

# FPのアップグレード – デバイスのヘルスマニタリング

## 内容

---

[はじめに](#)

[背景情報](#)

[機能の概要](#)

[機能の詳細7.0](#)

[FTD:FP 7.0で導入されたメトリック](#)

[機能の詳細6.7](#)

---

## はじめに

このドキュメントでは、6.7および7.0リリースで追加された新しいデバイスヘルスマニタリング機能について説明します。

## 背景情報

課題:

ヘルスマニタリングシステムは、デバイスのパフォーマンスを可視化し、事後対処的なデバッグや予防的なアクションを実行します。

包括的な可視性と分析は、次の方法で得られます。

- 主要なメトリックのトレンド・チャート
- イベントオーバーレイ
- カスタマイズ可能なダッシュボード
- 統合されたヘルスマニタリングアーキテクチャ：すべてのマネージャに対して同じデータを表示
- 多数の新しいメトリックとメトリックの拡張性により、さらに多くのメトリックを追加

## 7.0リリースの新機能

FP 7.0との新機能または相違点

- HAをサポートするFMCダッシュボード
- FTDの110以上の新しいメトリック
- FTDスプリットブレインシナリオのヘルスアラート
- 新しい正常性メトリックのカスタム実行間隔

利点

- 異なるサブシステムからのデータとデバイス上のリソースを関連付ける機能を提供することで、システムのデバッグを支援
- さまざまなシステムパフォーマンスメトリックの可視化
- キャパシティプランニング

## 6.7の新機能

新規リリースまたは直前のリリースと異なるリリース (概要):

- FMCでのデバイスヘルスマニタリング用の新しいユーザインターフェイス
- FTD Device REST API:device-metric API : 多くの新しいメトリックが追加されました。
- FMC API : 新しいAPI : ヘルスアラート、ヘルスマトリック、導入の詳細
- ハイレベルなマーケットプレイスの概要、実際のアプリケーション
- 異なるサブシステムからのデータとデバイス上のリソースを関連付ける機能を提供することで、システムのデバッグを支援
- 可視性
- キャパシティプランニング

## 機能の概要

### 仕組み

- FP 7.0でのデバイスヘルスマニタリング
- FMC向けの新しいヘルスダッシュボードで、トレンドチャート、オーバーレイ、カスタムダッシュボードを提供
- FTDダッシュボードで新しいFTDメトリックを利用可能
- 12のカテゴリをカバーする110以上のメトリック
- FTD API : 外部エンティティによるクエリーにメトリックを使用可能にします。

### ボンネットの下で -

- Telegraf ( オープンソースのメトリック収集フレームワーク ) を使用してデバイスの状態を収集します。

### 追加情報

#### ヘルスマニタリングデータが使用可能

- FMCのヘルスダッシュボードで、システムメニュー(System > Health > Monitor)からアクセスできます。
- FMC REST APIから
- デバイスがFDMによって管理されている場合、FTD Device REST APIを使用します。

一部のメトリック ( FMCとFTDの両方 ) はデフォルトで無効になっています

- 一部のメトリックを表示するには、正常性ポリシーの正常性モジュールを有効にして展開する必要があります。

FP 6.7 IFT担当者が要求する機能拡張の実装

- 既定で自動更新
- ダッシュボード上のカスタム時間範囲を使用したフィルタ
- インターフェイスセレクトで、ユーザ定義名（および物理インターフェイス名）でインターフェイスを選択します
- ヘルスモニタの「ホーム」ページからのクロス起動デバイスダッシュボード

#### FP 6.7でのデバイスヘルスマニタリング

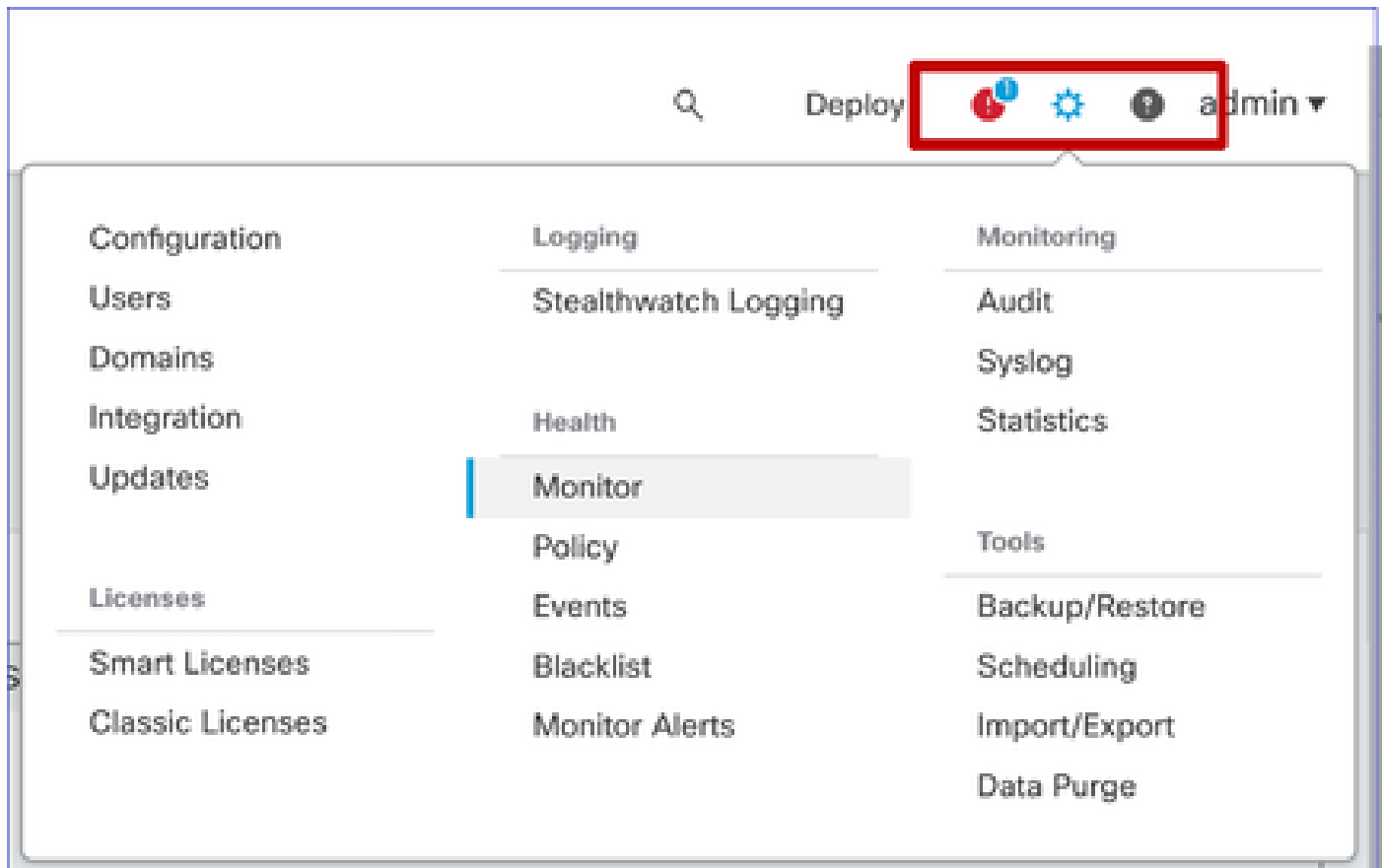
- FMCの新しいUIにより、トレンド・グラフ、オーバーレイ、カスタム・ダッシュボードを提供
- FTD API：外部エンティティによるクエリに同じメトリックを使用できるようにする

#### 制限の概要：

- この機能は、FDM GUIまたはCDOではサポートされていません
- 新しいヘルスマニタリングUIでのFMC自体のモニタリングはサポートされていません。
- ポーリング間隔は設定できません。デバイスごとに異なるポーリング間隔を設定することはできません。すべて、固定の1分間隔でポーリングされます。

#### 導入例

- 機能のテストに特定の導入は必要ありません。FMCとデバイスをFP 6.7にアップグレードするだけです。
- ヘルスモニタリングデータは、FMCのヘルスダッシュボードのシステムタブからアクセスできます。



