監控

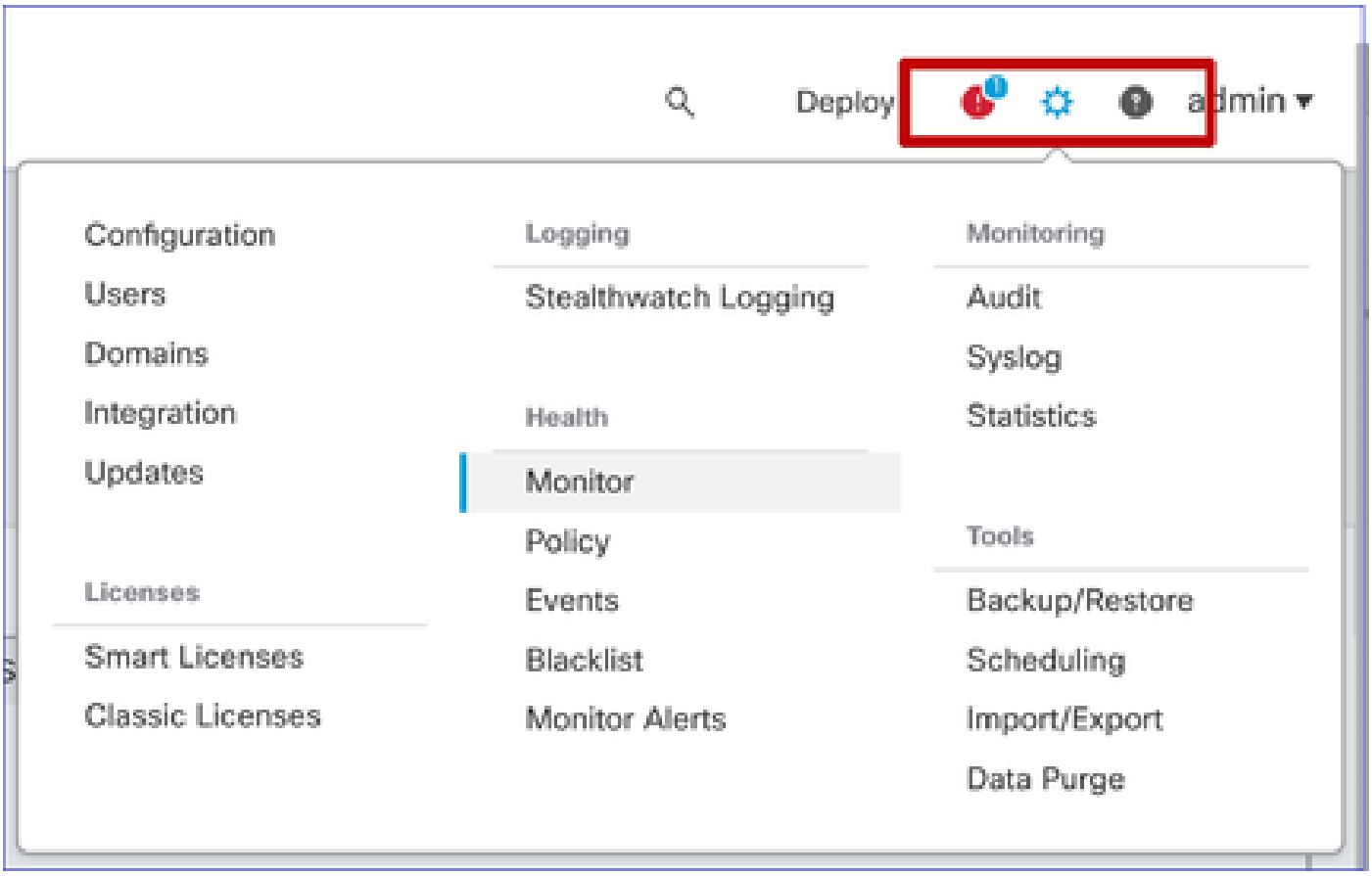
- FMC上的新UI，提供趨勢圖、重疊和自定義儀表板。
- FTD API：使外部實體查詢的度量相同

限制摘要：

- FDM GUI或CDO不支援此功能
- 不支援在新的運行狀況監視UI中監視FMC本身。
- 輪詢間隔不可配置。不能為不同的裝置配置不同的輪詢間隔。所有輪詢都以固定的一分鐘間隔進行。

部署示例

- 無需特定部署即可測試該功能。只需將FMC和裝置升級到FP 6.7。
- FMC運行狀況控制面板中提供了運行狀況監控資料，您可以從系統頁籤訪問這些資料。



必要條件和支援的平台

最低支援的軟體和硬體平台

支援的最低管理器版本	受管裝置	需要支援的最低受管裝置版本	備註
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	僅受FTD支援
FTD裝置REST API	FTD 6.7	FXOS 2.9.1 FTD 6.7	僅限FTD裝置REST API （不是FDM或CDO

			GUI ）

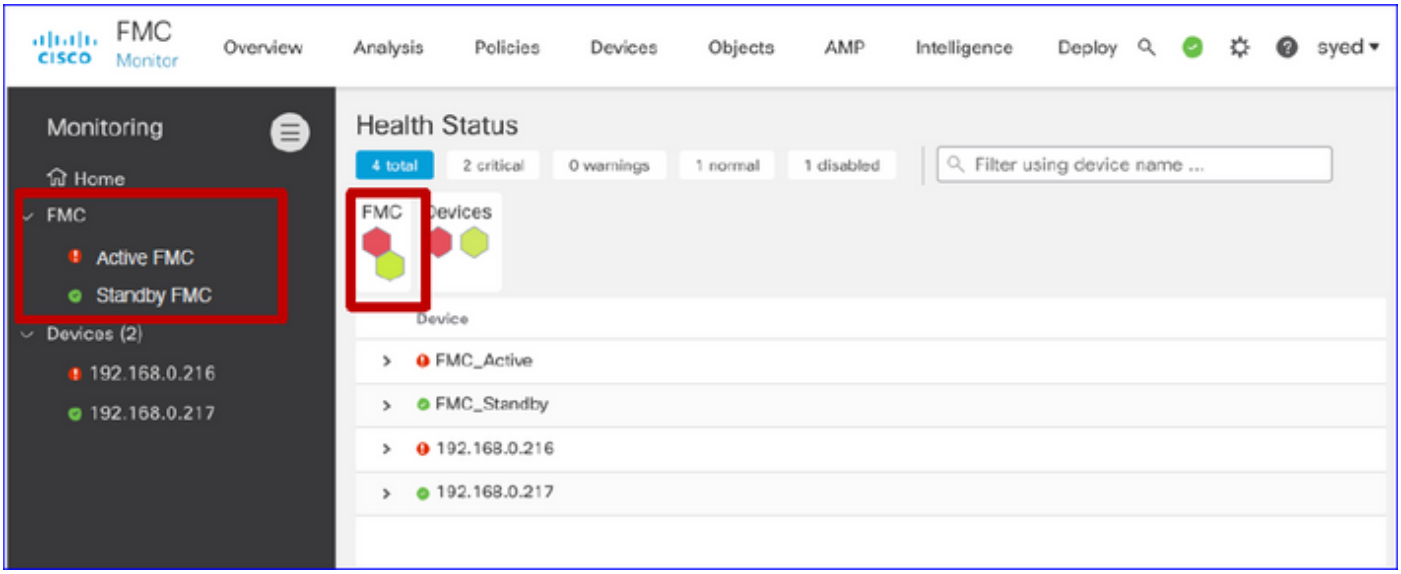
互通性

對互操作性沒有特定要求。

功能詳細資訊7.0

FMC UI：獨立和HA支援

運行狀況監控頁面導航



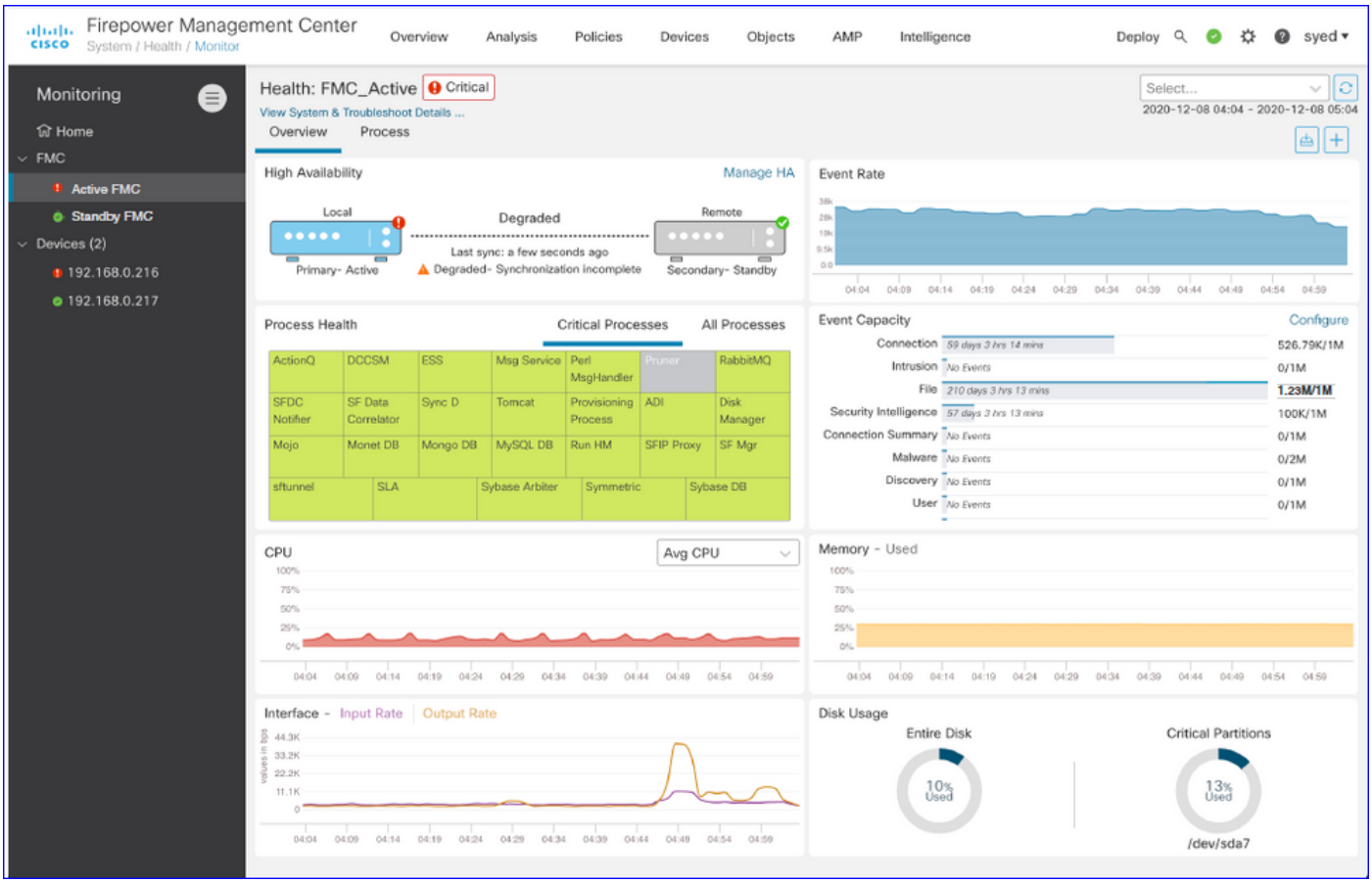
- 獨立FMC顯示為單個節點
- FMC HA顯示為一對節點
- 顯示每個FMC的健康狀況

