

Atualizar FP - Monitoramento de integridade do dispositivo

Contents

[Introdução](#)

[Informações de fundo](#)

[Visão geral do recurso](#)

[Detalhes do recurso 7.0](#)

[FTD: Métricas Introduzidas no FP 7.0](#)

[Detalhes do recurso 6.7](#)

Introdução

Este documento descreve o novo recurso de monitoramento da Integridade do Dispositivo adicionado nas versões 6.7 e 7.0.

Informações de fundo

O problema:

O sistema de monitoramento de integridade oferece visibilidade do desempenho do dispositivo para depuração reativa e ações proativas.

Visibilidade e análise abrangentes são obtidas por:

- Gráficos de tendência para métricas-chave
- Sobreposição de eventos
- Painéis personalizáveis
- Arquitetura de monitoramento de integridade unificada - ver os mesmos dados para todos os gerentes
- Muitas métricas novas e extensibilidade de métricas para adicionar muito mais

Novidades na versão 7.0

Novidades ou diferenças em comparação com o FP 7.0

- Painel FMC com suporte a HA
- Mais de 110 novas métricas para FTD
- Alerta de integridade para o cenário de divisão de cérebro de FTD
- Intervalo de tempo de execução personalizado para métricas de integridade mais recentes

Benefícios

- Auxilia na depuração do sistema, fornecendo a capacidade de correlacionar dados de diferentes subsistemas e recursos no dispositivo
- Visibilidade de várias métricas de desempenho do sistema
- Planejamento de capacidade

Novidades no 6.7

Novo ou diferente em comparação com a versão imediatamente anterior (alto nível):

- Nova interface de usuário para monitoramento de integridade de dispositivos no FMC
- API REST de dispositivo FTD: API de métrica de dispositivo: muitas métricas novas adicionadas
- APIs do FMC: novas APIs: alertas de integridade, métricas de integridade e detalhes de implantação
- Visão geral do mercado de alto nível, aplicativos reais
- Auxilia na depuração do sistema, fornecendo a capacidade de correlacionar dados de diferentes subsistemas e recursos no dispositivo
- Visibilidade
- Planejamento de capacidade

Visão geral do recurso

Como funciona

- Monitoramento da integridade do dispositivo no FP 7.0
- Novo painel de integridade para o FMC, que fornece gráficos de tendências, sobreposições e painéis personalizados
- Novas métricas de FTD disponíveis nos painéis de FTD
- Mais de 110 métricas abrangendo 12 categorias
- APIs de FTD: disponibiliza métricas para consulta por entidades externas

Sob o capô,

- Coleta a integridade de um dispositivo com Telegraf (uma estrutura de coleta métrica de código aberto)

Notas adicionais

Dados de monitoramento de integridade disponíveis

- No Painel de saúde do FMC, acessível no menu do sistema (Sistema > Saúde > Monitor)
- Da API REST do FMC
- Quando o dispositivo é gerenciado pelo FDM, por meio da API REST do Dispositivo FTD

Algumas das métricas (FMC e FTD) são desativadas por padrão

- Os módulos de Integridade na Política de Integridade precisam ser habilitados e implantados para que algumas métricas sejam exibidas.

Implementação das melhorias solicitadas pelos IFT do 6.7 PQ

- Atualização automática por padrão
- Filtrar com intervalo de tempo personalizado no painel
- Selecione as interfaces pelo nome definido pelo usuário (assim como o nome da interface física) no seletor de interface
- Painel do dispositivo de inicialização cruzada a partir da página 'Home' do Health Monitor

Monitoramento da integridade do dispositivo no 6.7 do PQ

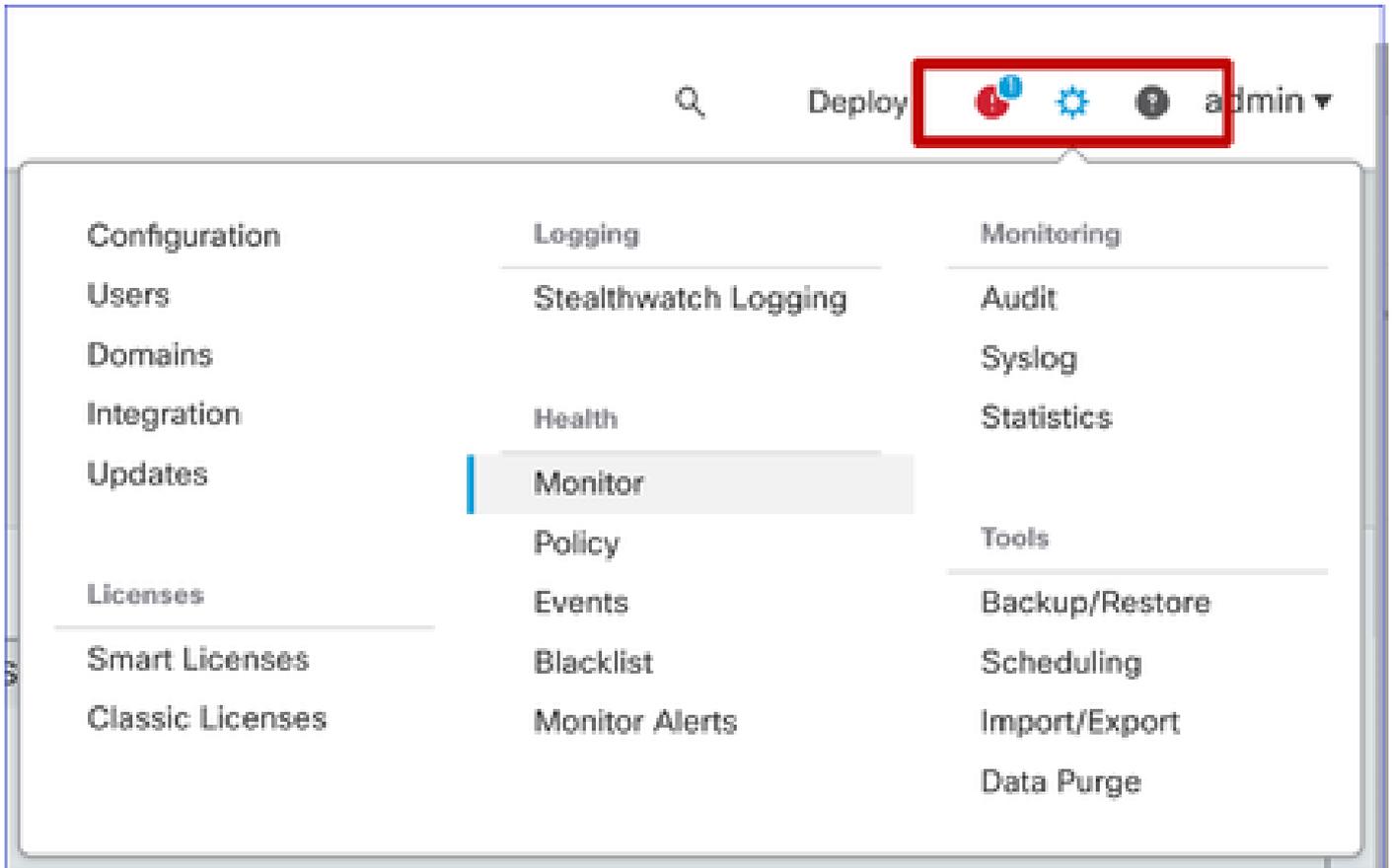
- Nova interface do usuário no FMC, que fornece gráficos de tendências, sobreposições e painéis personalizados.
- APIs de FTD: disponibiliza as mesmas métricas para consulta por entidades externas

Resumo das limitações:

- O recurso não tem suporte na GUI ou no CDO do FDM
- Não há suporte para o monitoramento do próprio FMC na nova interface do usuário de monitoramento de integridade.
- Os intervalos de pesquisa não são configuráveis. Não é possível configurar intervalos de pesquisa diferentes para dispositivos diferentes. Todos são pesquisados no intervalo fixo de um minuto.