## 前提条件とサポートされるプラットフォーム

### サポートされる最低限のソフトウェアおよびハードウェアプラットフォーム

サポートされる Manager の最小バージョン	管理対象デバイス	サポートされる管理対象デバイスの最小バージョンが必要	注意事項
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	FTDでのみサポート
FTDデバイスREST API	FTD 6.7	FXOS 2.9.1 FTD 6.7	FTDデバイスREST APIのみ ( FDMまたはCDO GUI以外 )

### 相互運用性

相互運用性に関する特別な要件はありません。

## 機能の詳細7.0

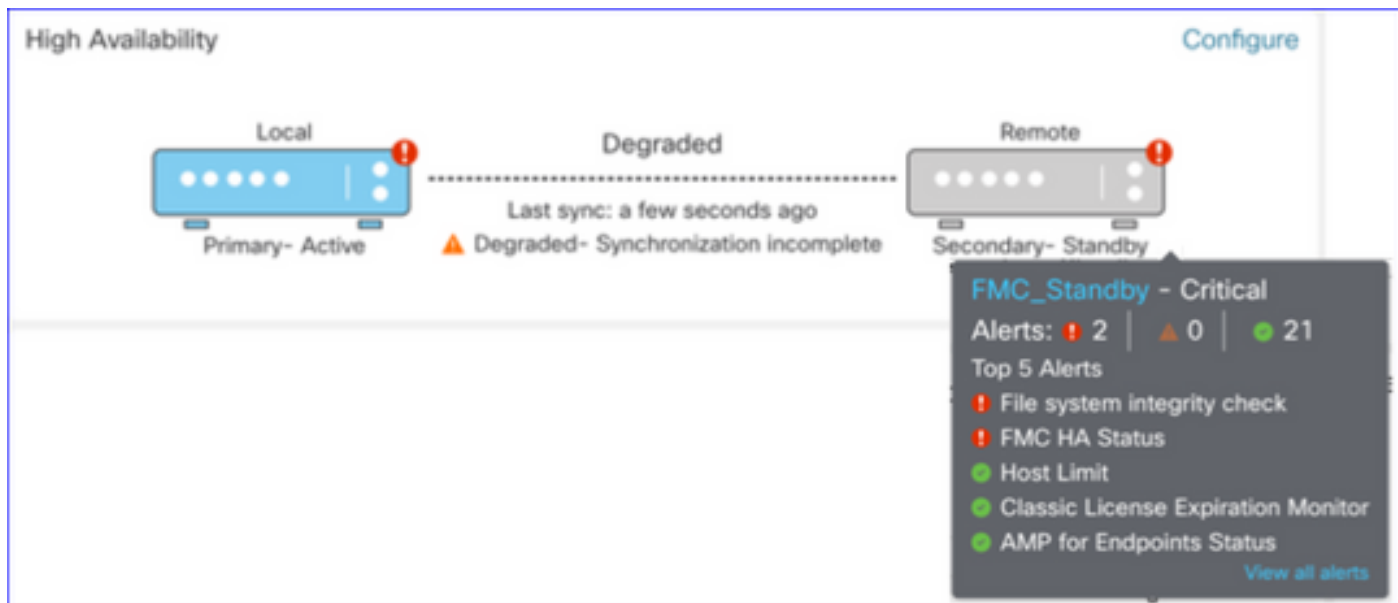
FMC UI : スタンドアロンおよびHAサポート

ヘルスマonitoringページのナビゲーション

The screenshot shows the Cisco FMC Monitor interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', and 'Deploy'. The left sidebar has 'Monitoring' selected, with 'FMC' and 'Devices (2)' listed. The main content area is titled 'Health Status' and shows a summary of 4 total devices (2 critical, 0 warnings, 1 normal, 1 disabled). Below this, there are two columns: 'FMC' and 'Devices'. The 'FMC' column shows 'Active FMC' (critical) and 'Standby FMC' (normal). The 'Devices' column shows 'FMC\_Active' (critical), 'FMC\_Standby' (normal), and two IP addresses (192.168.0.216 and 192.168.0.217) with their respective health status icons.

- スタンドアロンFMCは単一ノードとして表示されます
- ノードのペアとして表示されるFMC HA
- 各FMCにはヘルスステータスが表示されます





## HAパネルに

- 現在のHAステータス
- アクティブとスタンバイ
- 前回の同期時刻
- デバイスヘルス

## FMCダッシュボード：イベントレートとキャパシティ

### イベントレート

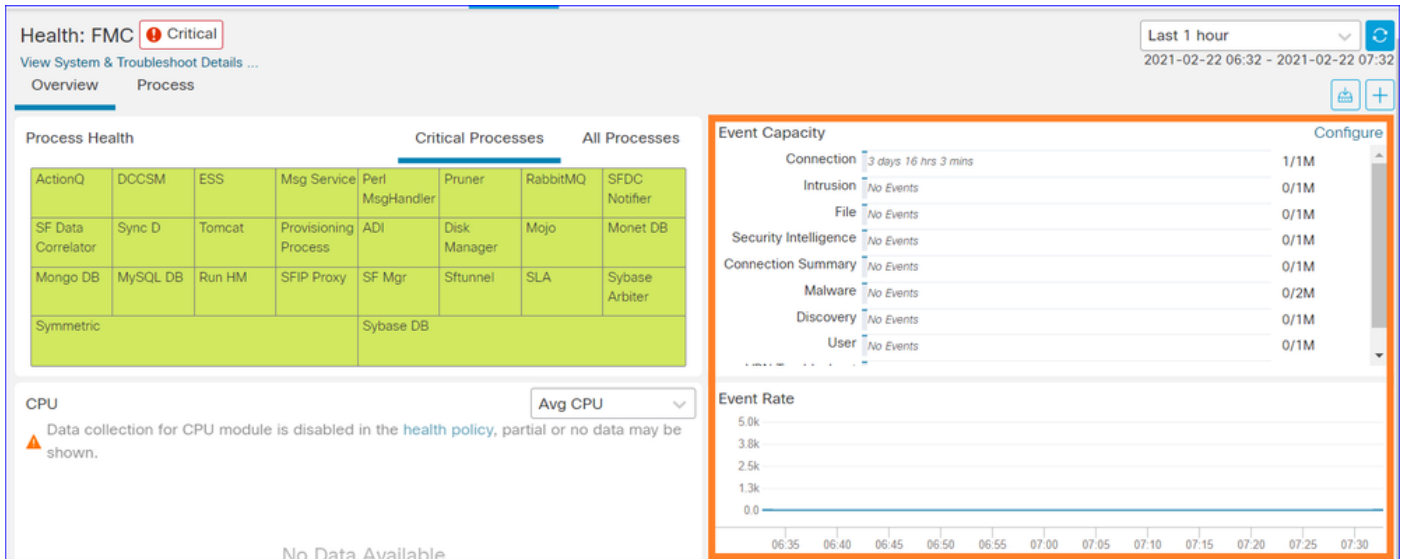
- ベースラインとしての最大イベントレート
- FMCが受信する全体的なイベントレート