運行狀況

- FMC HA以雙六邊形顯示。
- FMC主用和備用裝置也列在警報表中。

FMC控制面板

7.0中的FMC運行狀況監控儀表板



以下內容的摘要檢視：

- 高可用性
- 事件速率和容量
- 進程運行狀況
- CPU
- 記憶體
- 介面
- 磁碟

此儀表板可用於主用和備用FMC。使用者可以建立自定義儀表板來監控他們選擇的指標。

FMC控制面板：FMC HA面板

高可用性面板顯示

- 當前HA狀態
- 主用與備用
- 上次同步時間
- 裝置運行狀況

FMC控制面板：事件速率和容量

事件速率

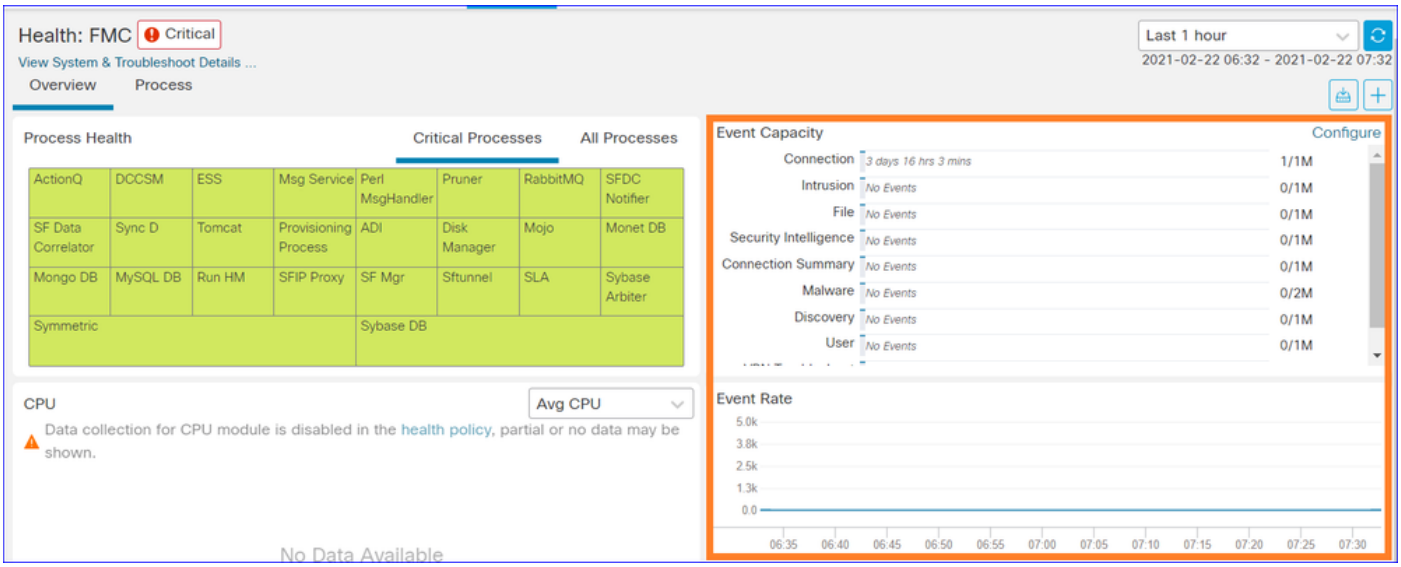
- 作為基線的最大事件速率
- FMC接收的總事件速率

事件容量

- 按事件類別劃分的當前消耗量
- 事件的保留時間
- 當前與最大值

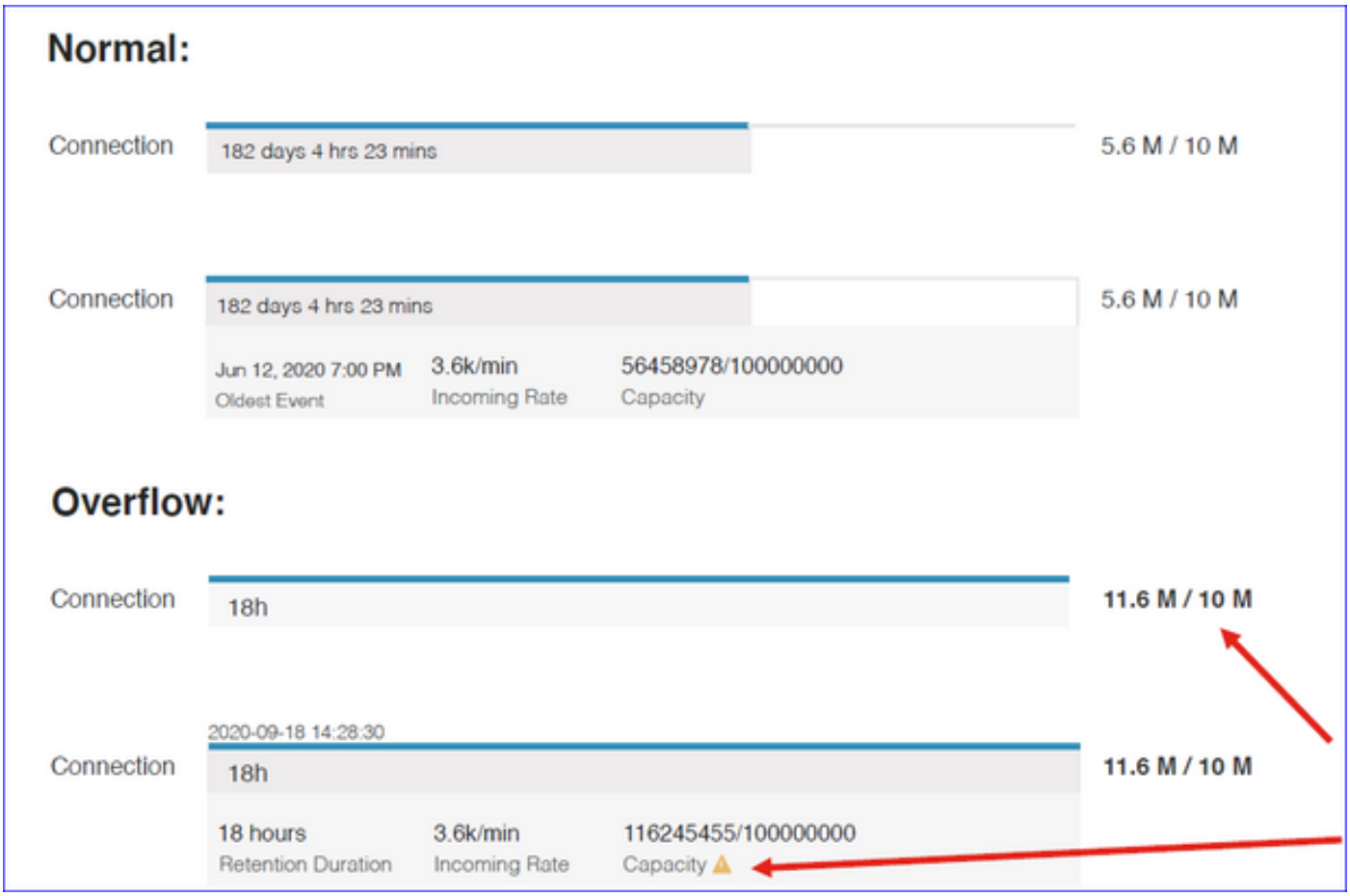
事件容量

- 容量溢位標籤



FMC控制面板：事件容量

正常事件容量消耗狀態



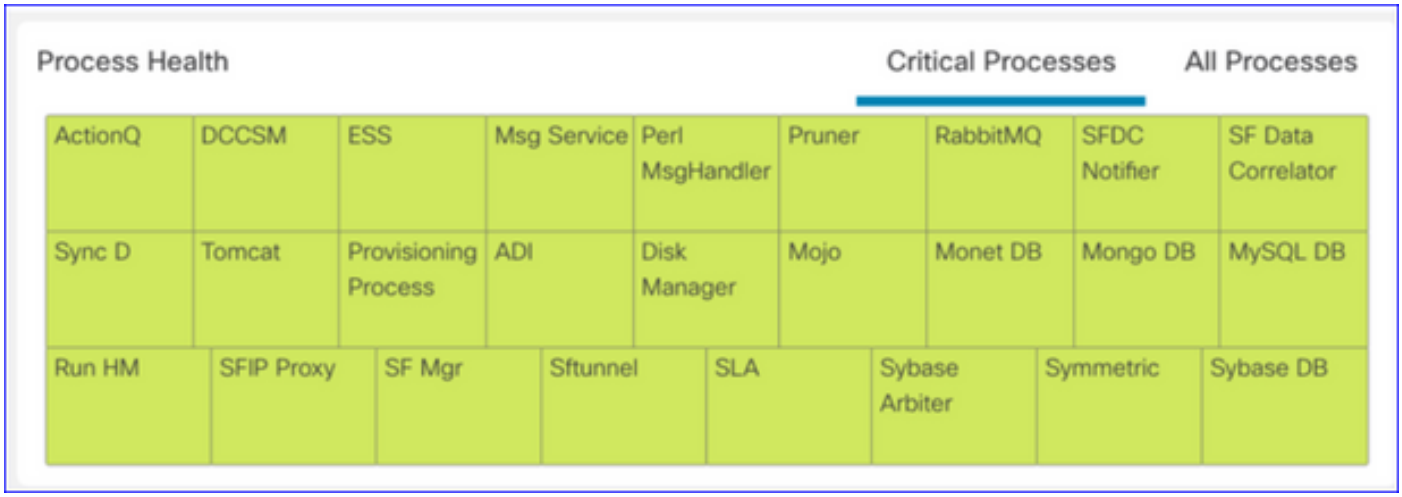
溢位情況：事件儲存超出配置的最大容量。

- 粗體文本表示溢位
- 警告圖示突出顯示容量溢位

FMC控制面板：FMC流程面板

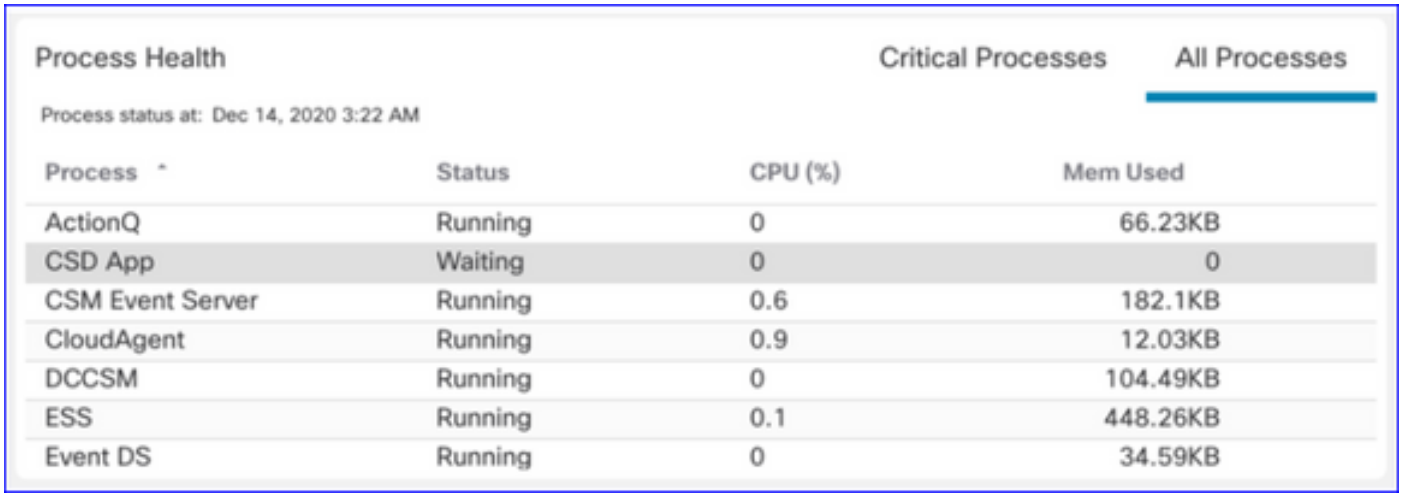
關鍵進程面板顯示

- 處理當前狀態
- 進程重新啟動計數



「進程」面板顯示所有「pmconfig」進程的以下度量：

- 當前狀態
- CPU使用率
- 記憶體使用率



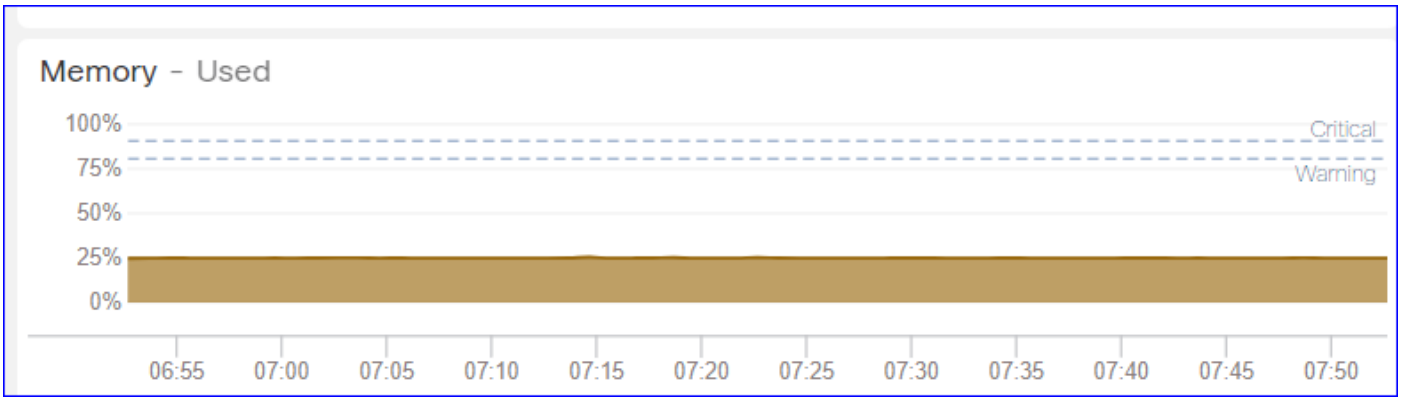
FMC控制面板：FMC CPU

CPU面板顯示

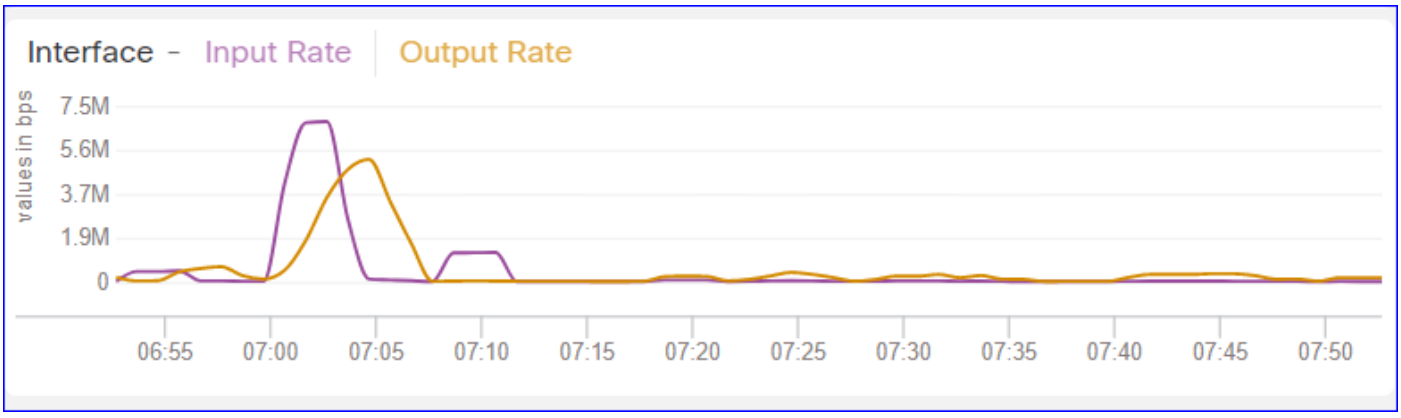