Exemplos de implantação

- Nenhuma implantação específica é necessária para testar o recurso. Basta atualizar o FMC e o dispositivo para o FP 6.7.
- Os dados de monitorização da saúde estão disponíveis no painel de controlo da saúde do CVP, acessível a partir da guia do sistema.



Pré-requisitos e plataformas suportadas

Plataformas mínimas de software e hardware suportadas

Mín. de Versão do Gerenciador com Suporte	Dispositivos gerenciados	Mín. de Dispositivos Gerenciados com Suporte Versão Necessária	Notas
CVP 6.7	FTD 6,7	FXOS 2.9.1 FTD 6,7	Suportado apenas em FTDs
API REST de Dispositivo FTD	FTD 6,7	FXOS 2.9.1 FTD 6,7	Somente API REST de Dispositivo FTD (não GUIs de FDM ou CDO)

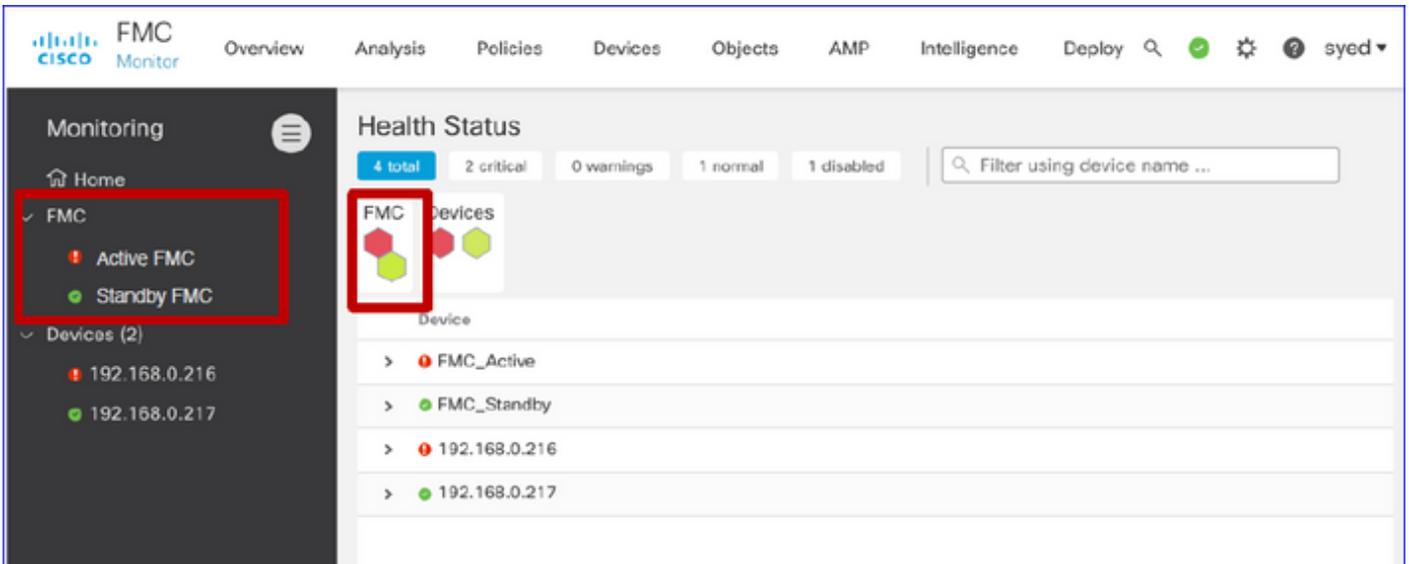
Interoperabilidade

Não existem requisitos específicos de interoperabilidade.

Detalhes do recurso 7.0

Interface do usuário do FMC: suporte autônomo e HA

Navegação da Página de Monitoramento de Integridade



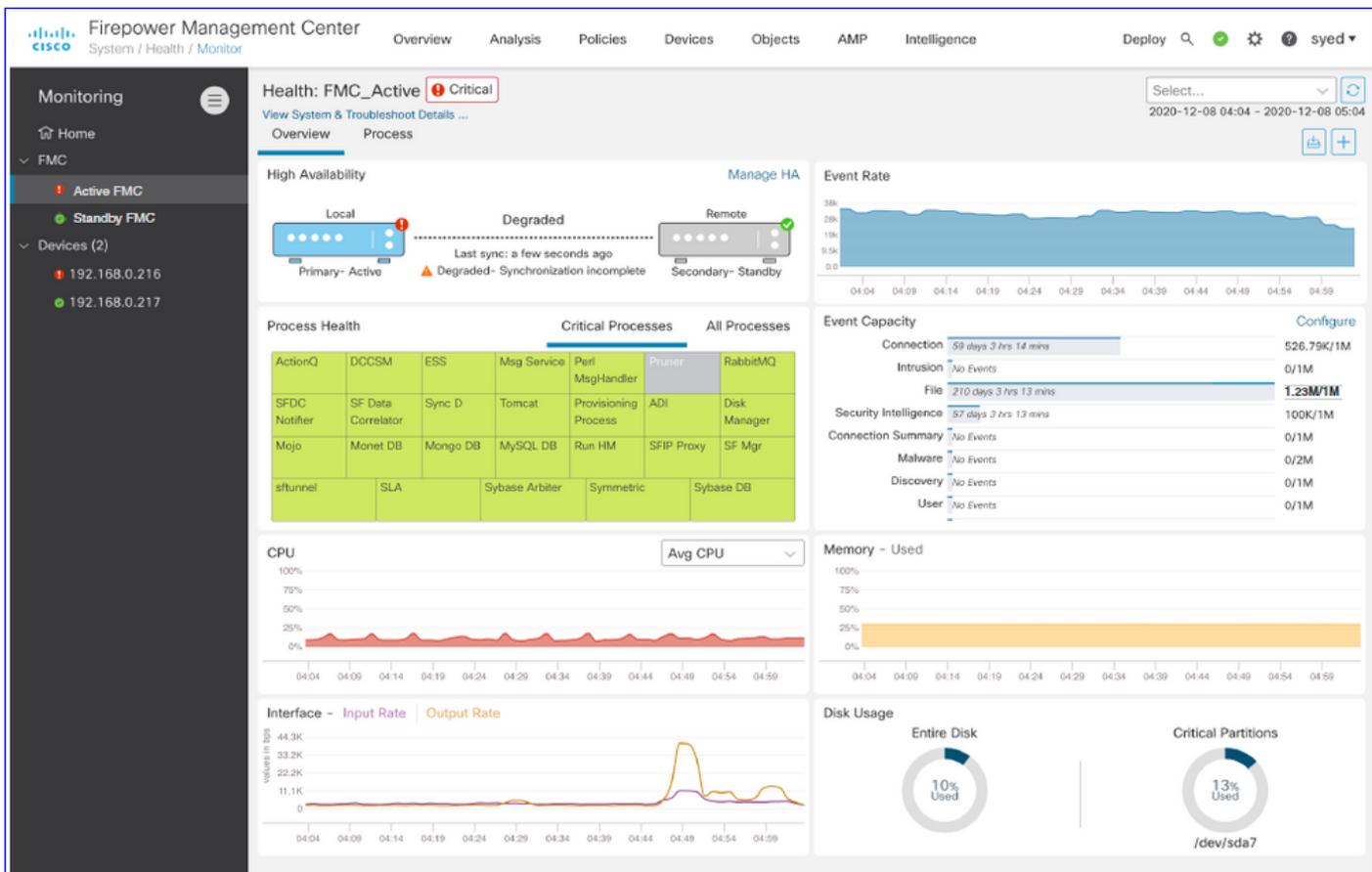
- O CVP autônomo é apresentado como um único nó
- HA FMC mostrado como um par de nós
- Cada CVP é apresentado com o estatuto sanitário

Status de Integridade

- O HA do FMC é mostrado em hexágono duplo.
- Os dispositivos ativos e em standby do FMC também estão listados na tabela de alertas.