### イベント容量

- イベントカテゴリ別の現在の消費量
- イベントの保持時間
- 現在と最大

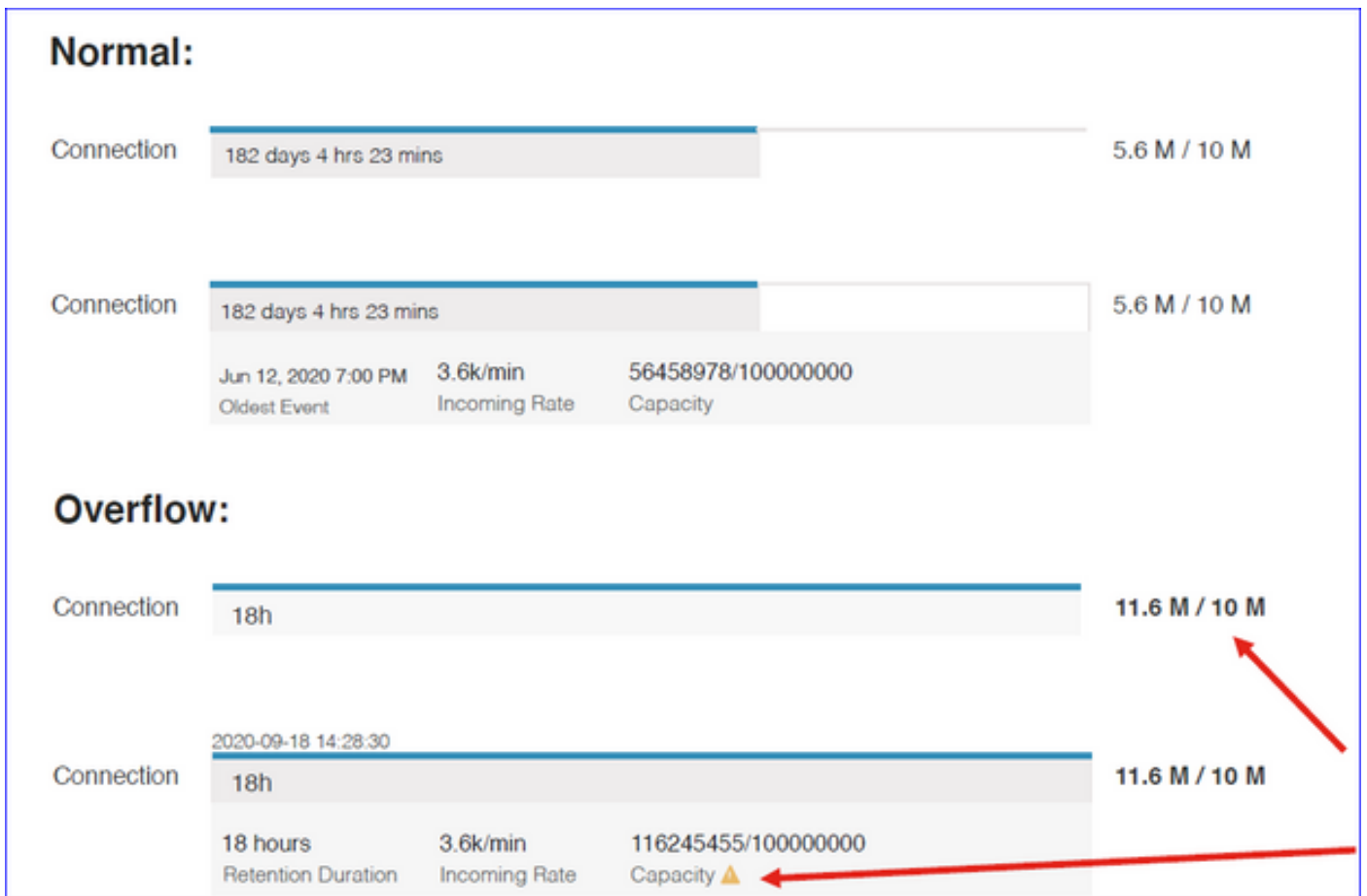
### イベントキャパシティ

- キャパシティオーバーフローマーカー



## FMCダッシュボード : Event Capacity

### 通常イベントの容量消費状態



イベントが設定された最大容量を超えて保存された場合のオーバーフローシナリオ。

- 太字はオーバーフローを示します。
- 警告アイコンがキャパシティオーバーフローを強調表示します

## FMCダッシュボード : FMCプロセスパネル

## 重要なプロセス・パネルの表示

- 現在の状態の処理
- プロセスの再起動カウント

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	

プロセスパネルには、すべての「pmconfig」プロセスに関する次のメトリックが表示されます。

- 現在の状態
- CPU使用率
- メモリ使用量

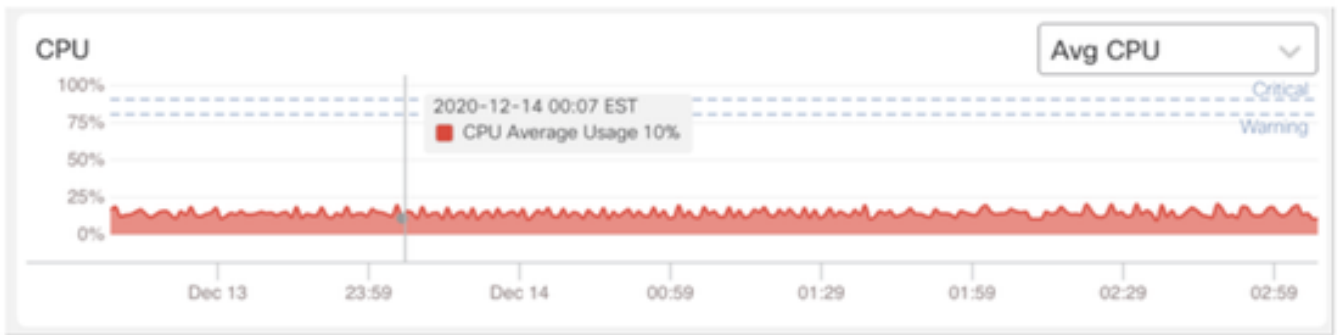
Process Health		Critical Processes		All Processes
Process status at: Dec 14, 2020 3:22 AM				
Process	Status	CPU (%)	Mem Used	
ActionQ	Running	0	66.23KB	
CSD App	Waiting	0	0	
CSM Event Server	Running	0.6	182.1KB	
CloudAgent	Running	0.9	12.03KB	
DCCSM	Running	0	104.49KB	
ESS	Running	0.1	448.26KB	
Event DS	Running	0	34.59KB	