- 平均CPU（預設）
- 所有核心

FMC控制面板：其他面板

記憶體面板顯示FMC上的整體記憶體使用情況



介面面板顯示所有介面的平均輸入/輸出速率

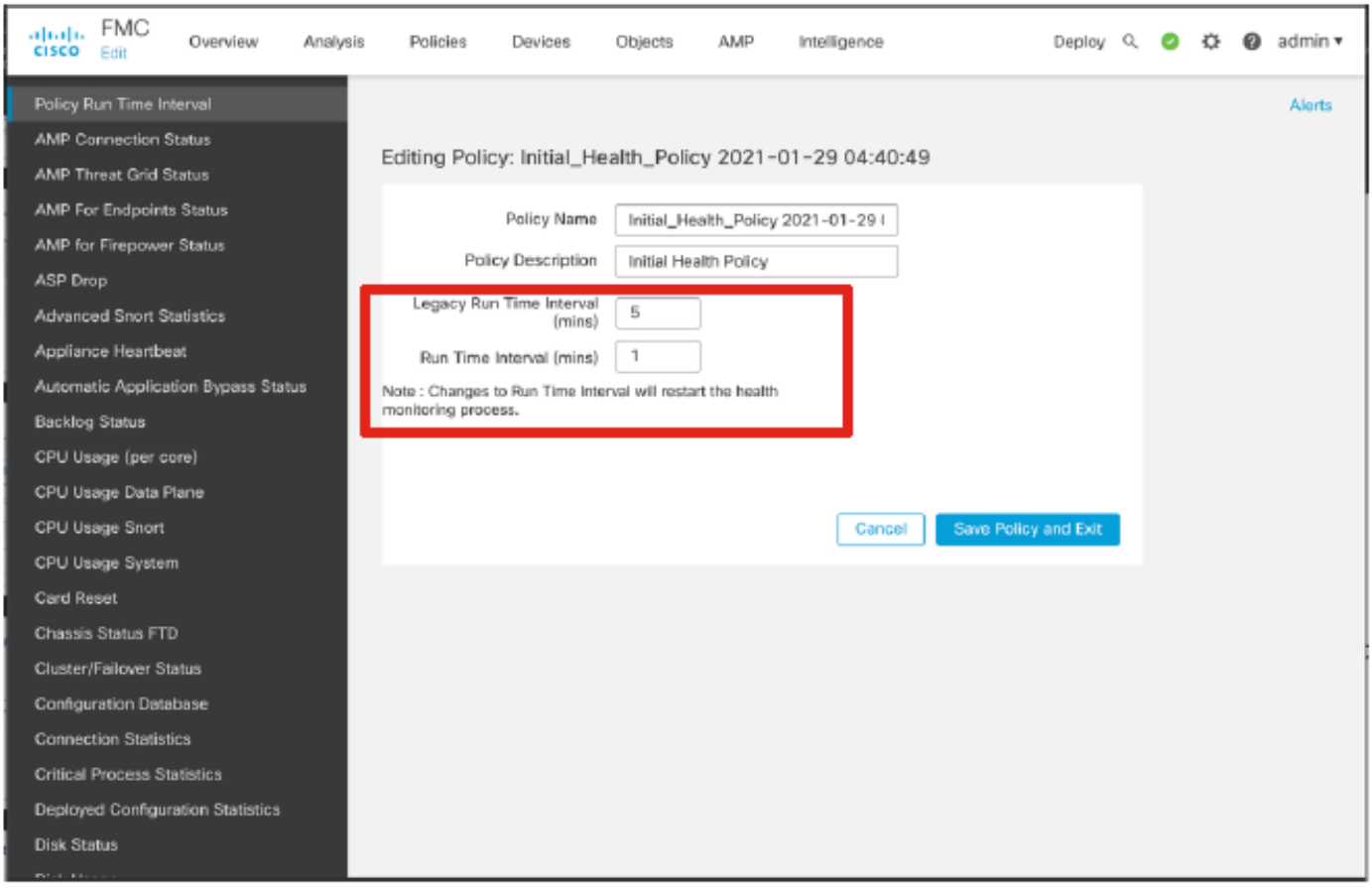


磁碟面板顯示

- 整個磁碟容量
- 儲存FMC資料的關鍵分割槽容量

運行時間間隔

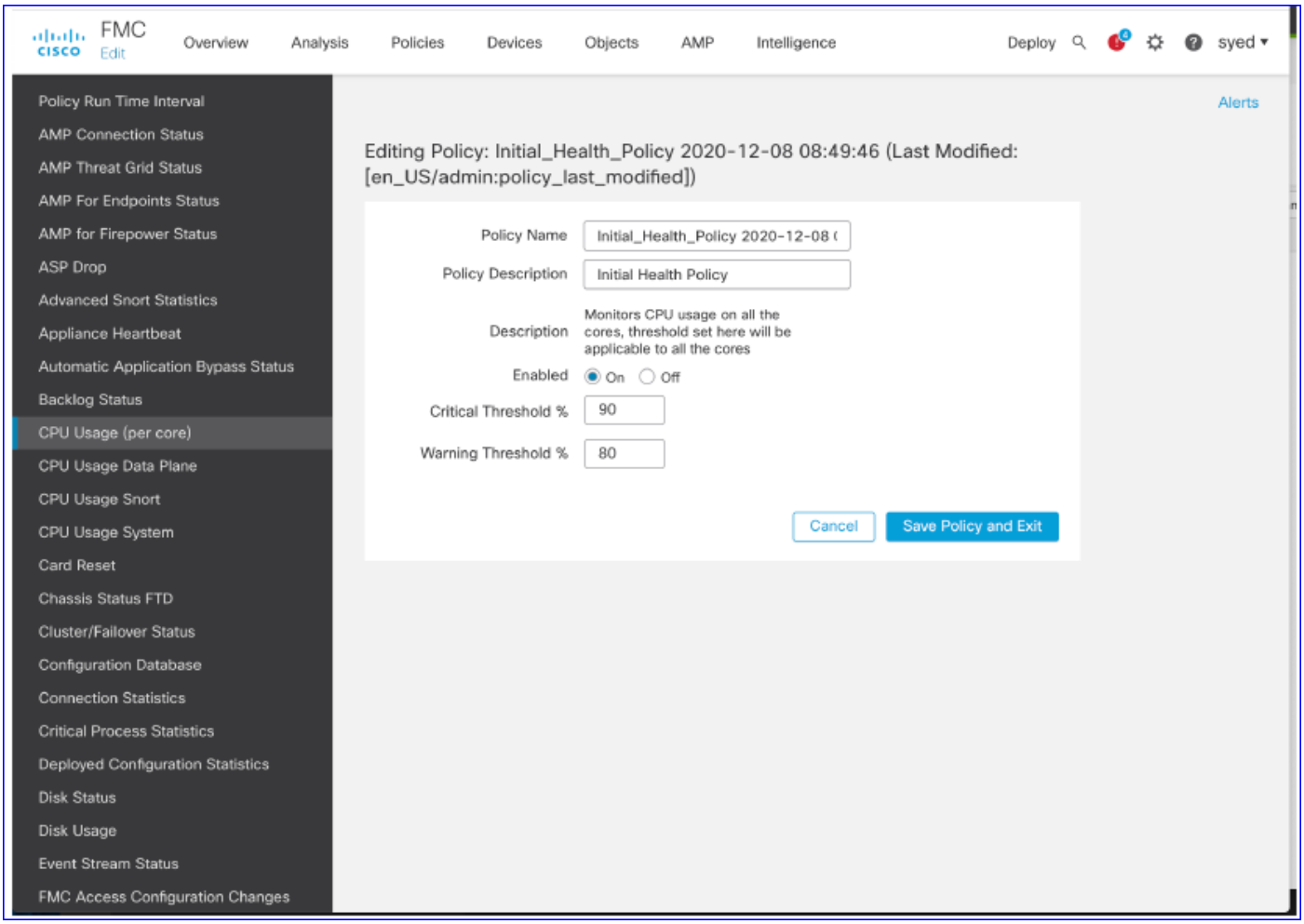
- 舊運行狀況模組的運行時間間隔重新命名為「舊運行時間間隔」(Legacy Run Time Interval)
- 「運行時間間隔」以新的基於Telegraf的運行狀況模組為目標
- 全域性設定，影響所有裝置



可用指標

可用於自定義控制面板的度量

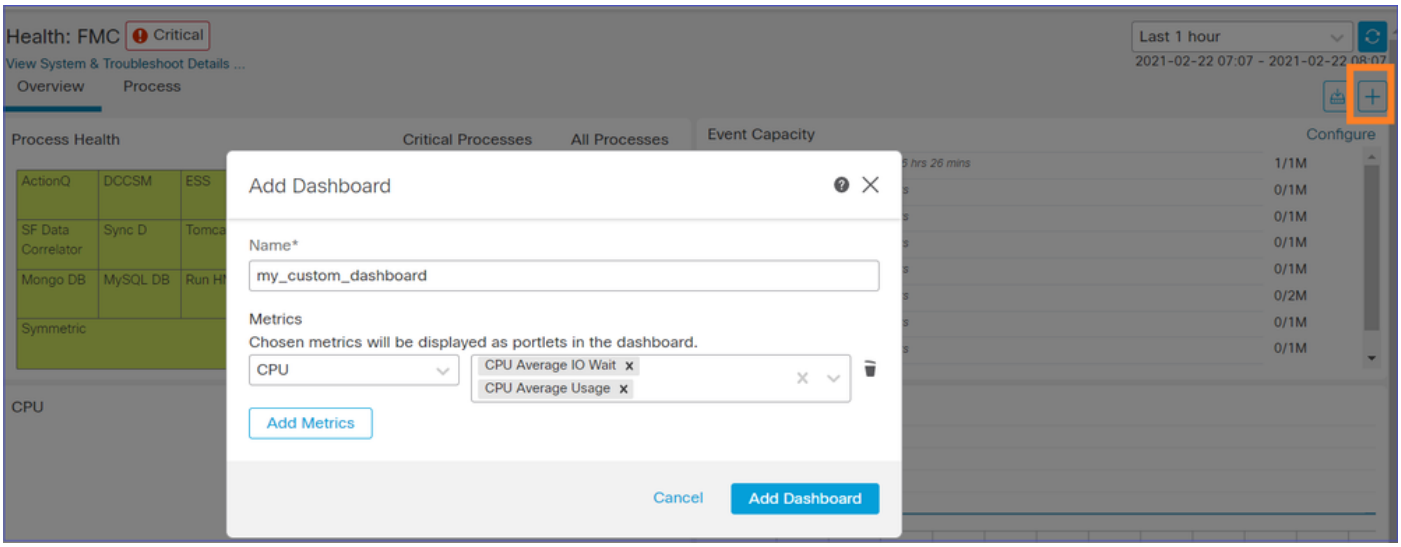
- 如果使用者想要製作自定義控制面板，則這些幻燈片是可用指標的指南。
- 某些度量必須在運行狀況策略中啟用，才能在自定義運行狀況控制面板中使用



FMC使用者介面：FMC自定義控制面板

7.0中的新FMC監控指標類別

- CPU
- 記憶體
- 介面
- 磁碟
- 活動
- 程序
- RabbitMQ
- Sybase
- MySQL



FMC UI:FMC指標

跨不同類別新增了40個指標（在自定義控制面板中提供）。若要啟用已禁用的度量，請在關聯的運行狀況策略(System > Health > Policy)中啟用相應的運行狀況模組。

度量組名稱	預設啟用	說明
CPU	否	監視FMC CPU
記憶體	是	監視FMC記憶體
磁碟	是	監視FMC磁碟使用情況
介面	是	監控FMC介面
程序	是	監視FMC進程
活動	是	監視事件速率
MySQL	否	監視MySQL
RabbitMQ	否	監視RabbitMQ