Painel do FMC

Painel de Monitoramento de Integridade do FMC no 7.0

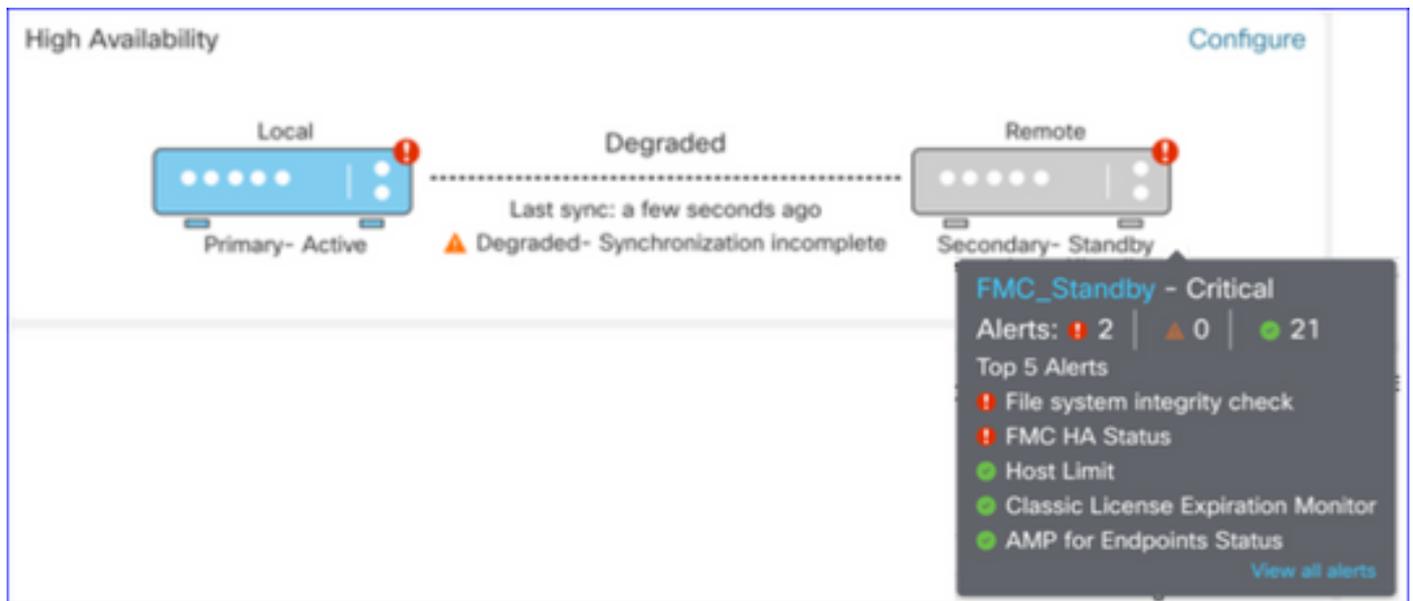


Exibição resumida de:

- Alta Disponibilidade
- Taxa e capacidade de eventos
- Integridade do Processo
- CPU
- Memória
- Interface
- Disco

Este painel está disponível para os CVP ativos e em espera. O usuário pode criar painéis personalizados para monitorar as métricas de sua escolha.

Painel do FMC: painel HA do FMC



O painel HA mostra

- Status de HA atual
- Ativo vs. Em espera
- Hora da última sincronização
- Integridade do dispositivo

Painel do FMC: taxa e capacidade de eventos

Taxa de eventos

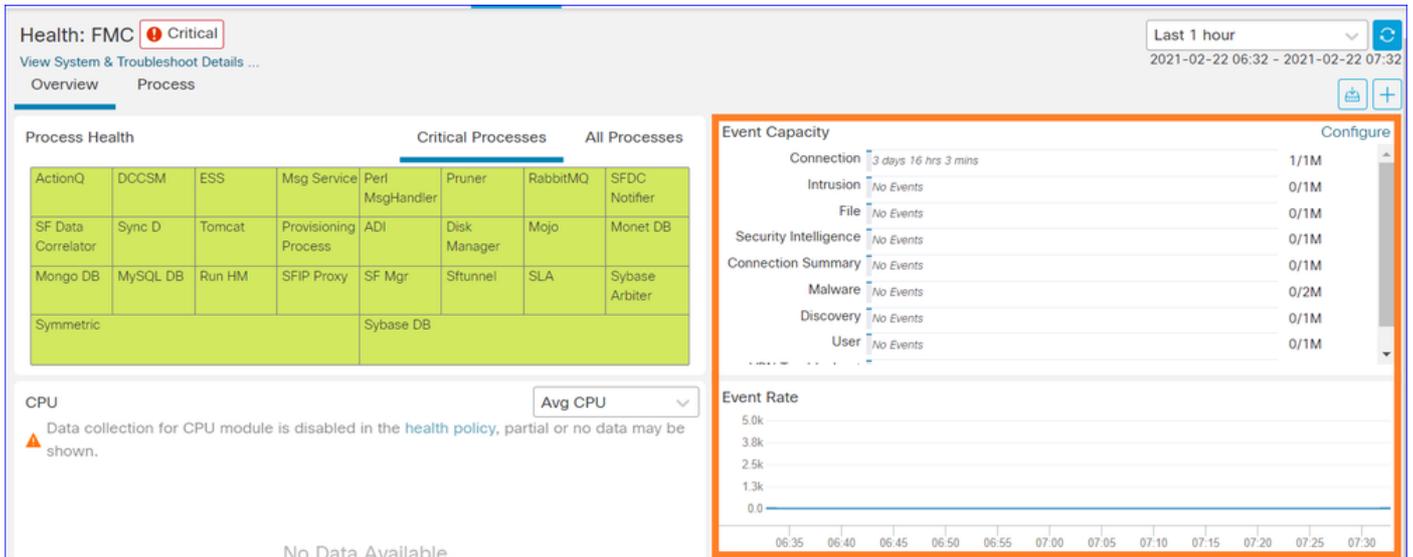
- Taxa máxima de eventos como linha de base
- Taxa global de eventos que o FMC recebe

Capacidade do evento

- Consumo atual por categorias de evento
- Tempo de retenção dos eventos
- Atual vs. Máximo