## FMCダッシュボード : FMC CPU

### CPUパネルに

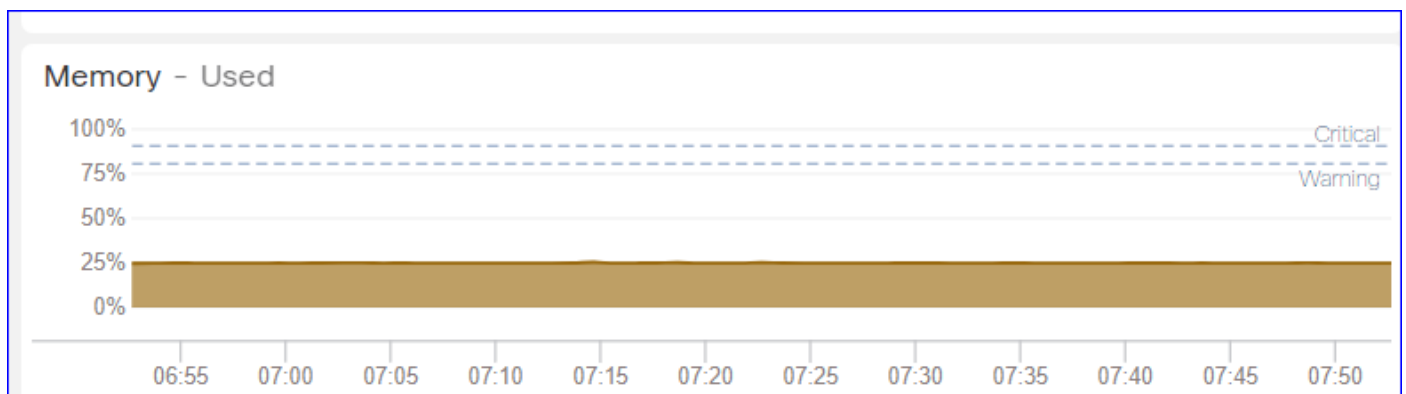
- 平均CPU ( デフォルト )
- すべてのコア



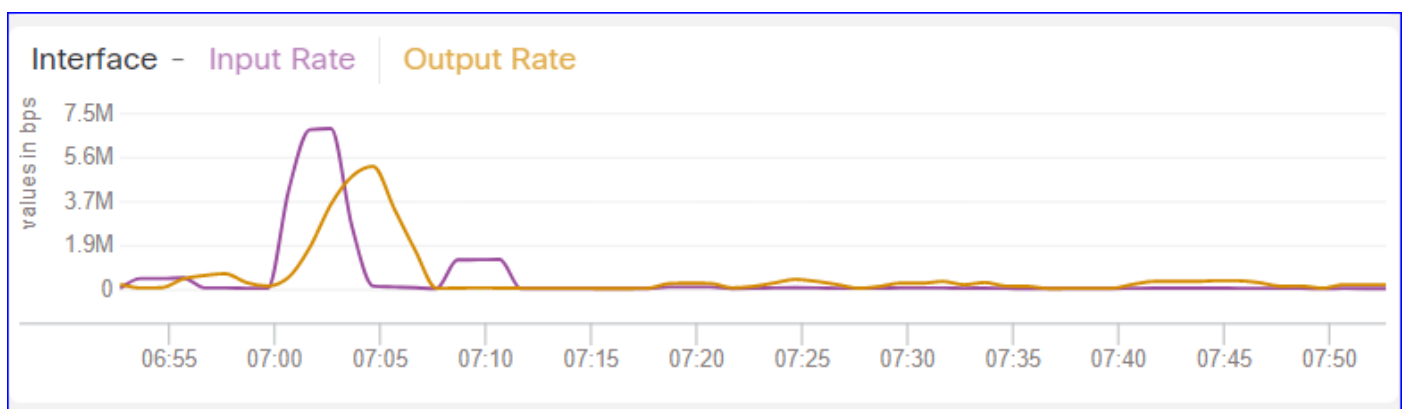


FMCダッシュボード：その他のパネル

MemoryパネルにFMCの全体的なメモリ使用量が表示されます。

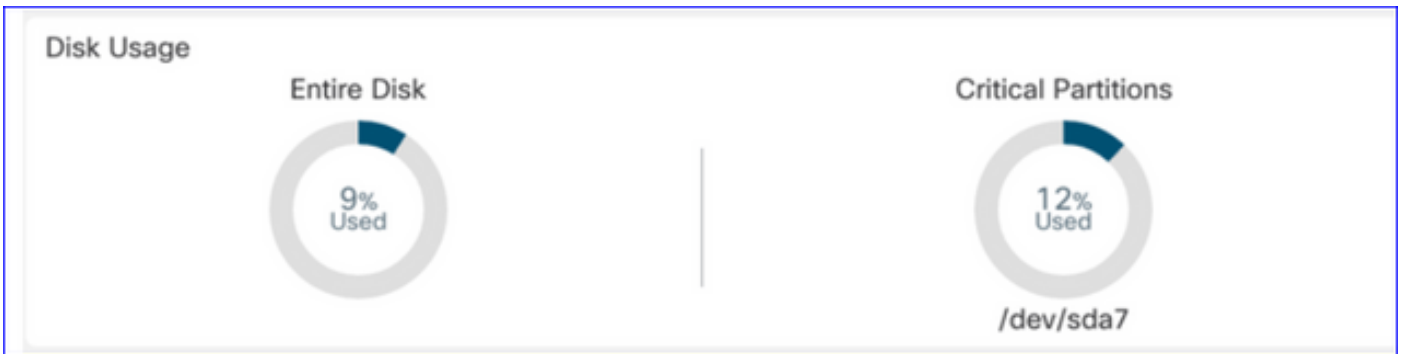


Interface panelは、すべてのインターフェイスの平均の入出力レートを示します。



ディスク・パネルに

- ディスク全体の容量
- FMCデータが保存される重要なパーティション容量



## 実行間隔

- 古い正常性モジュールの実行間隔は'レガシ実行間隔'に名前が変更されています
- 「実行間隔」は、新しいTelegrafベースのヘルスマジュールを対象としています。
- グローバル設定、すべてのデバイスに影響

The screenshot shows the Cisco FMC interface for editing a policy. The policy name is 'Initial\_Health\_Policy 2021-01-29 04:40:49' and the description is 'Initial Health Policy'. Two input fields are highlighted with a red box: 'Legacy Run Time Interval (mins)' with a value of 5, and 'Run Time Interval (mins)' with a value of 1. Below these fields is a note: '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.

## 利用可能なメトリック

### カスタムダッシュボードで利用可能なメトリック

- カスタムダッシュボードを作成する場合、これらのスライドは利用可能なメトリックのガイドになります。
- 一部のメトリックは、カスタムヘルスダッシュボードで使用する前に、ヘルスポリシーで有

効にする必要があります

The screenshot shows the Cisco FMC 'Edit Policy' interface. The left sidebar contains a list of monitoring categories, with 'CPU Usage (per core)' selected. The main area displays the configuration for the policy 'Initial\_Health\_Policy 2020-12-08 08:49:46'. The configuration includes:

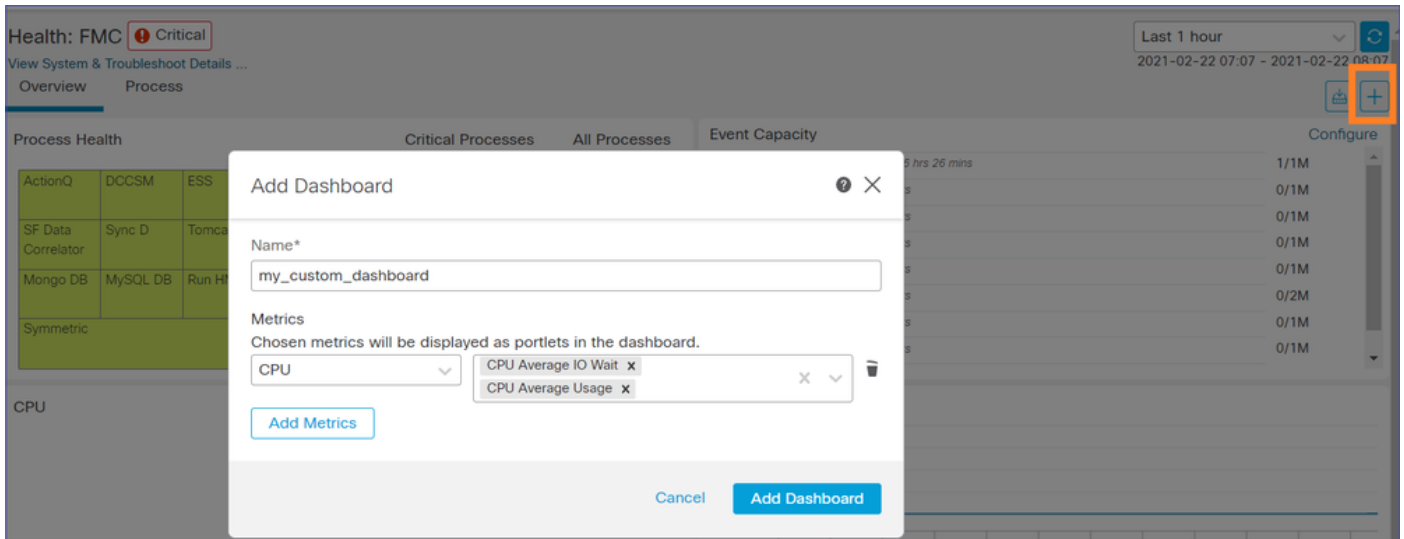
- Policy Name: Initial\_Health\_Policy 2020-12-08 ( )
- Policy Description: Initial Health Policy
- Description: Monitors CPU usage on all the cores, threshold set here will be applicable to all the cores
- Enabled:  On  Off
- Critical Threshold %: 90
- Warning Threshold %: 80

Buttons for 'Cancel' and 'Save Policy and Exit' are visible at the bottom right of the form.