Sybase	否	監視Sybase

FTD:FP 7.0中引入的指標

預設啟用：預設情況下收集度量。要啟用已禁用的度量，請在關聯的運行狀況策略(System > Health > Policy)中啟用相應的運行狀況模組。

度量組名稱	預設啟用	說明	平台
機箱狀態	是	監控不同的機箱引數，如風扇速度和溫度。	僅適用於FPR2100和FPR1000平台
流量卸載	是	監控硬體流解除安裝統計資訊	適用於FPR9300 和FPR4100平台
ASP刪除	是	監控Lina端封包捨棄	All
命中計數	否	監視訪問控制策略規則的命中計數	All
AMP Threat Grid狀態	是	監控與AMP的連線 ThreatGrid	All
AMP連線狀態	否	從FTD監控AMP雲連線	All
SSE聯結器狀態	否	從FTD監控SSE雲連線	All
NTP狀態	否	監視NTP時鐘同步引數 ftd	All
VPN統計資訊	是	監視S2S和RA VPN隧道統計資訊	All
路由統計資訊	是	監控Lina端封包捨棄	All
Snort 3效能統計資訊	是	監控某些Snort3效能統計資訊(perfstats)	All

xTLS計數器	否	監控xTLS/SSL流、記憶體和快取的有效性	All

REST API、系統日誌、SNMP

7.0中未引入新的FMC或FTD裝置REST API。現有的REST API支援7.0中新增的新指標。

系統日誌和SNMP

系統日誌

- 運行狀況監視器的系統日誌無更改

SNMP

- 用於「SNMP裝置運行狀況監控」的單獨的TOI

SAL/CTR/第三方產品整合

- 單獨的TOI支援「Azure Application Insights」
- 沒有進行具體的更改來支援將「運行狀況監控」與SAL/CTR/SecureX整合
- REST API可用於第三方整合