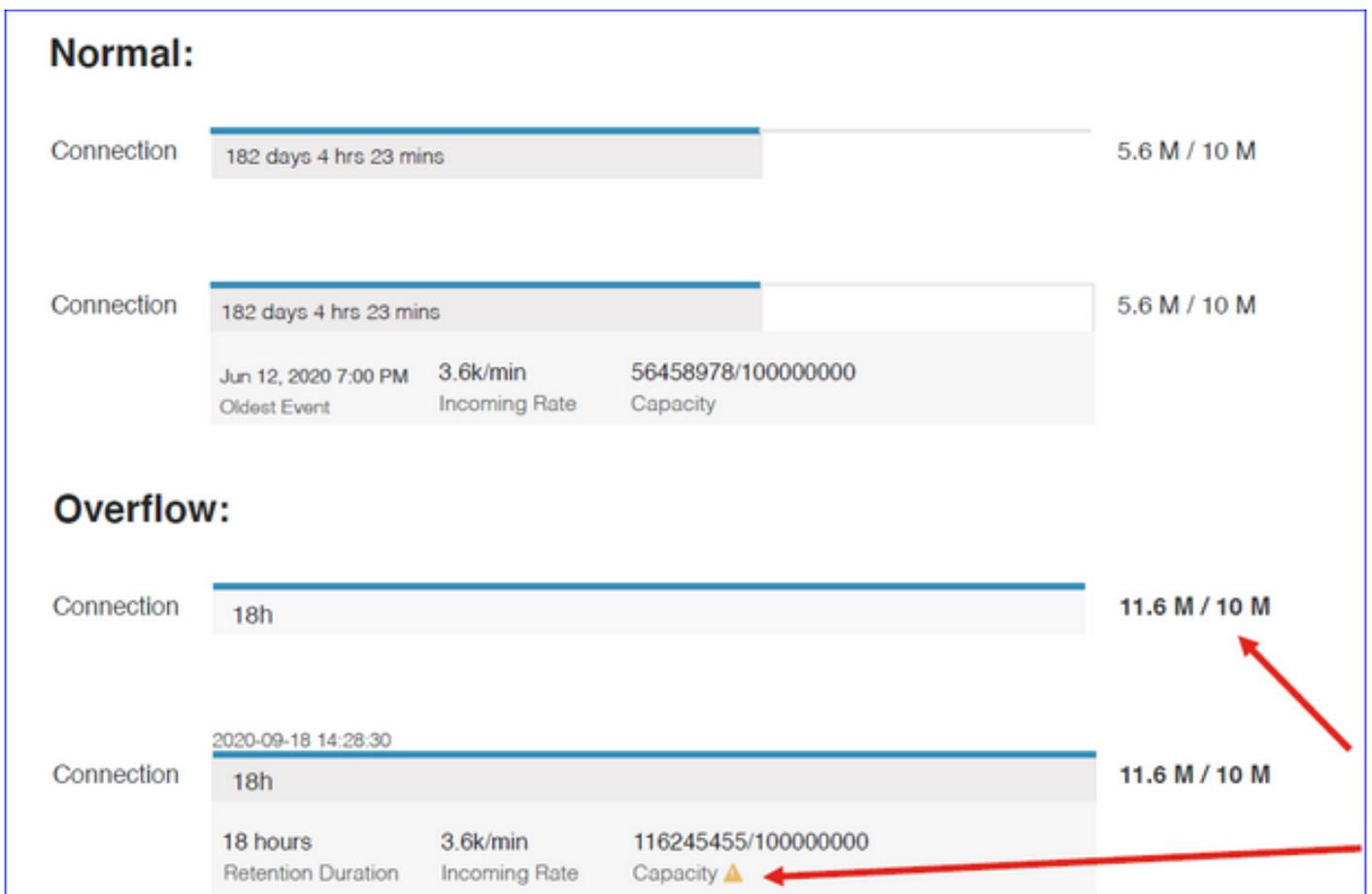
capacidade do evento

- Marcador de estouro de capacidade



Painel do FMC: capacidade de eventos

Estado de Consumo da Capacidade do Evento Normal



Cenário de sobrecarga, quando os eventos são armazenados além da capacidade máxima configurada.

- O texto em negrito indica estouro
- Um ícone de aviso destaca o estouro de capacidade

Painel do FMC: Painel de processo do FMC

O painel Processos críticos mostra

- Processar estado atual
- Contagem de reinicialização de processo

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	

O painel Processo mostra estas métricas para todos os processos 'pmconfig':

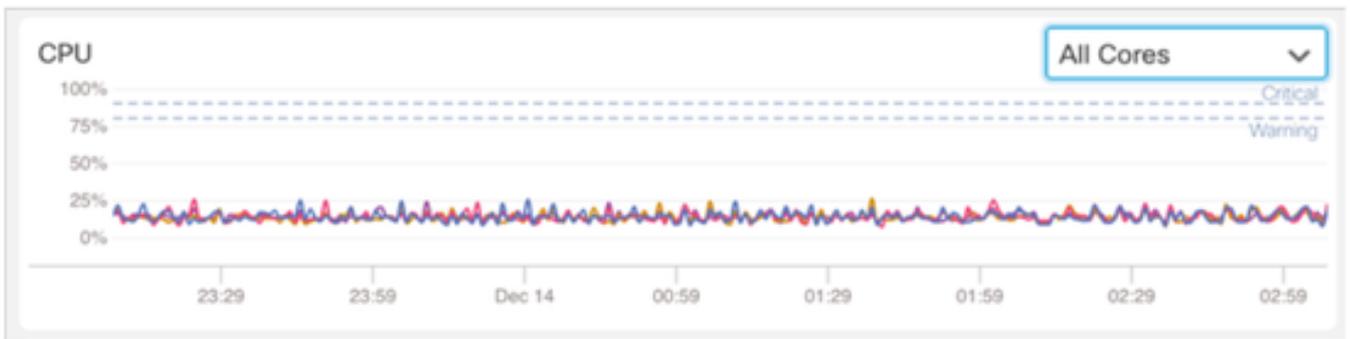
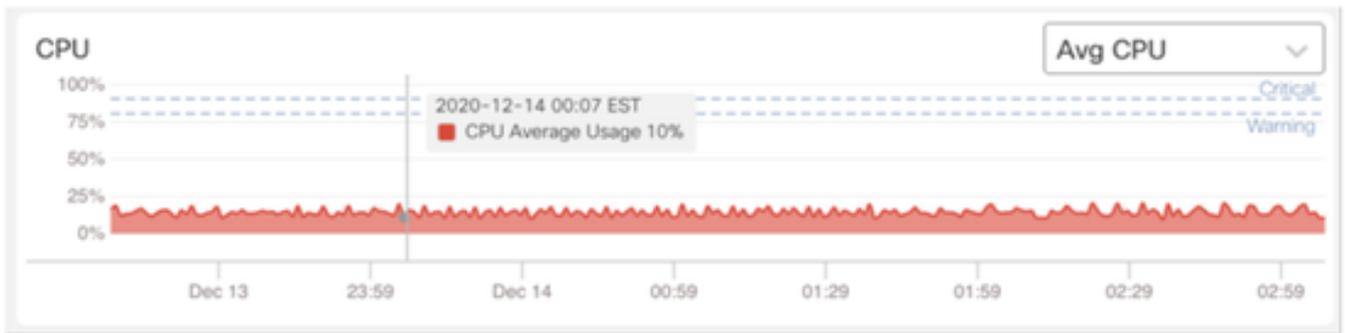
- Estado atual
- Uso da CPU
- Utilização de memória