## FMC UI:FMCカスタムダッシュボード

### 7.0の新しいFMCモニタリングメトリックのカテゴリ

- CPU
- メモリ
- インターフェイス
- Disk
- [Event]
- プロセス
- RabbitMQ
- Sybase
- MySQL



## FMC UI:FMCメトリック

さまざまなカテゴリで40個のメトリックが追加されました（カスタムダッシュボードで使用可能）。無効なメトリックを有効にするには、関連付けられた正常性ポリシー(System > Health > Policy)で対応する正常性モジュールを有効にします。

メトリックグループ名	デフォルトで有効	説明
CPU	いいえ	FMC CPUのモニタ
メモリ	Yes	FMCメモリのモニタ
Disk	Yes	FMCのディスク使用率の監視
インターフェイス	Yes	FMCインターフェイスの監視
プロセス	Yes	FMCプロセスの監視
[Event]	Yes	イベントレートの監視
MySQL	いいえ	MySQLの監視
RabbitMQ	いいえ	RabbitMQのモニタ
Sybase	いいえ	Sybaseの監視

## FTD:FP 7.0で導入されたメトリック

デフォルトで有効：メトリックはデフォルトで収集されます。無効なメトリックを有効にするには、関連付けられた正常性ポリシー（[システム] > [正常性] > [ポリシー]）で対応する正常性モジュールを有効にします。

メトリックグループ名	デフォルトで有効	説明	Platform
シャーシのステータス	Yes	ファンの速度や温度など、さまざまなシャーシパラメータを監視します。	FPR2100およびFPR1000プラットフォームにのみ適用可能
フロー オフロード	Yes	ハードウェアフローのオフロード統計情報の監視	FPR9300に適用可能 およびFPR4100プラットフォーム
ASPドロップ	Yes	Lina側のパケットドロップの監視	すべて
ヒットカウント	いいえ	アクセスコントロールポリシーのヒットカウントの監視	すべて
AMP Threat Gridのステータス	Yes	AMPへの接続を監視 ThreatGrid	すべて
AMP接続ステータス	いいえ	FTDからAMPクラウド接続を監視	すべて
SSEコネクタステータス	いいえ	FTDからSSEクラウド接続を監視	すべて
NTPステータス	いいえ	NTPクロック同期パラメータをモニタする FTD	すべて
VPN統計情報	Yes	S2SおよびRA VPNトンネル	すべて

		の統計情報を監視します。	
ルート統計情報	Yes	Lina側のパケットドロップの監視	すべて
Snort 3パフォーマンス統計情報	Yes	特定のSnort3パフォーマンス統計情報の監視(perfstats)	すべて
xTLSカウンタ	いいえ	xTLS/SSLフロー、メモリ、およびキャッシュの有効性を監視	すべて

## REST API、Syslog、SNMP

7.0では、新しいFMCまたはFTDデバイスREST APIは導入されていません。既存のREST APIは、7.0で追加された新しいメトリックをサポートします。

### SyslogおよびSNMP

#### Syslog

- ヘルスマニタのsyslogに変更なし

#### SNMP

- 「SNMPデバイスヘルスマニタリング」用の個別のTOI

### SAL/CTR/サードパーティ製品統合

- 「Azure Application Insights」サポート用にTOIを分離
- 「ヘルスマニタリング」とSAL/CTR/SecureXの統合をサポートする具体的な変更は行われていない
- REST APIはサードパーティの統合に利用できる

## ソフトウェア技術

## 機能の詳細6.7

### FTDの健全性とパフォーマンスに対する新しいNGFWヘルスマニタリング

#### 次の機能をユーザに提供

- 問題が発生した後の根本原因の分析などの事後的なデバッグ
- 使用状況や飽和状態の監視などの予防的なアクションにより、潜在的なキャパシティの問題を特定し、ユーザがキャパシティの拡張やリファクタリングを実行できるようにします。

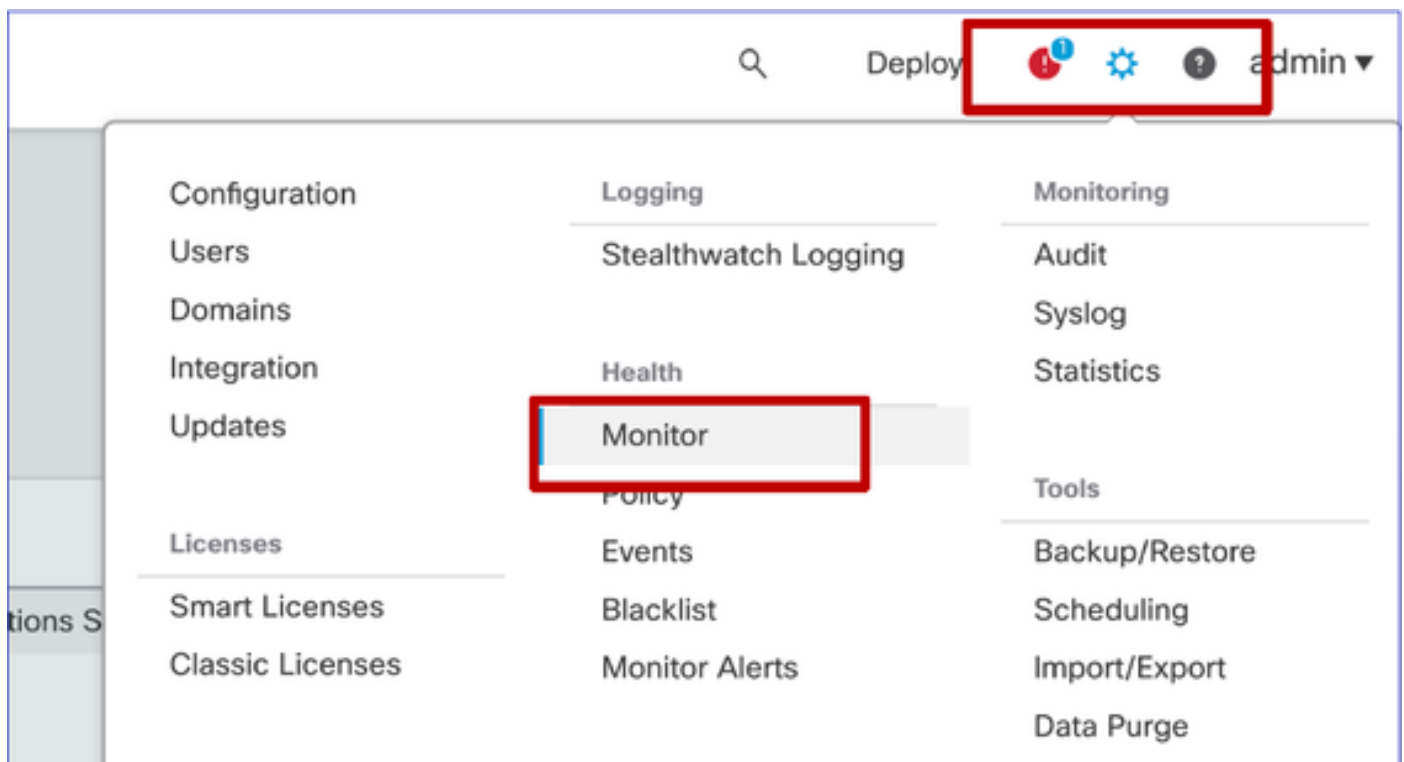
## ハイライト

- 傾向グラフ：傾向グラフを使用すると、異常を簡単に検出し、問題の根本原因を特定できます。目視でトレンドを確認し、異なるメトリック間に相関関係をプロットして、メトリック間の因果関係を見つけることができます。
- イベントオーバーレイ：イベントオーバーレイには、構成の展開や傾向グラフでのSRU更新など、因果関係を示す重要な情報が表示されます。
- カスタマイズ可能なダッシュボード：ユーザは独自のダッシュボードを作成して、メトリックを1ページにまとめて表示できます。
- ユニファイドヘルスマonitoringアーキテクチャ：どのマネージャがメトリックに関心を持っているかに関係なく、メトリックの収集とエクスポートを一元的に行うことができます。FTD APIとFMCは、同じメトリックコレクタのデータを使用します。
- メトリックの拡張性：プラットフォームのアーキテクチャの目標の1つは、新しいメトリックを簡単に追加できることでした。これは、オープンソースのメトリック収集およびストレージツールと、カスタマイズ可能なダッシュボードを使用して実現されます。