軟體技術

功能詳細資訊6.7

針對FTD運行狀況和效能的新NGFW運行狀況監控

幫助使用者

- 被動調試，如發生問題後的根本原因分析
- 主動操作（如監控使用情況和飽和級別）以確定潛在的容量問題，從而幫助使用者執行容量增強或重構。

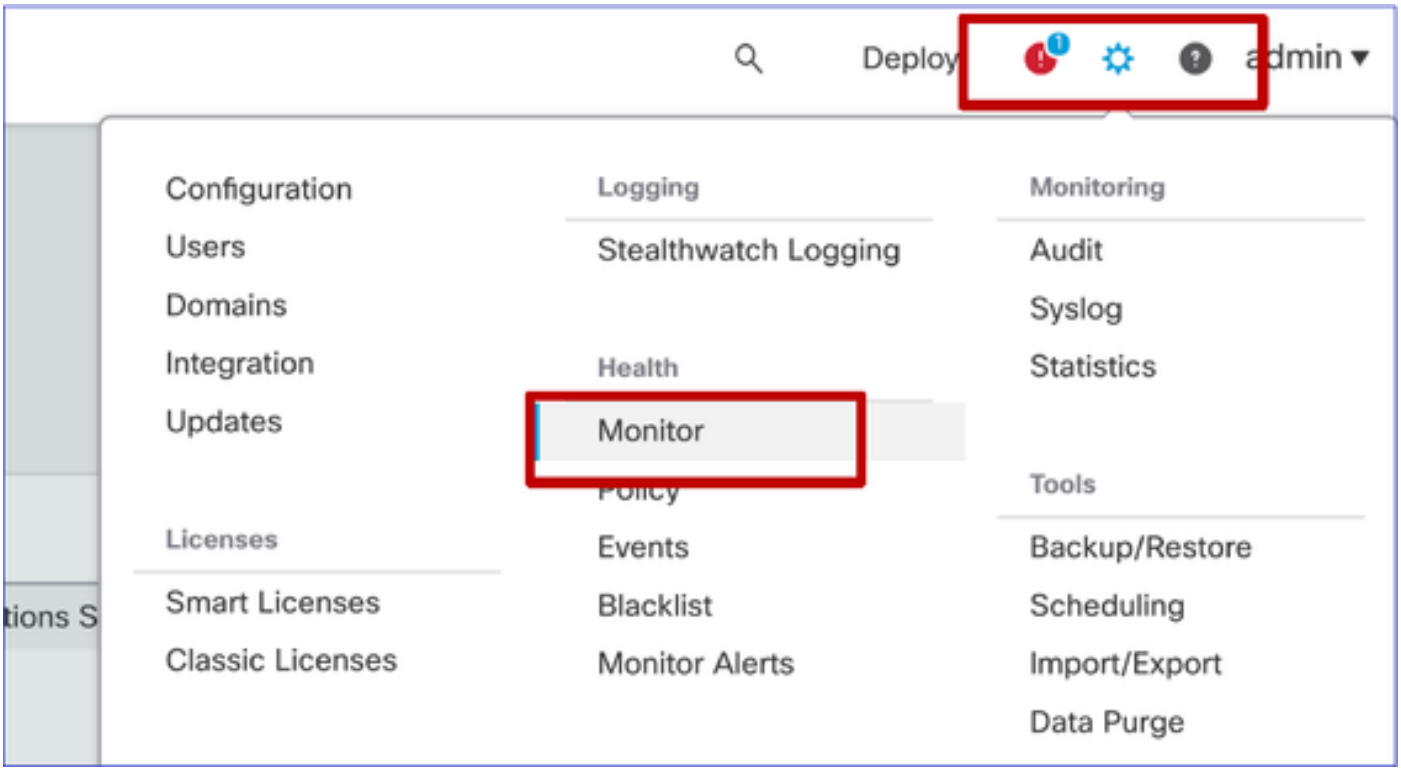
亮點

- 趨勢圖：趨勢圖可以非常輕鬆地檢測異常並確定問題的根本原因。利用視覺檢測技術可以發現檢測趨勢，並繪製不同度量之間的相關關係，從而發現它們之間的因果關係。
- 事件重疊：事件重疊顯示重要資訊，例如趨勢圖上的配置部署和SRU更新以指示因果關係。
- 可自定義的儀表板：使用者可以建立自己的儀表板，將希望在一頁上一起檢視的指標分組。
- 統一運行狀況監控架構：無論哪個經理對指標「感興趣」，都為指標提供單點收集和匯出。FTD API以及FMC使用來自同一度量收集器的資料。
- 指標的可擴展性：該平台架構的目標之一是能夠輕鬆新增新的指標。這是通過使用開源指標收集和儲存工具以及可自定義的控制面板來實現的。

FMC GUI

FMC UI：導航到運行狀況

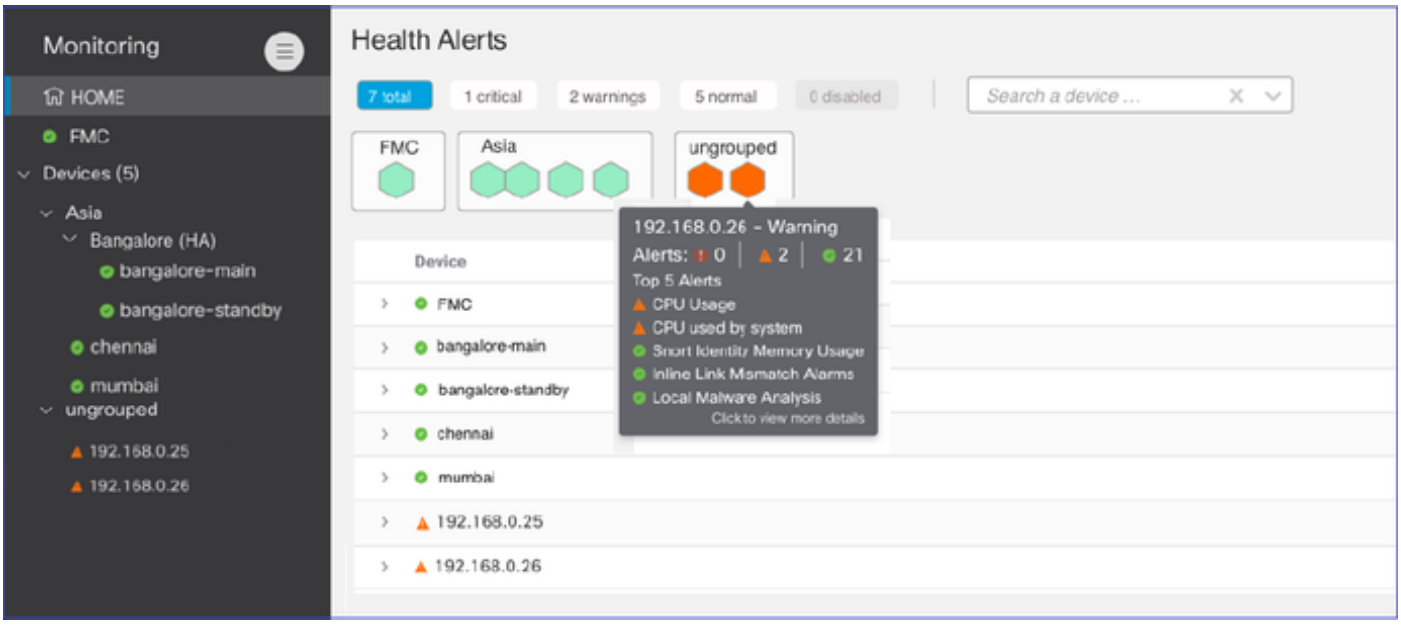
在FMC上，按一下System圖示> Health > Monitor以導航到Health Status頁面。



FMC UI：新建運行狀況狀態頁面

Health Status頁面用於顯示FMC管理的所有裝置的運行狀況概述，包括FMC的運行狀況。

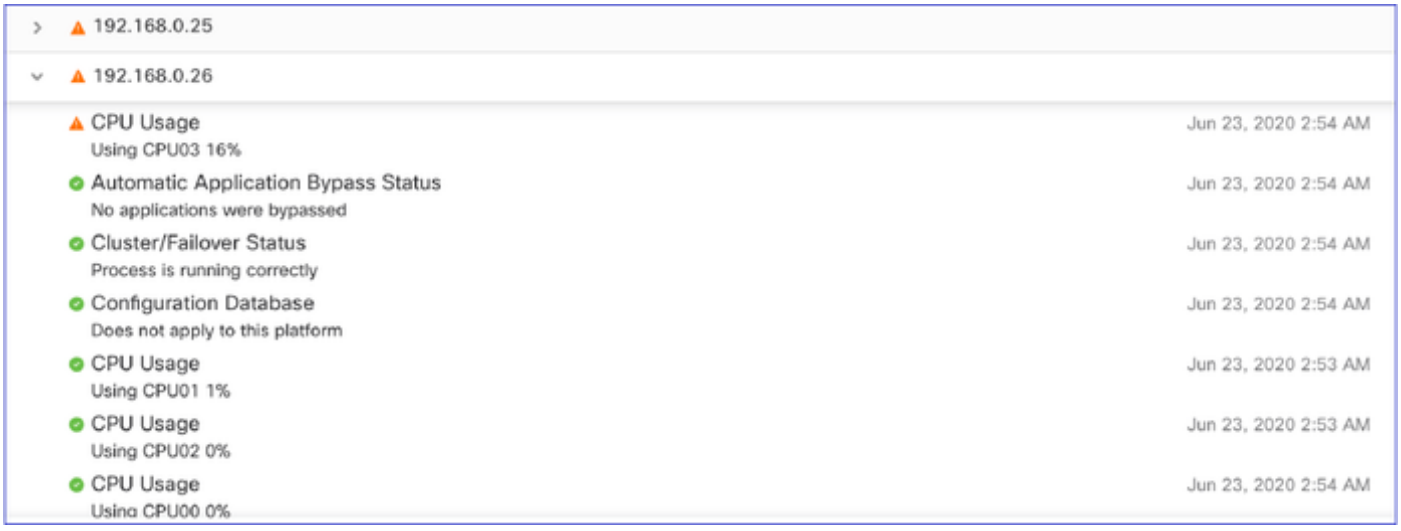
- 裝置按其組/ha/群集分組。
- 裝置左側的點表示其運行狀況
- 綠色 — 無警報
- 橙色 — 至少一個健康警告
- 紅色 — 至少有一個嚴重健康警報
- 將滑鼠懸停在表示裝置運行狀況的六邊形上時會顯示運行狀況摘要。
- 可以在運行狀況策略中配置警告和嚴重級別的閾值，其配置方式與FP 6.7之前的配置方式相同。