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	

Painel do FMC: CPU do FMC

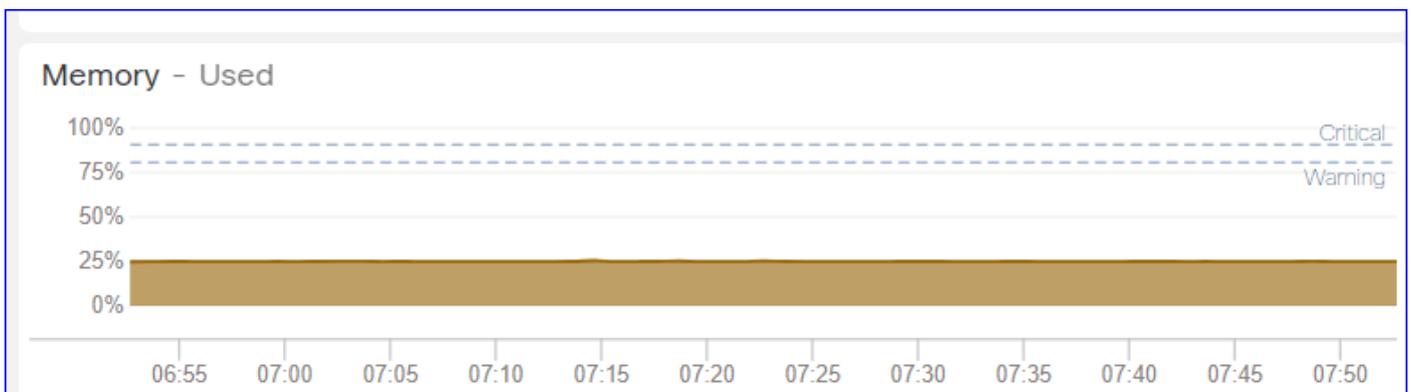
CPU Panel mostra

- Média de CPU (padrão)
- Todos os núcleos

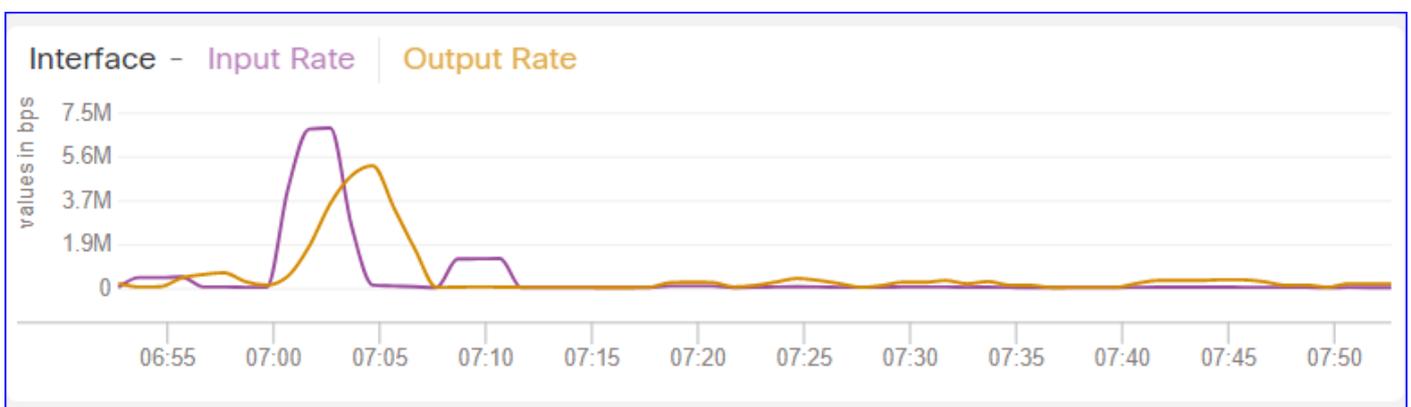


Painel do FMC: outros painéis

O painel Memória mostra o uso geral de memória no FMC

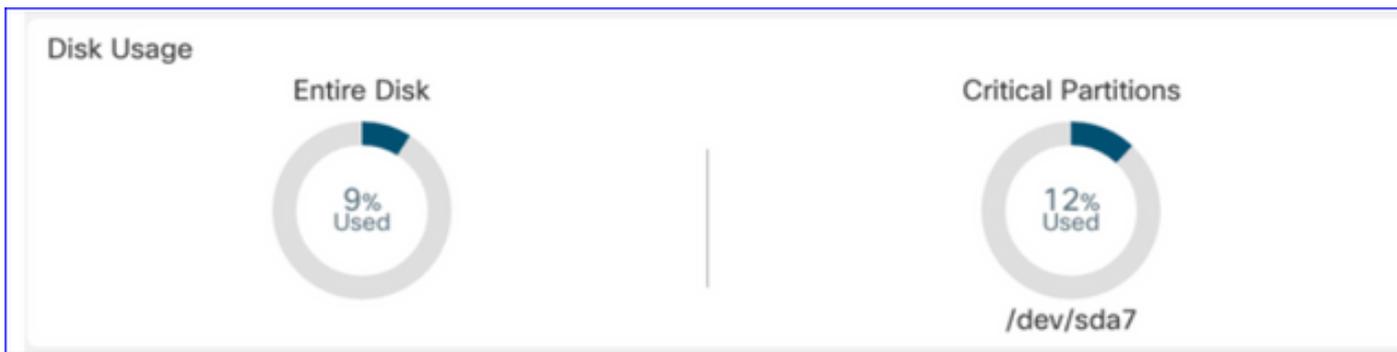


O painel Interface mostra a taxa de entrada/saída média de todas as interfaces



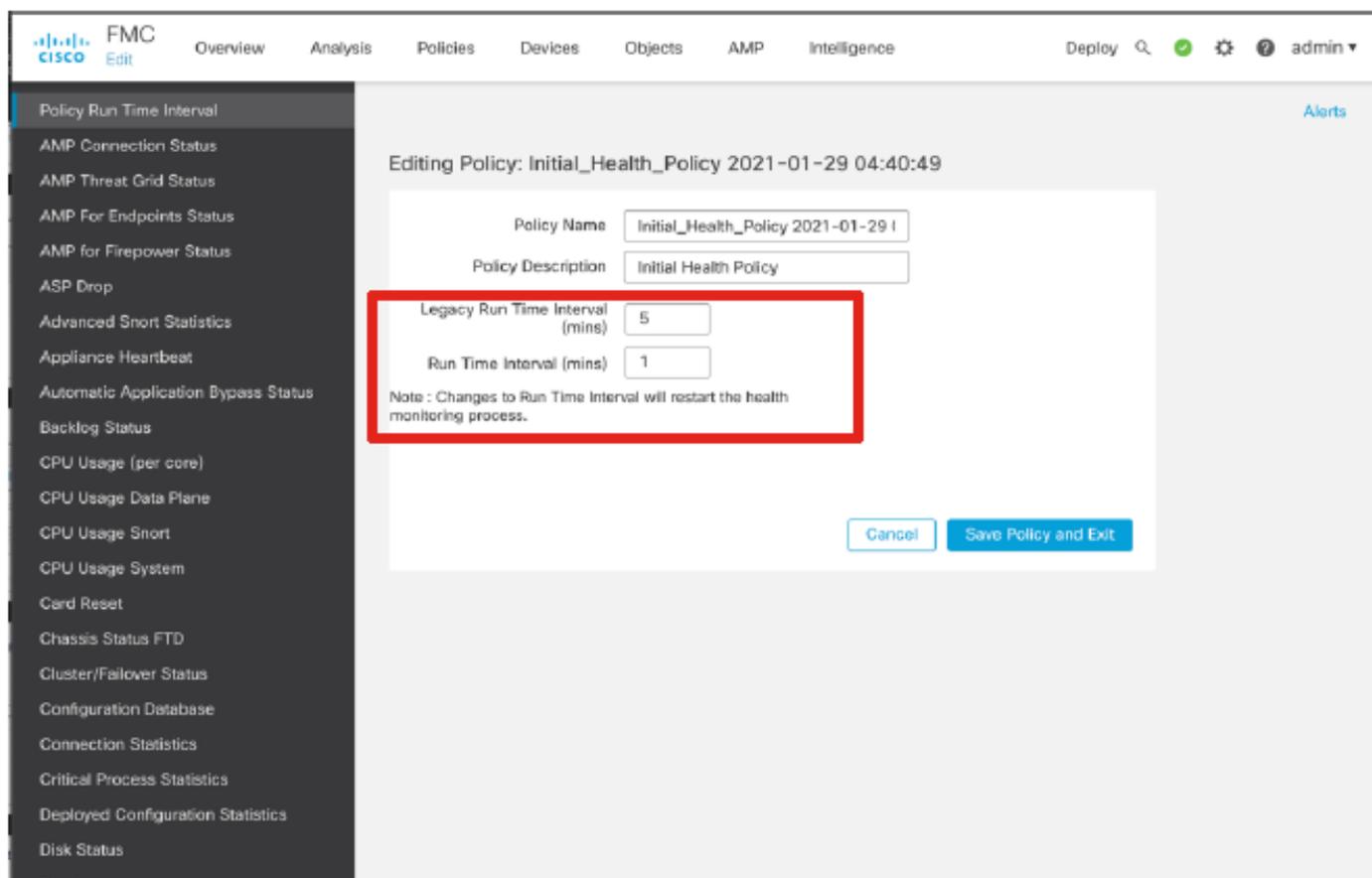
O painel Disco mostra

- Toda a capacidade do disco
- Capacidade crítica de partição onde são armazenados os dados do CVP



Intervalo de tempo de execução

- O intervalo de tempo de execução do módulo de integridade antigo foi renomeado como "Intervalo de tempo de execução herdado"
- O 'Intervalo de tempo de execução' destina-se aos novos módulos de integridade baseados no Telegraf
- Configuração global, afeta todos os dispositivos