## FMCのGUI

### FMC UI：ヘルスステータスへの移動

FMCで、Systemアイコン> Health > Monitorの順にクリックして、Health Statusページに移動します。

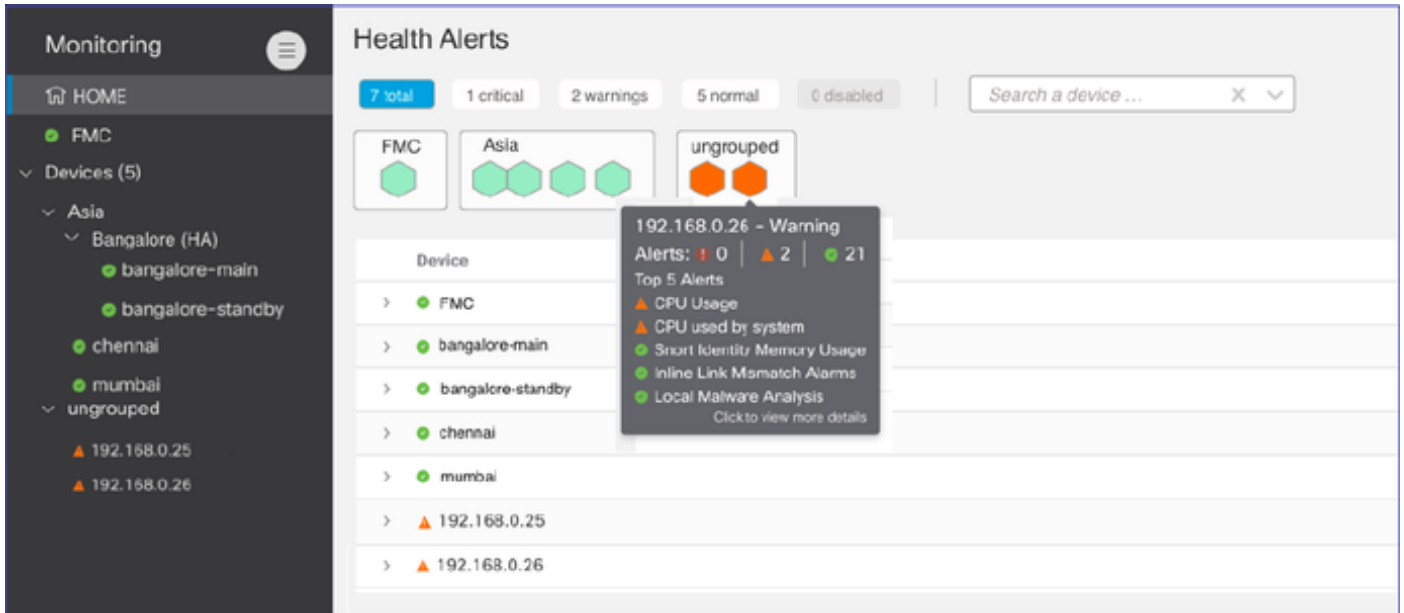


### FMC UI：新しいヘルスステータスページ

Health Statusページには、FMCの健全性を含む、FMCが管理するすべてのデバイスの健全性の概要が表示されます。

- デバイスは、グループ/ha/クラスタごとにグループ化されます。

- デバイスの左側にあるドットは、デバイスの状態を示します
- 緑 – アラームなし
- オレンジ – 少なくとも1つの正常性警告
- 赤 – 少なくとも1つの重大なヘルスアラーム
- デバイスの健全性を示す六角形にマウスを合わせると、健全性の概要が表示されます。
- 警告と重大のしきい値は、FP 6.7より前と同じ方法で、正常性ポリシーで設定できます。



## FMC UI : デバイスのヘルスイベント

下部のパネルでデバイスをクリックすると、デバイスに関連するヘルスイベントが表示されます。アラートはヘルスステータス ( 重大度 ) でソートされます。

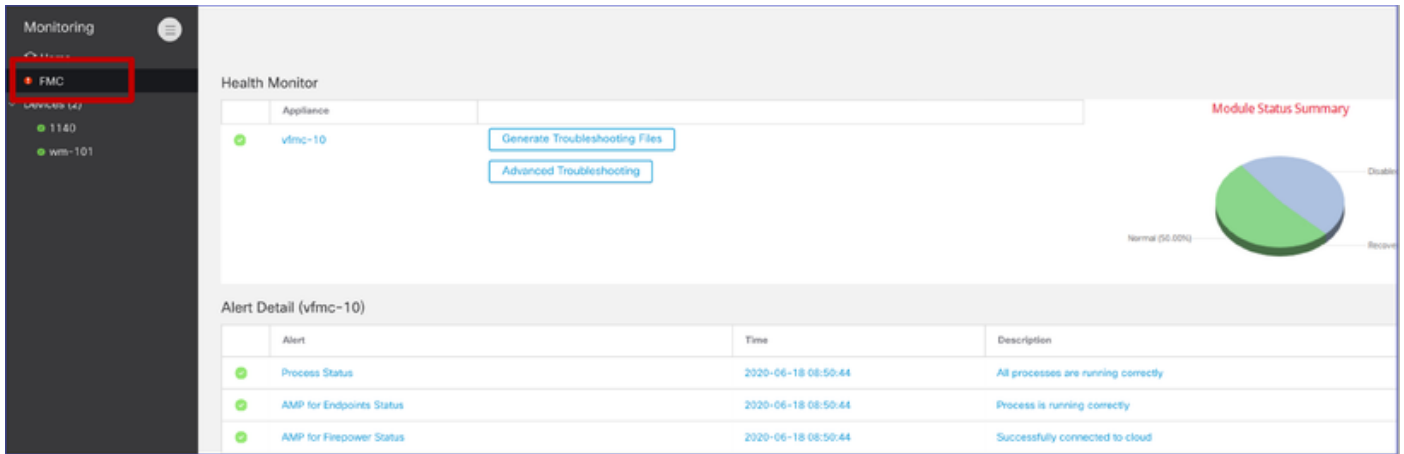
## ヘルスマニタリングページ

>	▲ 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

FMC UI:FMCヘルスマニタリングは変更されていません

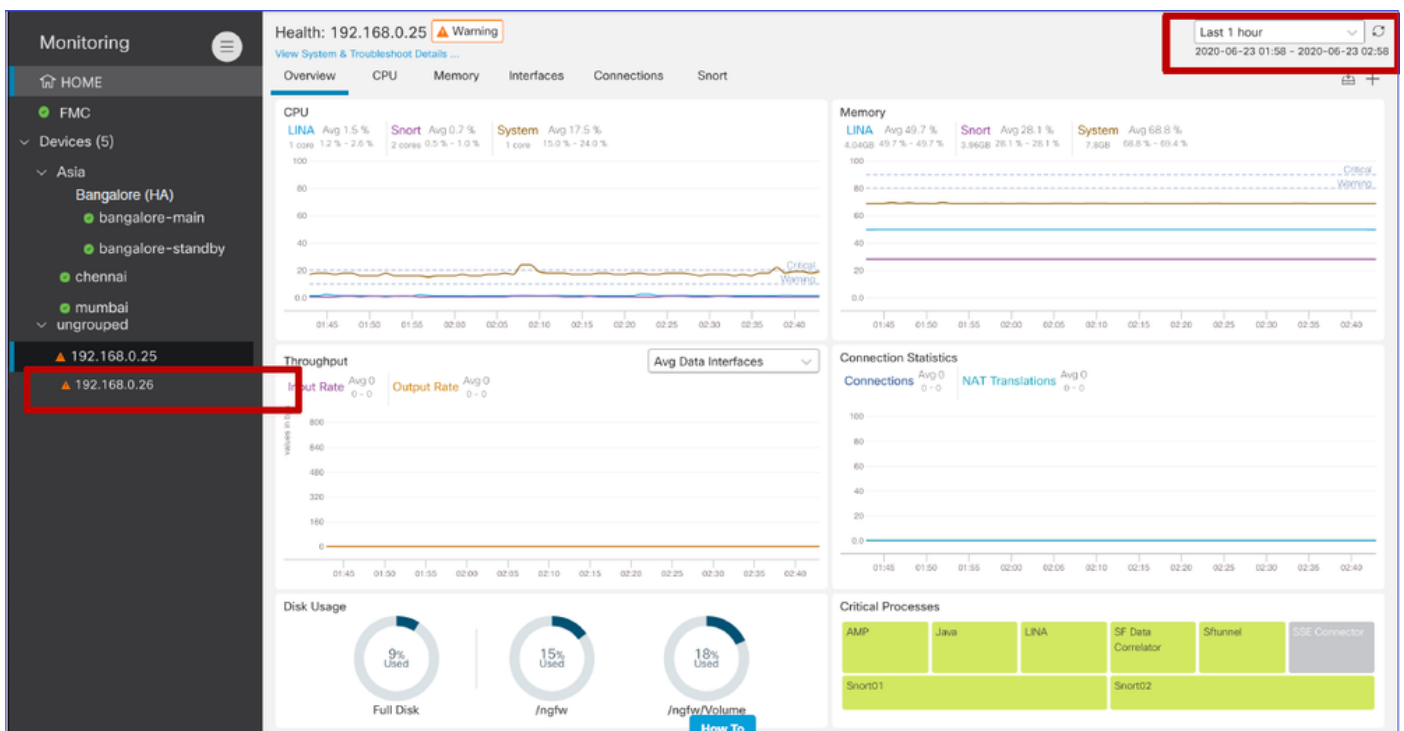
FMCの健全性ページは引き続きレガシーページです。新しいUIは、6.7以降のFTDでのみサポートされます