FMC UI：裝置運行狀況事件

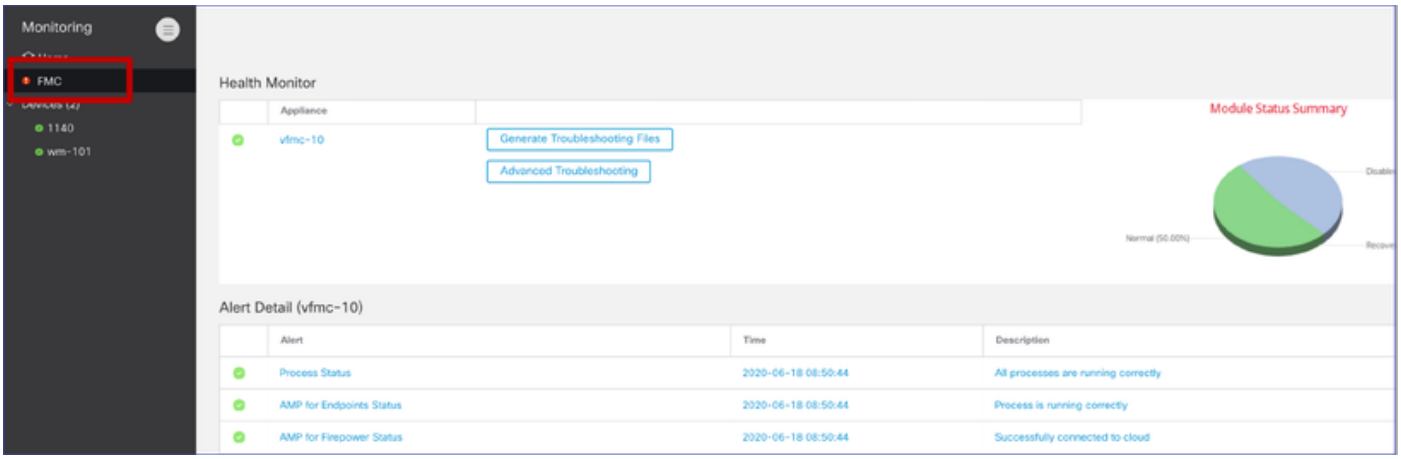
按一下底部面板中的裝置以顯示與裝置關聯的運行狀況事件。警報按其運行狀況狀態（嚴重性）排序。

運行狀況監控頁面



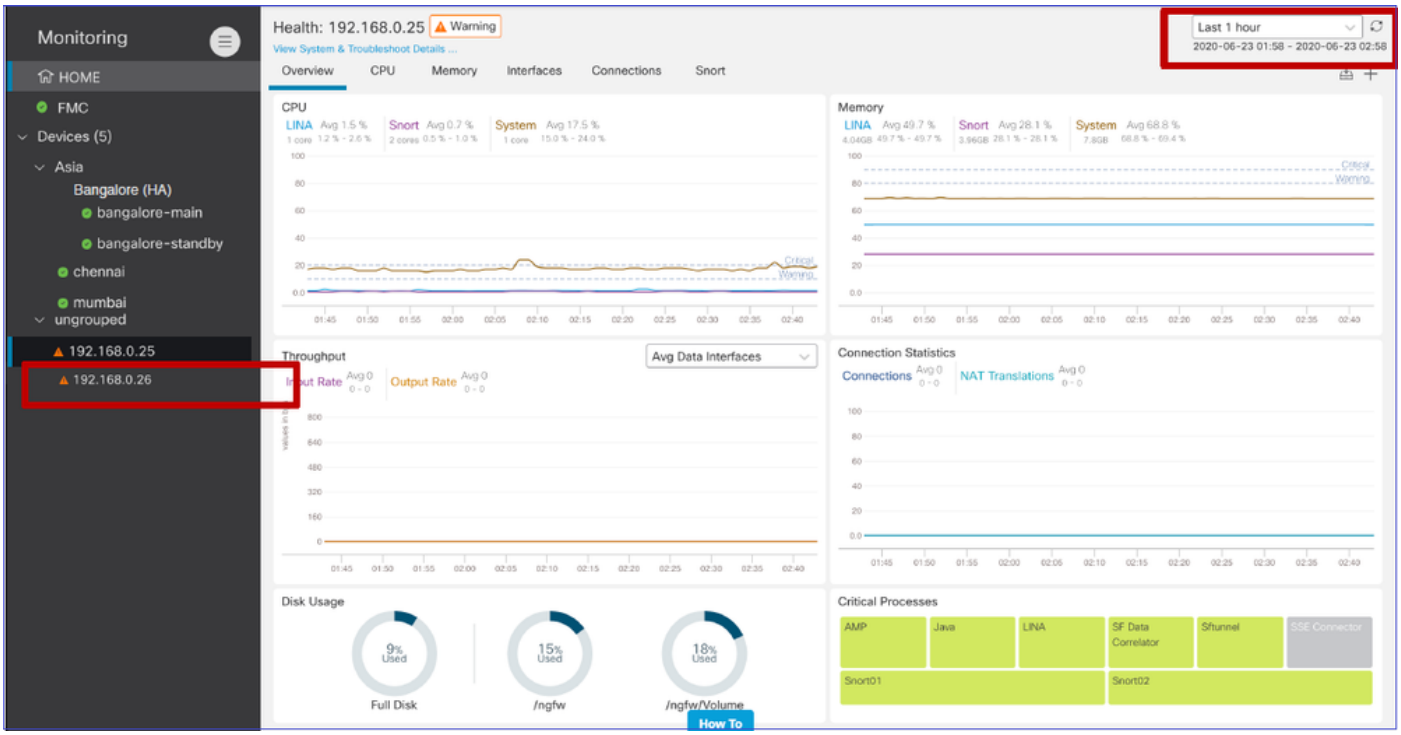
FMC UI:FMC運行狀況監控未更改

FMC運行狀況頁面仍然是舊頁面。只有使用6.7+的FTD支援新的UI



FMC UI：全新！裝置儀表板

- 按一下左窗格中的裝置名稱，進入裝置的運行狀況概述頁面。
- 運行狀況概述包含所有關鍵運行狀況指標趨勢圖。
- 可使用各種時間範圍（預設為過去1小時）
- 自動刷新以重新載入圖形