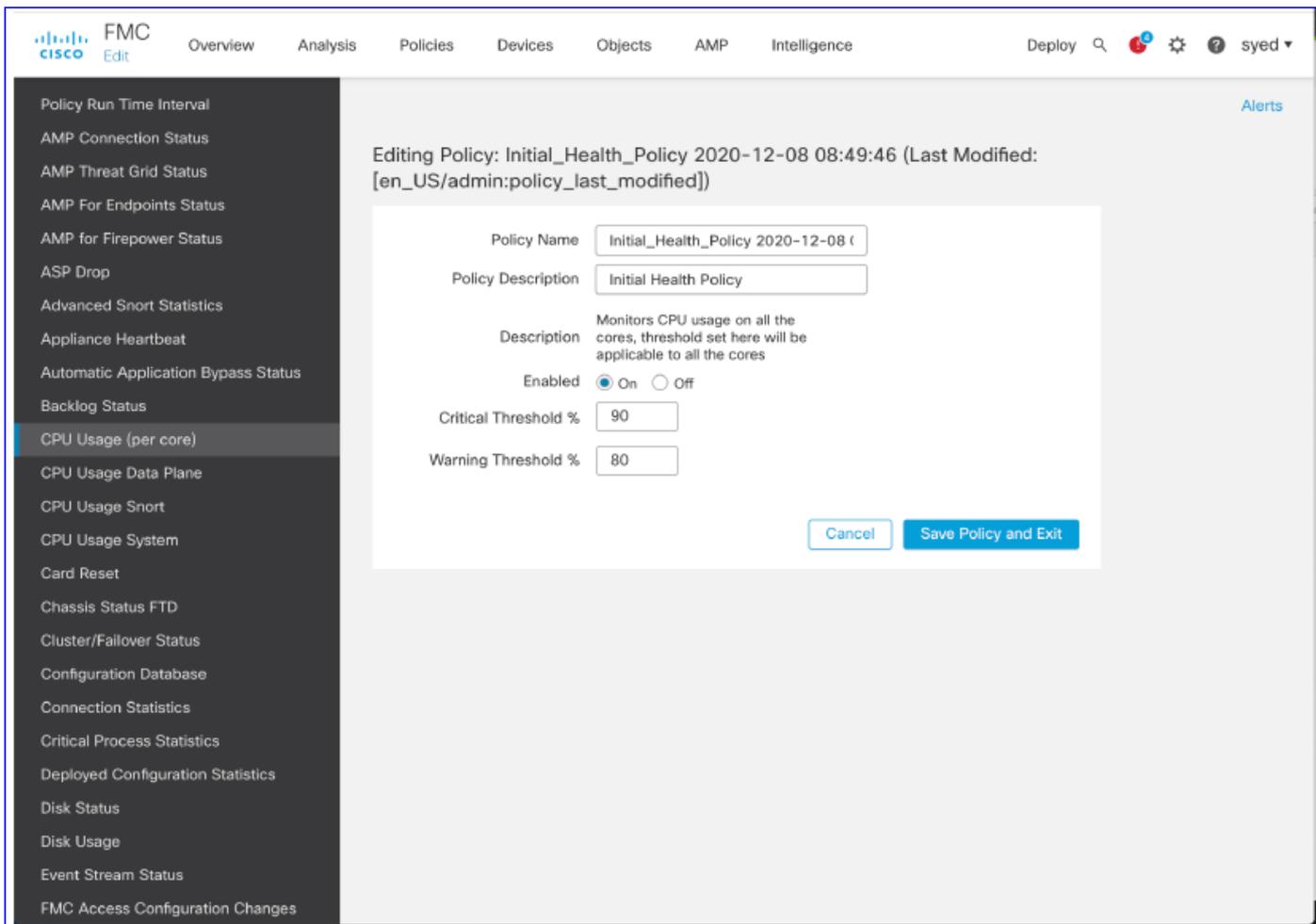
Métricas disponíveis

Métricas Disponíveis para Painéis Personalizados

- Se um usuário quiser criar um painel personalizado, esses slides são um guia para as

métricas disponíveis.

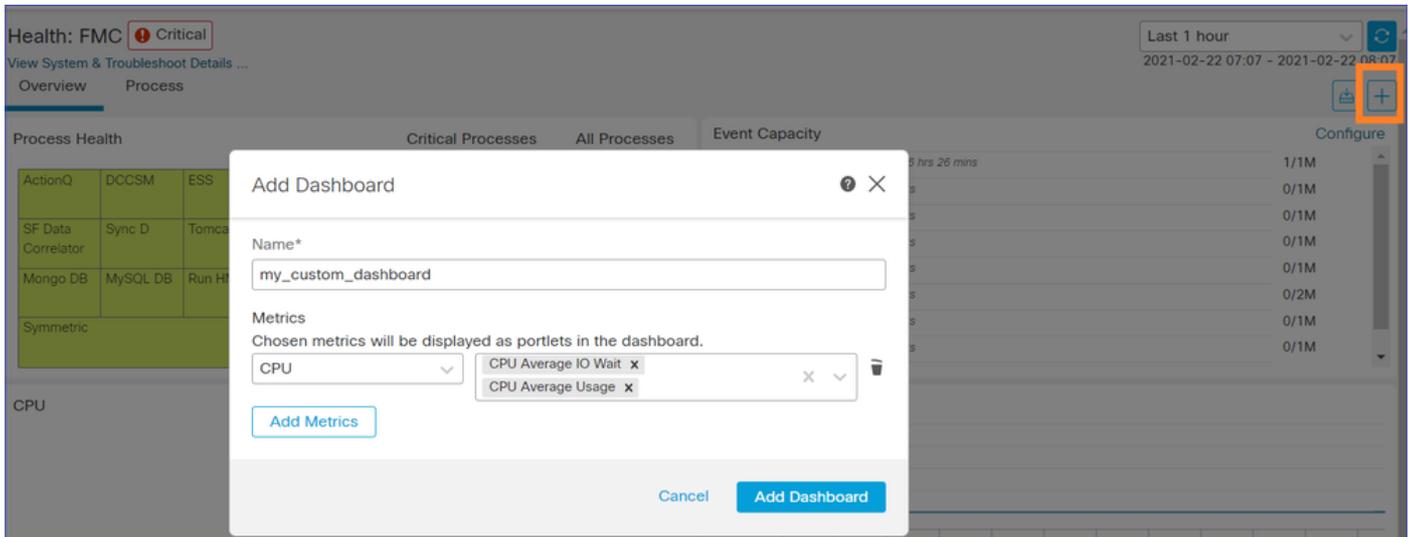
- Algumas métricas devem ser habilitadas na Política de Integridade antes de serem usadas em um Painel de Integridade Personalizado



Interface do usuário do FMC: painel personalizado do FMC

Novas categorias de métricas de monitorização do FMC na versão 7.0

- CPU
- Memória
- Interface
- Disco
- Evento
- Processo
- CoelhoMQ
- Sybase
- MySQL



Interface do usuário do FMC: Métricas do FMC

40 métricas adicionadas em diferentes categorias (disponíveis no painel personalizado). Para ativar as métricas desativadas, ative o módulo de funcionamento correspondente na política de funcionamento associada (Sistema > Funcionamento > Política).

Nome do Grupo de Métricas	Ativado por padrão	Descrição
CPU	No	Monitora a CPU do FMC
Memória	Yes	Monitora a memória FMC
Disco	Yes	Monitora o uso do disco FMC
Interface	Yes	Monitora a interface do FMC
Processo	Yes	Monitoriza os processos do CVP
Evento	Yes	Monitora a taxa de eventos
MySQL	No	Monitora o MySQL
CoelhoMQ	No	Monitora RabbitMQ

Sybase	No	Monitora o Sybase
--------	----	-------------------

FTD: Métricas Introduzidas no FP 7.0

Ativado por default: As métricas são coletadas por default. Para ativar as métricas desativadas, ative o módulo de funcionamento correspondente na política de funcionamento associada (Sistema > Funcionamento > Política).