## FMC UI : 新機能デバイスダッシュボード

- 左側のペインでデバイス名をクリックして、デバイスの健全性の概要ページに移動します。
- 健全性の概要には、主要な健全性メトリックのトレンドチャートがすべて含まれています。
- さまざまな時間範囲を使用できます ( デフォルトは過去1時間 )。
- グラフを再読み込みするには自動更新を行います



## FMC UI : 導入データのオーバーレイ

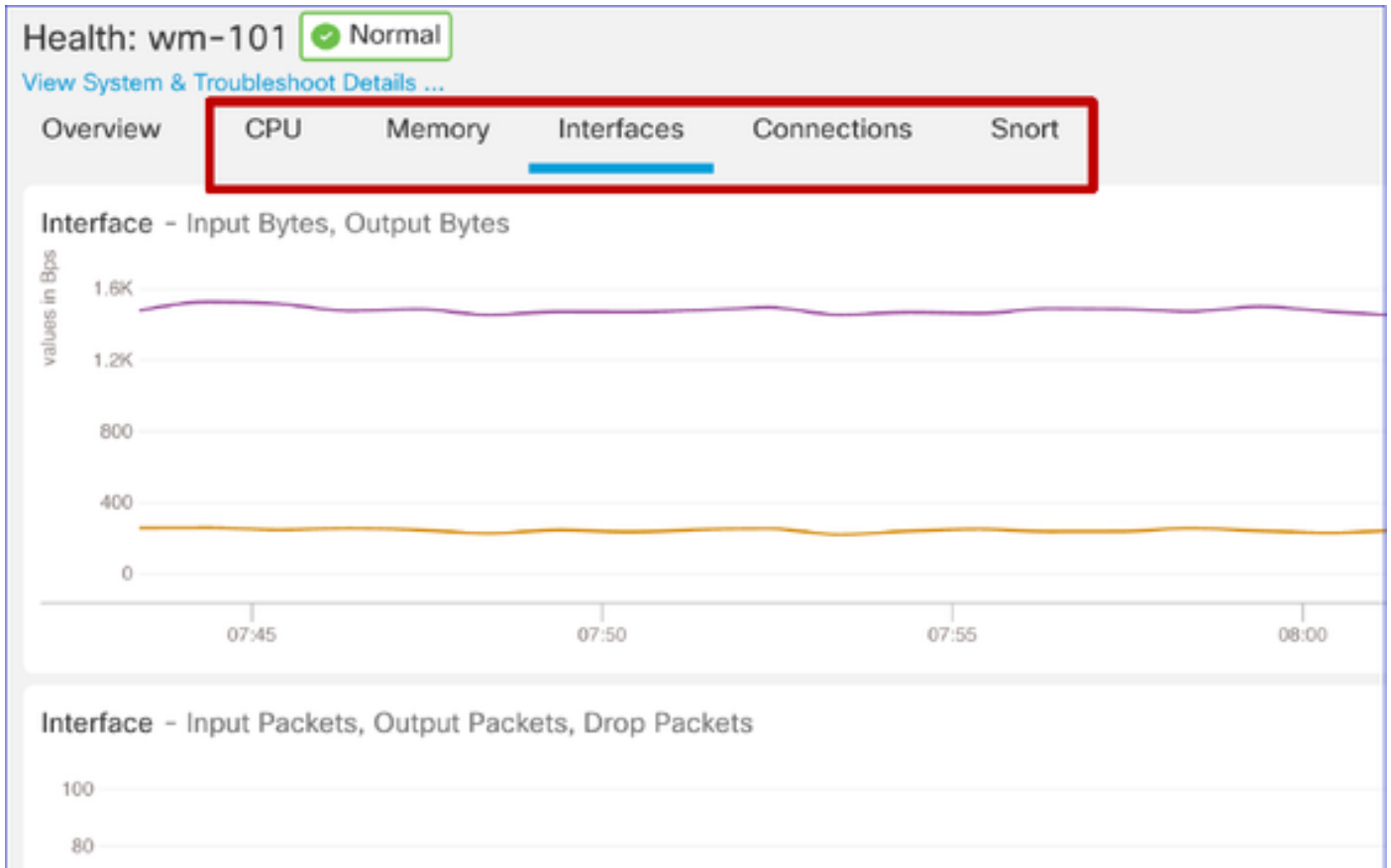
展開アイコンをクリックすると、選択した時間範囲の展開オーバーレイの詳細がグラフに表示されます

- アイコンは、選択した時間範囲内の導入数を示します
- バンドは、導入の開始時刻と終了時刻を示します。
- 複数の展開の場合、複数のバンド/ラインが表示されます
- 点線の上にあるアイコンをクリックして、詳細を表示します

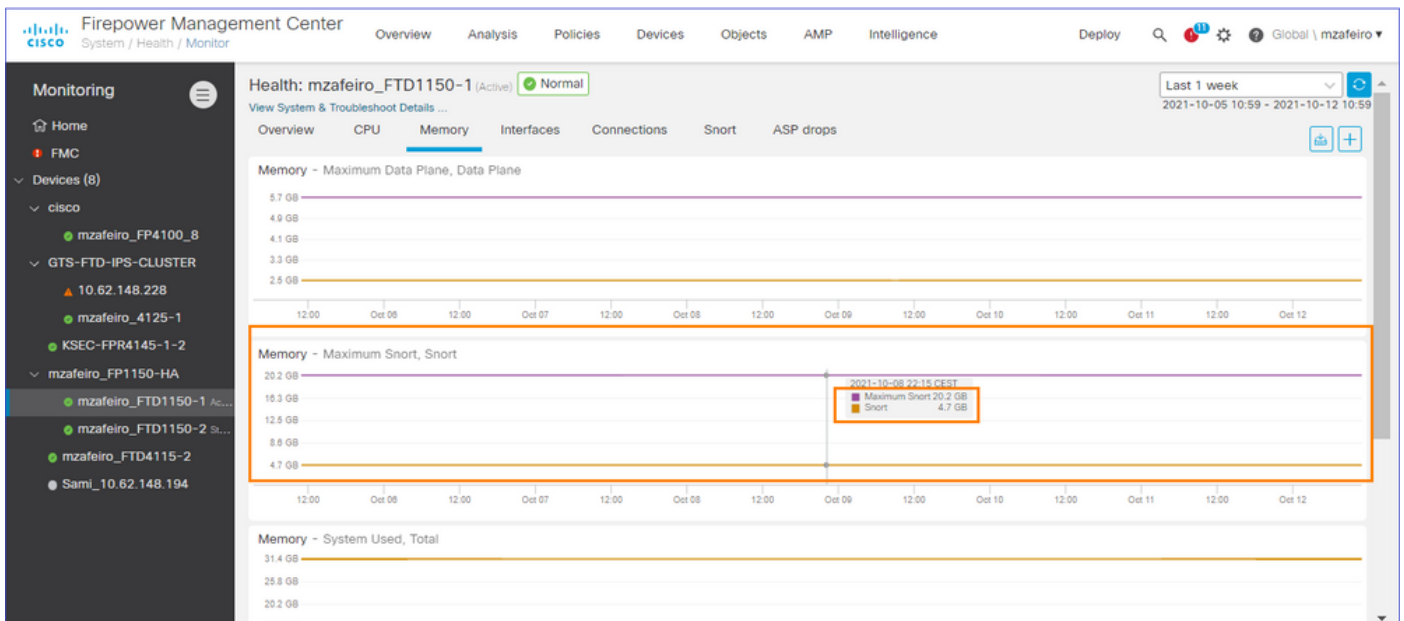


## FMC UI : デバイスの構築済みダッシュボード

- FMCのUIには、構築済みのヘルスダッシュボードが表示されます。
- これらの構築済みダッシュボードには、関連するメトリックがグループ化されて表示されます。
- インターフェイスダッシュボードには、さまざまなインターフェイスの入出力バイト、パケット、平均パケットサイズなど、すべてのインターフェイス関連メトリックのトレンドチャートがあります。