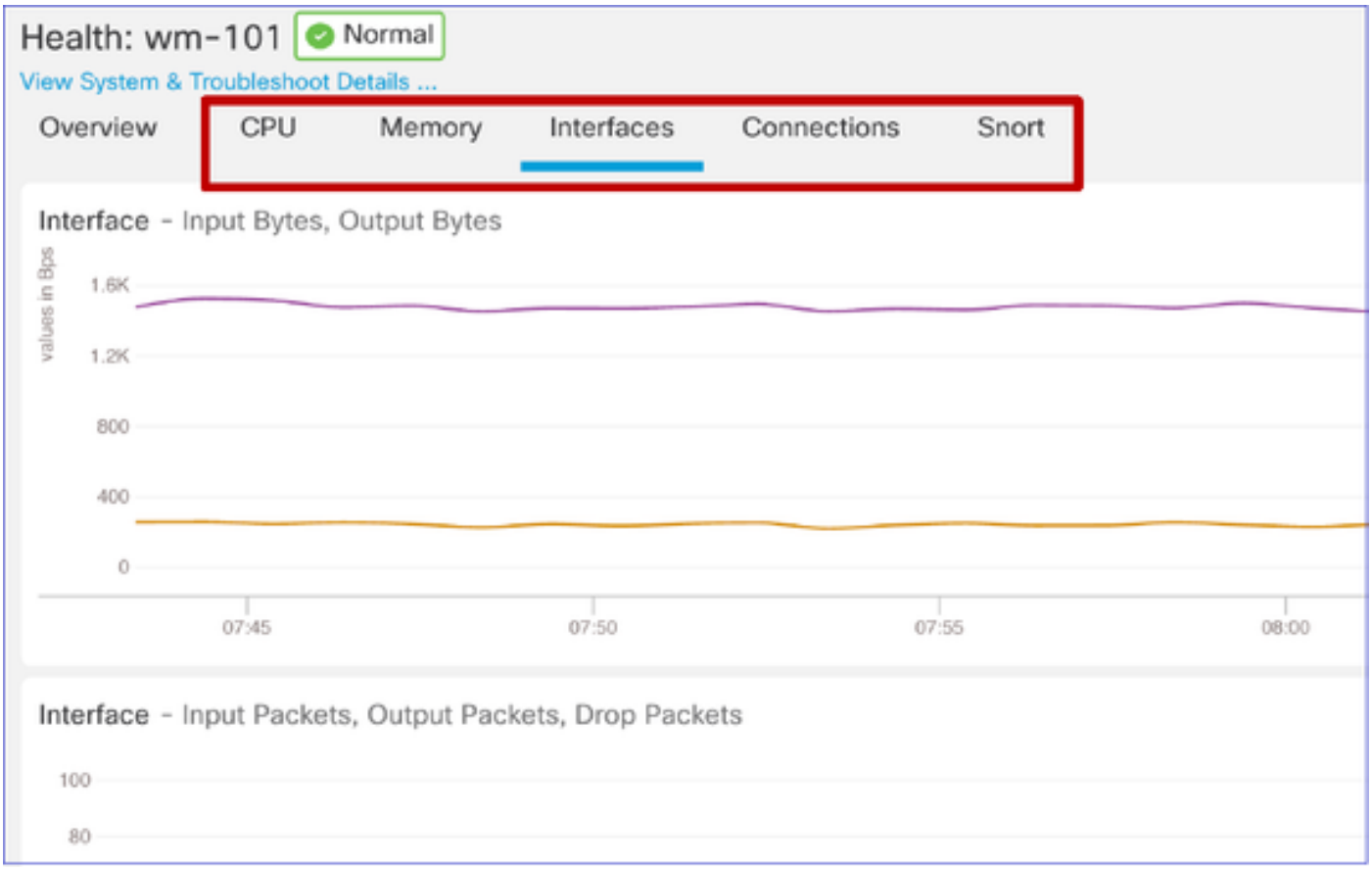
FMC UI：部署資料覆蓋

點選部署圖示以顯示圖上選定時間範圍的部署覆蓋詳細資訊

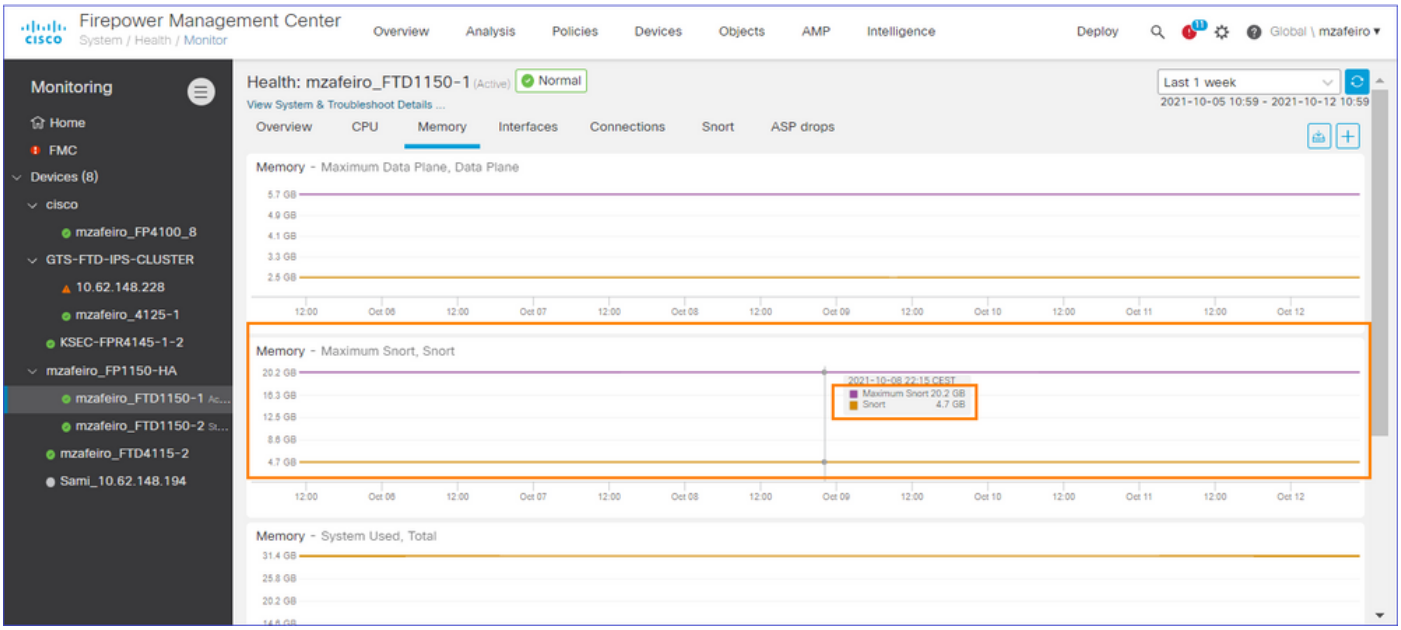
- 圖示指示所選時間範圍內的部署數量
- 顯示頻段以指示部署開始和結束時間。
- 如果部署較多，則會顯示多個頻段/線路
- 按一下虛線頂部的圖示以顯示詳細資訊

FMC UI：裝置預構建儀表板

- FMC UI中存在預構建的運行狀況儀表板。
- 這些預構建的控制面板帶有組合在一起的相關指標。
- 介面控制面板具有所有介面相關度量（如輸入/輸出位元組、資料包以及不同介面的平均資料包大小）的趨勢圖。



FTD Snort記憶體 — 它源自何處？

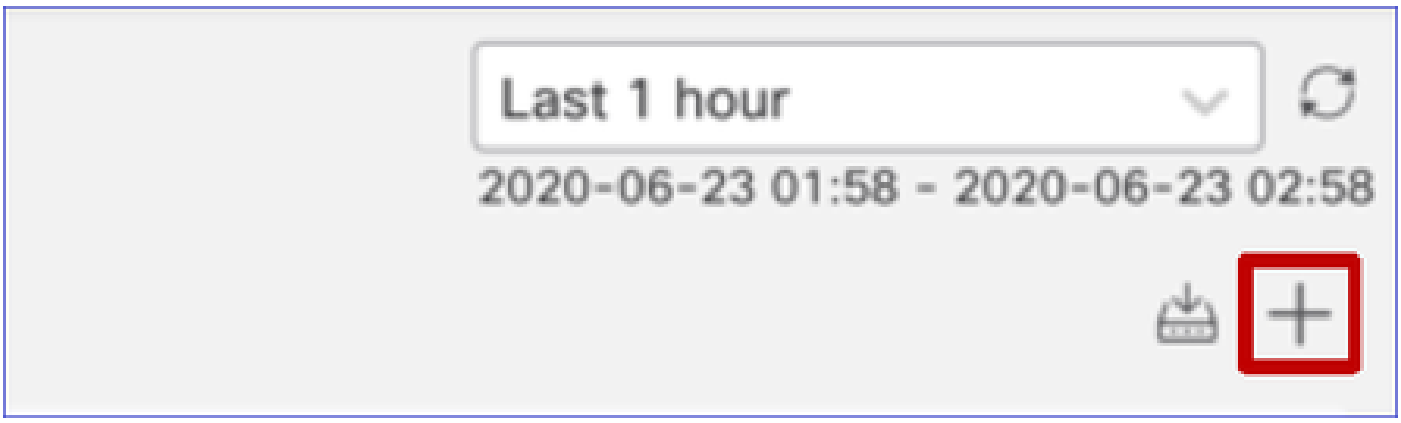


FMC UI：可以建立自定義儀表板

使用者可以建立自己的自定義儀表板

- 除了預構建的控制面板外，使用者還可以建立自定義的控制面板。
- 在自定義控制面板中，可以新增任意數量的度量。

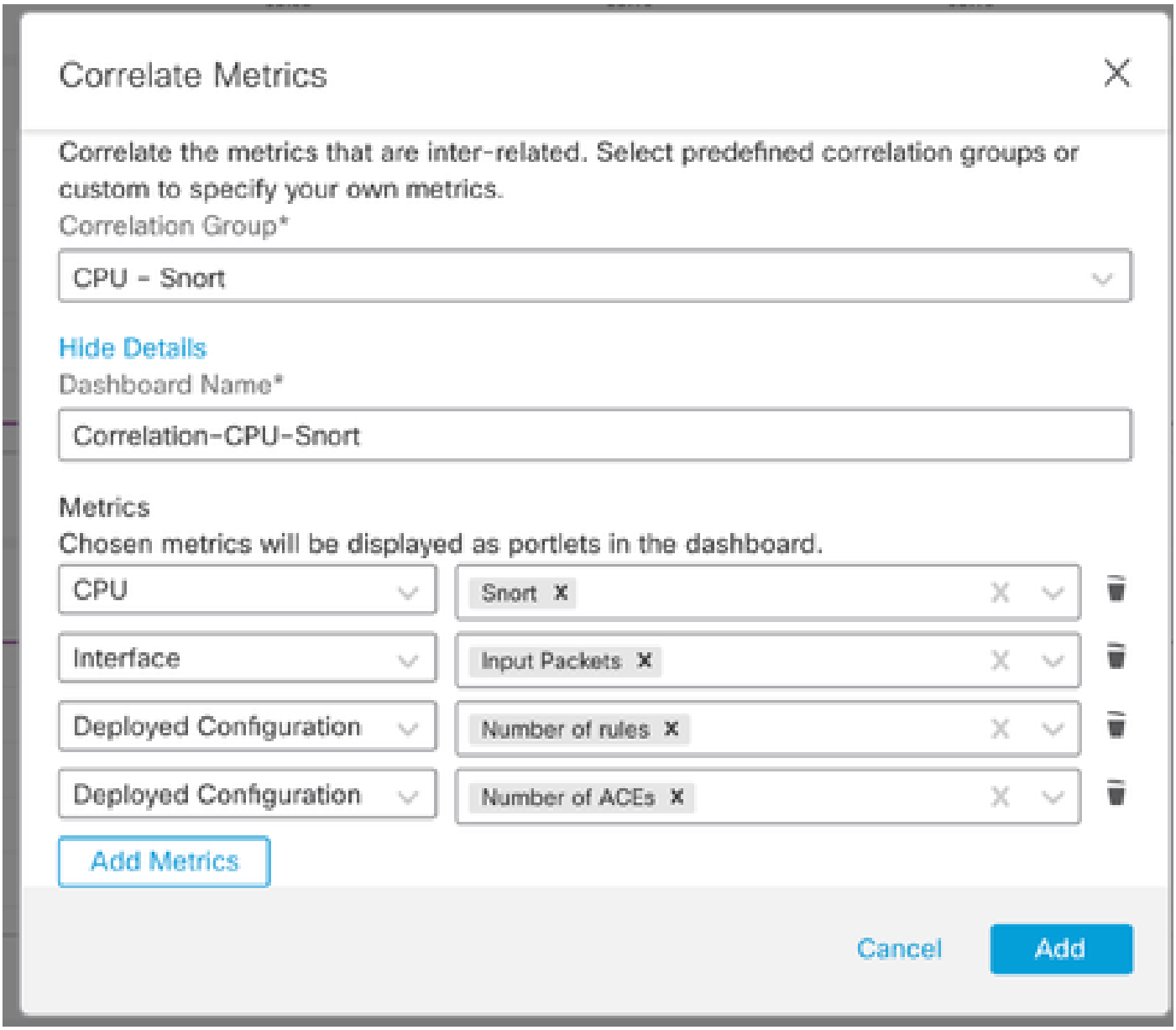
- 通常，如果來自不同度量組的度量可以相互關聯以找到問題的根本原因，則會建立一個自定義的控制面板。
- 在Lina CPU使用率較高的情況下，可以看到每秒傳入連線(CPS)、介面狀態等，這可能會導致CPU使用率過高。