Nome do Grupo de Métricas	Ativado por padrão	Descrição	Platform
Status do chassi	Yes	Monitora diferentes parâmetros do chassi, como velocidade e temperatura do ventilador.	Aplicável somente a plataformas FPR2100 e FPR1000
Transferência de fluxo	Yes	Monitora estatísticas de descarregamento de fluxo de hardware	Aplicável ao FPR9300 e FPR4100
Quedas de ASP	Yes	Monitora quedas de pacotes laterais de Lina	Todos
Contagens de ocorrências	No	Monitora contagens de ocorrências para Regras de Política de Controle de Acesso	Todos
Status do AMP Threat Grid	Yes	Monitora a conectividade com o AMP ThreatGrid	Todos
Status de conectividade da AMP	No	Monitora a conectividade de nuvem da AMP no FTD	Todos
status do conector SSE	No	Monitora a conectividade de nuvem SSE do FTD	Todos
Status de NTP	No	Monitora os parâmetros de	Todos

		sincronização de relógio NTP em o DTF	
Estatísticas de VPN	Yes	Monitora estatísticas de túnel VPN S2S e RA	Todos
Estatísticas de rota	Yes	Monitora quedas de pacotes laterais de Lina	Todos
Snort 3 perf stats	Yes	Monitora determinadas estatísticas de desempenho do Snort3 (perfstats)	Todos
contadores xTLS	No	Monitora fluxos xTLS/SSL, eficiência de memória e cache	Todos

APIs REST, Syslog, SNMP

Nenhuma nova API REST de dispositivo FMC ou FTD foi introduzida na versão 7.0. As APIs REST atuais suportam novas métricas adicionadas na versão 7.0.

Syslog e SNMP

Syslog

- Nenhuma alteração no syslog do monitor de integridade

SNMP

- Interface de usuário separada para "Monitoramento de integridade de dispositivo SNMP"

Integração de SAL/CTR/produtos de terceiros

- TOI separado para suporte do 'Azure Application Insights'
- Nenhuma alteração específica foi feita para oferecer suporte à integração do 'Health Monitoring' com SAL/CTR/SecureX
- A API REST pode ser utilizada para integração de terceiros

Tecnologia de software

Detalhes do recurso 6.7

Novo monitoramento de integridade de NGFW para integridade e desempenho de FTD

Ajuda os usuários com

- Depuração reativa, como análise da causa raiz do problema depois que ele ocorre
- Ações proativas, como monitorar o uso e os níveis de saturação para identificar possíveis problemas de capacidade e, dessa forma, ajudar os usuários a fazer melhorias ou refatoração da capacidade.

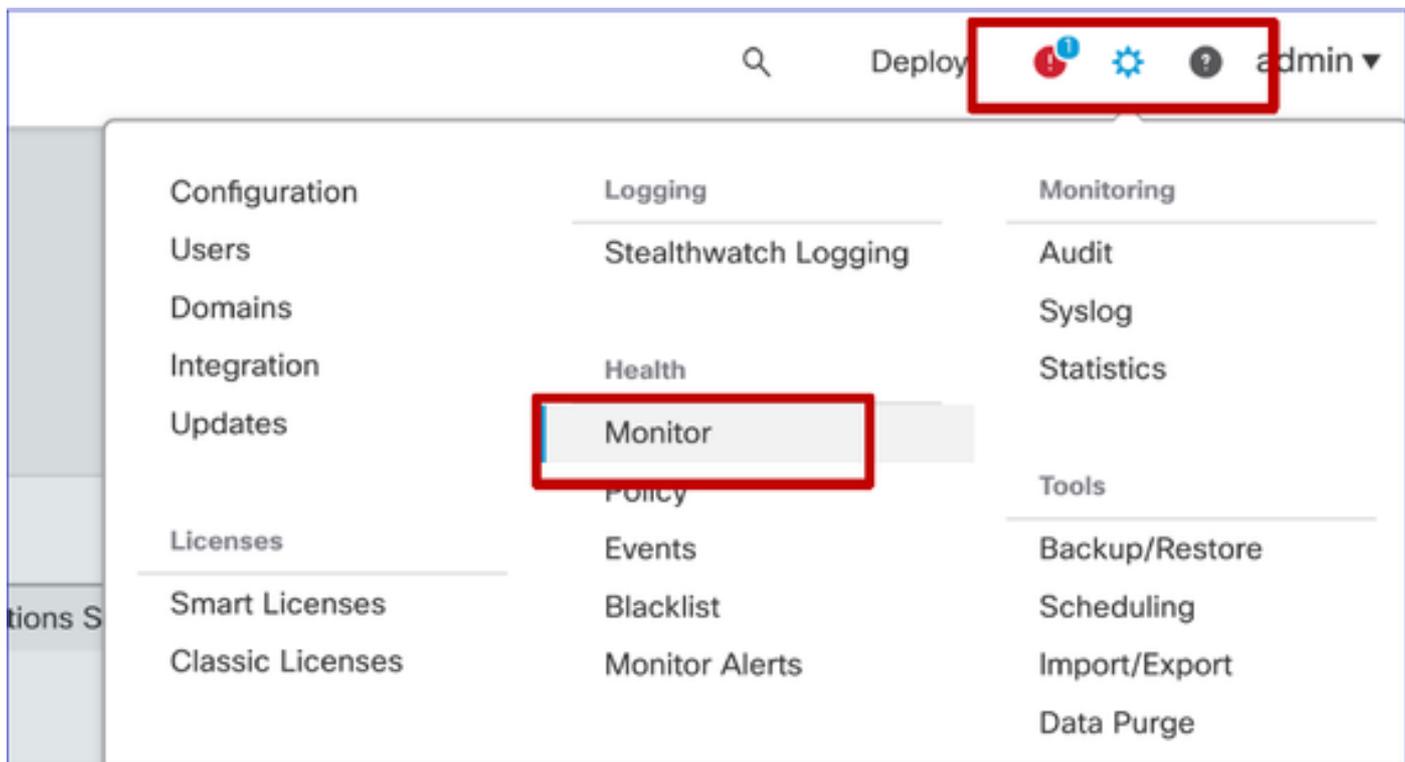
Destaques

- Gráficos de tendências: os gráficos de tendências facilitam muito a detecção de anomalias e determinam uma causa raiz de problemas. Com a inspeção visual, as tendências podem ser localizadas e as correlações podem ser plotadas entre diferentes métricas para encontrar a relação causal entre elas.
- Sobreposições de eventos: as sobreposições de eventos mostram informações importantes, como implantação de configuração e atualizações de SRU em gráficos de tendência para indicar relacionamentos causais.
- Painéis personalizáveis: os usuários podem criar seus próprios painéis para agrupar as métricas que desejam ver juntas em uma página.
- Arquitetura de monitoramento de integridade unificada: ponto único de coleta e exportação para métricas, independentemente do gerente "interessado" nas métricas. As APIs do FTD e o FMC usam dados do mesmo coletor de métricas.
- Extensibilidade das métricas: um dos objetivos da arquitetura da plataforma era poder adicionar facilmente novas métricas. Isso é obtido com o uso de ferramentas de armazenamento e coleta de métricas de código aberto e com painéis personalizáveis.