FTD Snortメモリ：どこから発生するか？

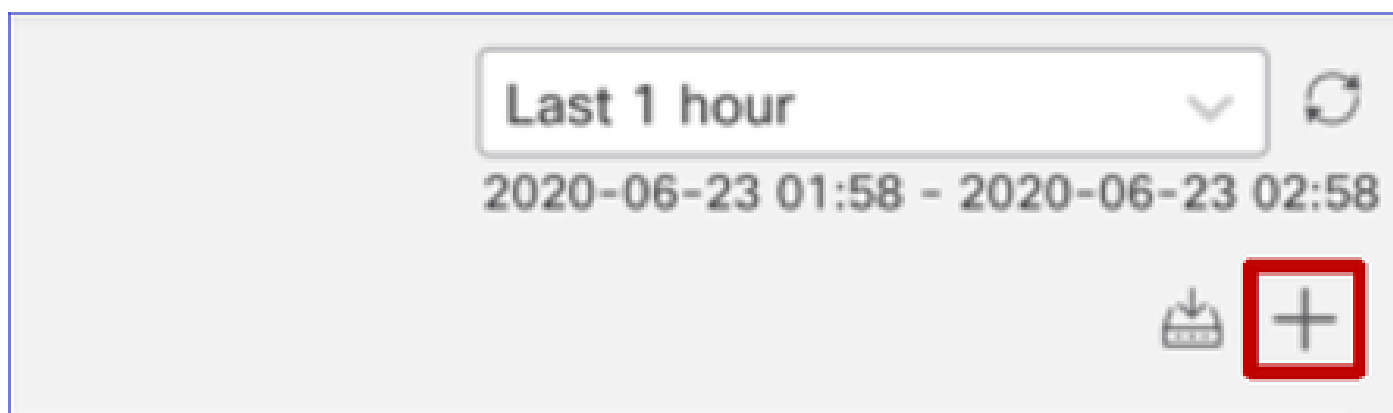


FMC UI：カスタムダッシュボードを作成可能

ユーザは独自のカスタムダッシュボードを作成できます

- 事前に作成されたダッシュボードに加えて、ユーザはカスタムダッシュボードを作成することもできます。

- カスタムダッシュボードでは、任意の数のメトリックを追加できます。
- 通常、異なるメトリックグループのメトリックを関連付けて問題の根本原因を突き止めることができれば、カスタムダッシュボードが作成されます。
- Lina CPUの使用率が高い場合、CPU使用率が高くなる原因となる着信接続/秒(CPS)、インターフェイス統計情報などを確認できます。



FMC UI : カスタムダッシュボードの作成

Correlate Metricsダイアログ

- ユーザが「+」をクリックしてカスタムダッシュボードを作成すると、[Correlate Metrics]ウィンドウが開きます。
- ユーザは、一緒にモニタしたいさまざまなメトリックを追加できます。

## 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>	
Interface <span style="float: right;">▼</span>	Input Packets <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>	
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>	

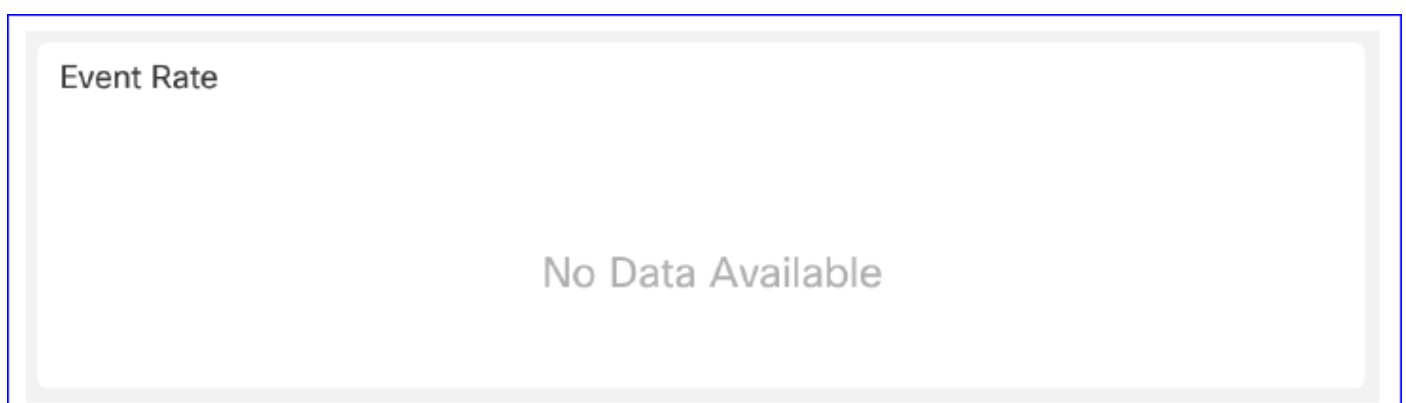
[Add Metrics](#)

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

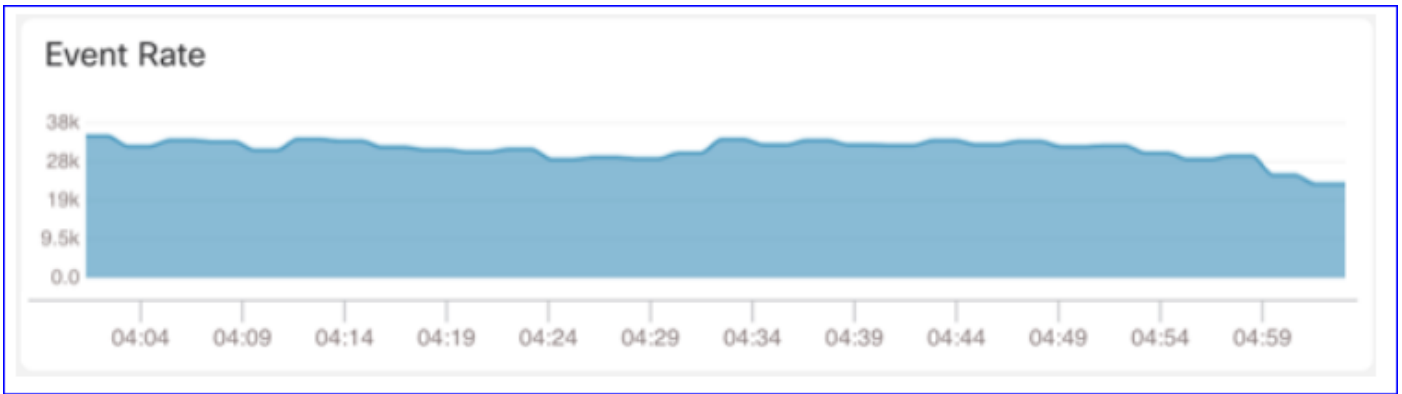
(デバイス)からのデータの収集 - GUI

GUIに表示される時間範囲のデータ

ヘルスマニタに選択した時間範囲のデータがない場合、GUIのダッシュボードパネルに「No Data Available」と表示されます。



データが使用可能な場合、グラフは次のように表示されます。



ブラウザのコンソールタブとネットワークタブの使用

ブラウザコンソールログとネットワークコールログ

- この例では、Chromeブラウザ開発者コンソールが表示されます
- エラーの場合、例外の詳細がコンソールログに表示されます

The screenshot displays 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, a browser developer console is open, showing 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".

ブラウザコンソールログの例

Console Tab

Exception details



## 参考資料

[FMCヘルスマニタリング - 6.7](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。