FMC UI：建立自定義儀表板

「關聯度量」對話方塊

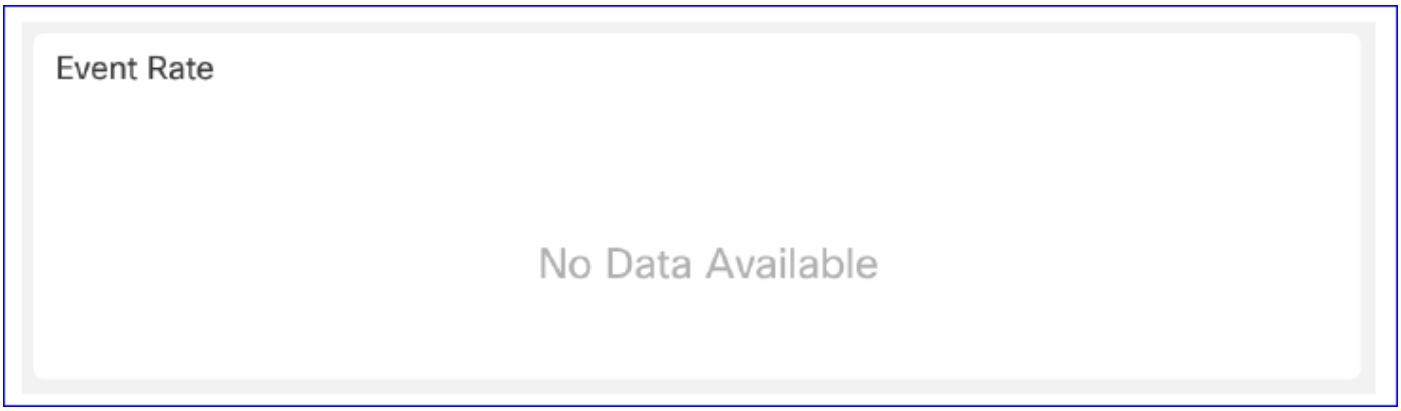
- 當使用者按一下「+」建立自定義儀表板時，將開啟「關聯度量」視窗。
- 使用者可以新增使用者想要一起監視的不同度量。



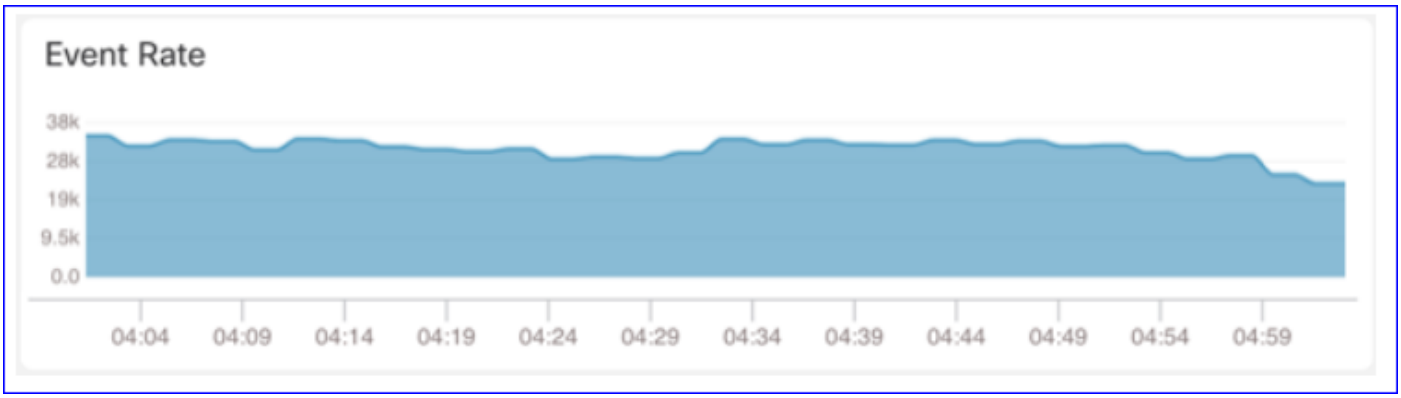
正在從（裝置）收集資料 — GUI

時間範圍的資料顯示在GUI中

如果運行狀況監視器沒有選定時間範圍內的資料，則GUI在儀表板面板中顯示「無可用資料」：



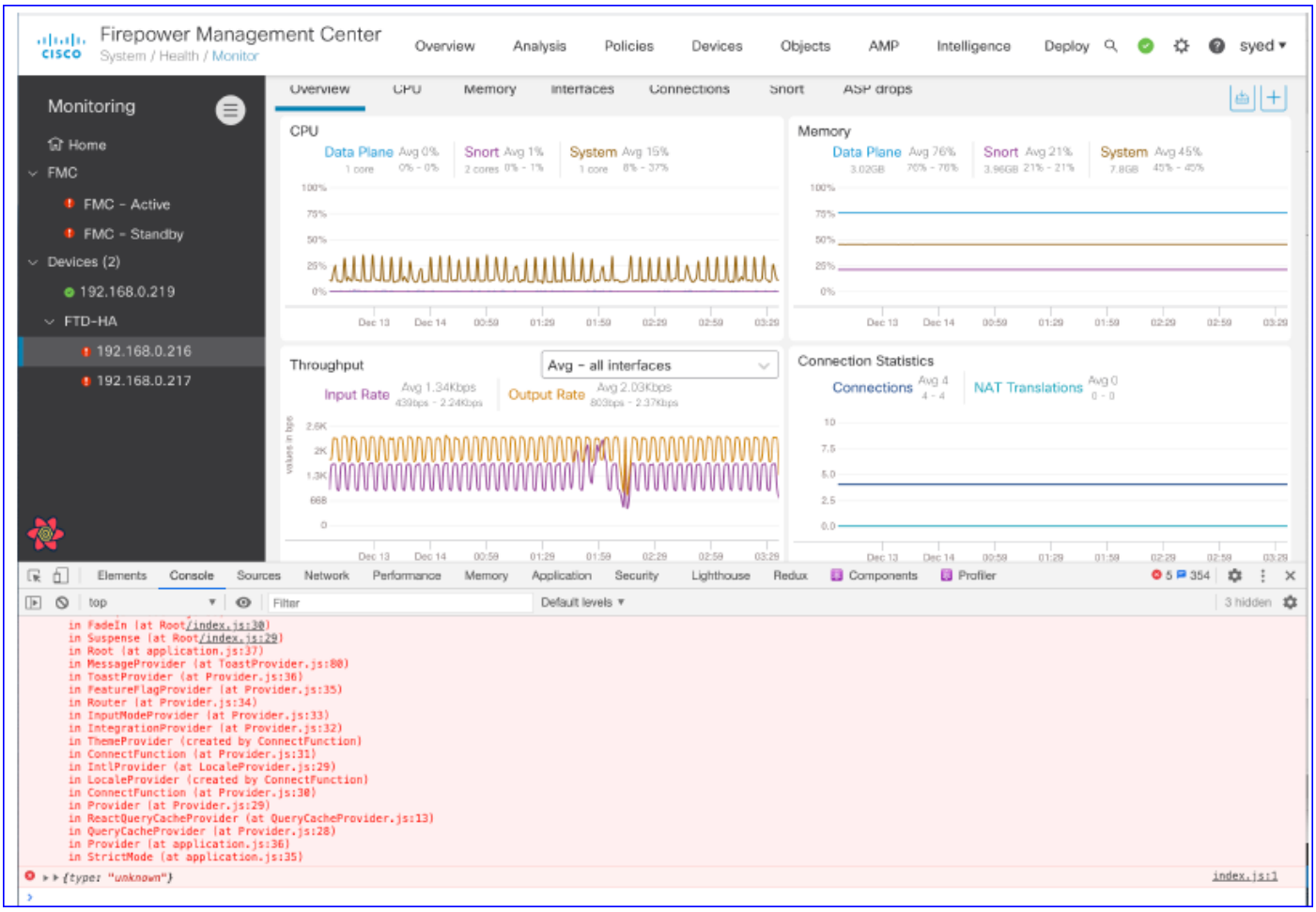
在資料可用時，圖形顯示如下：



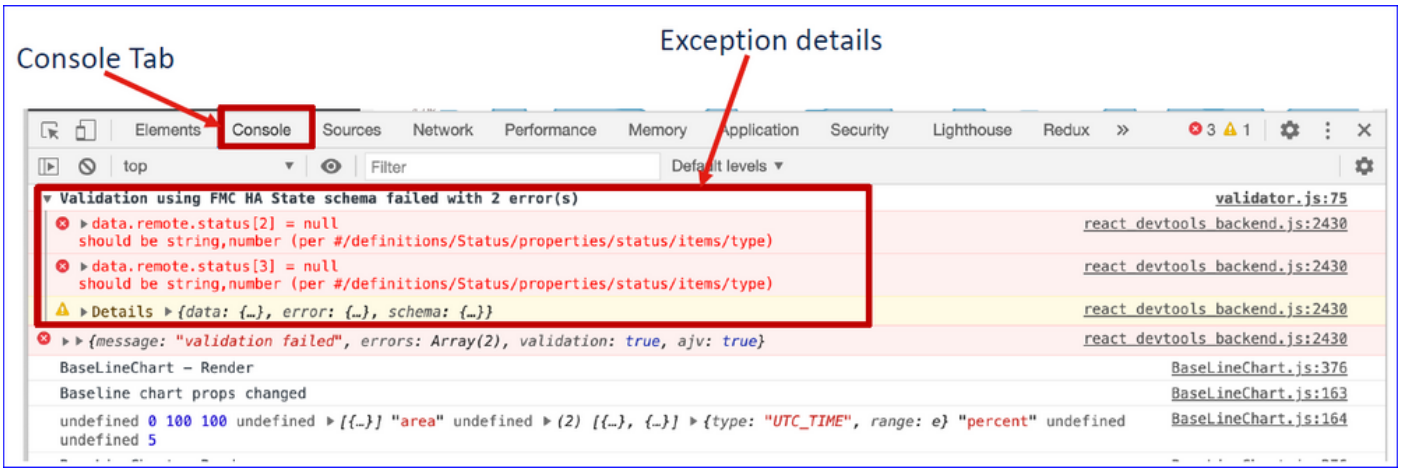
使用瀏覽器的控制檯和網路頁籤

瀏覽器控制檯日誌和網路呼叫日誌

- 在此示例中，顯示Chrome瀏覽器開發者控制檯
- 發生錯誤時，例外詳細資訊會顯示在主控台日誌中



瀏覽器控制檯日誌示例



參考資料

[FMC健康監控 — 6.7]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。