GUI do FMC

IU do FMC: Navegue até o Status da Integridade

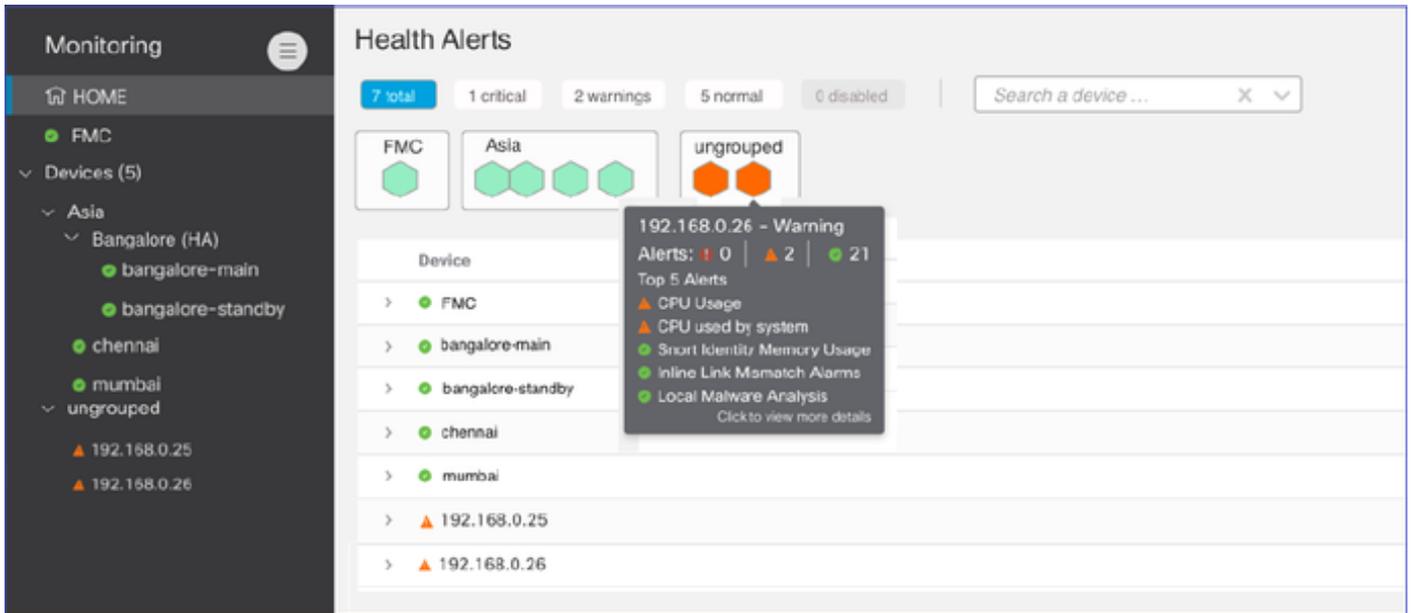
No FMC, clique no ícone System > Health > Monitor para navegar até a página Health Status.



IU do FMC: nova página de status de integridade

A página "Estado de saúde" destina-se a apresentar uma panorâmica da saúde de todos os dispositivos que o CVP gere, incluindo a saúde do CVP.

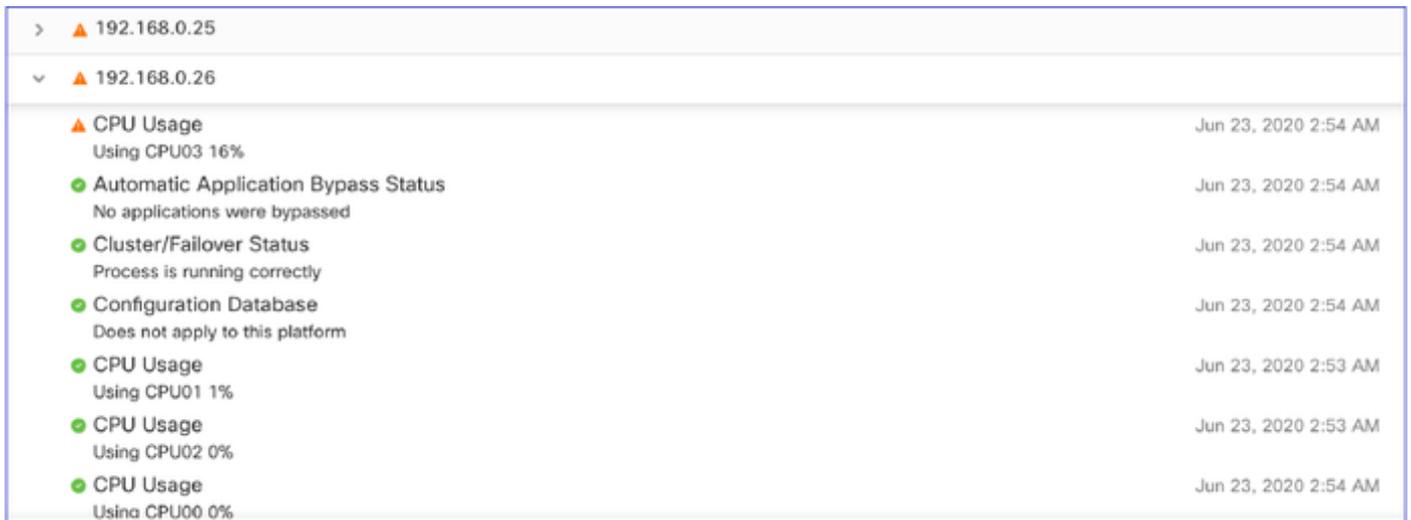
- Os dispositivos são agrupados de acordo com seu grupo/ha/cluster.
- Um ponto à esquerda do dispositivo indica sua integridade
- Verde - sem alarmes
- Laranja - pelo menos uma advertência de saúde
- Vermelho - pelo menos um alarme de integridade crítico
- O resumo da integridade é mostrado ao passar o mouse sobre o hexágono que representa a integridade do dispositivo.
- Os limiares de alerta e de crítica podem ser configurados na política de saúde, da mesma forma que foi feito antes do 6.7.º PQ.



Interface do usuário do FMC: Eventos de Integridade do Dispositivo

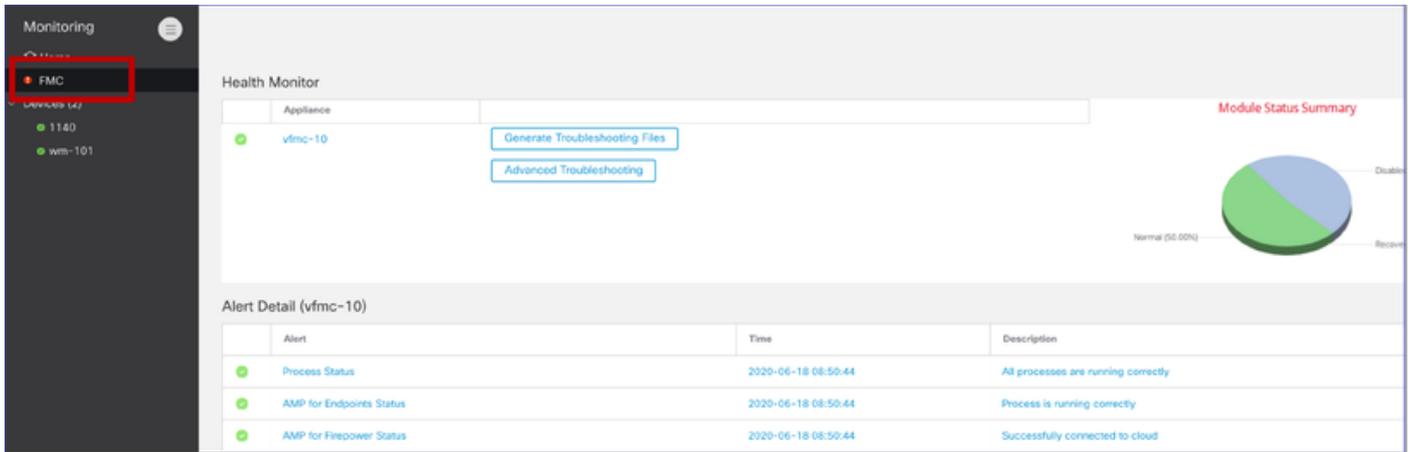
Clique no dispositivo no painel inferior para exibir os eventos de integridade associados ao dispositivo. Os alertas são classificados por seu status de integridade (gravidade).

Página de monitoramento de integridade



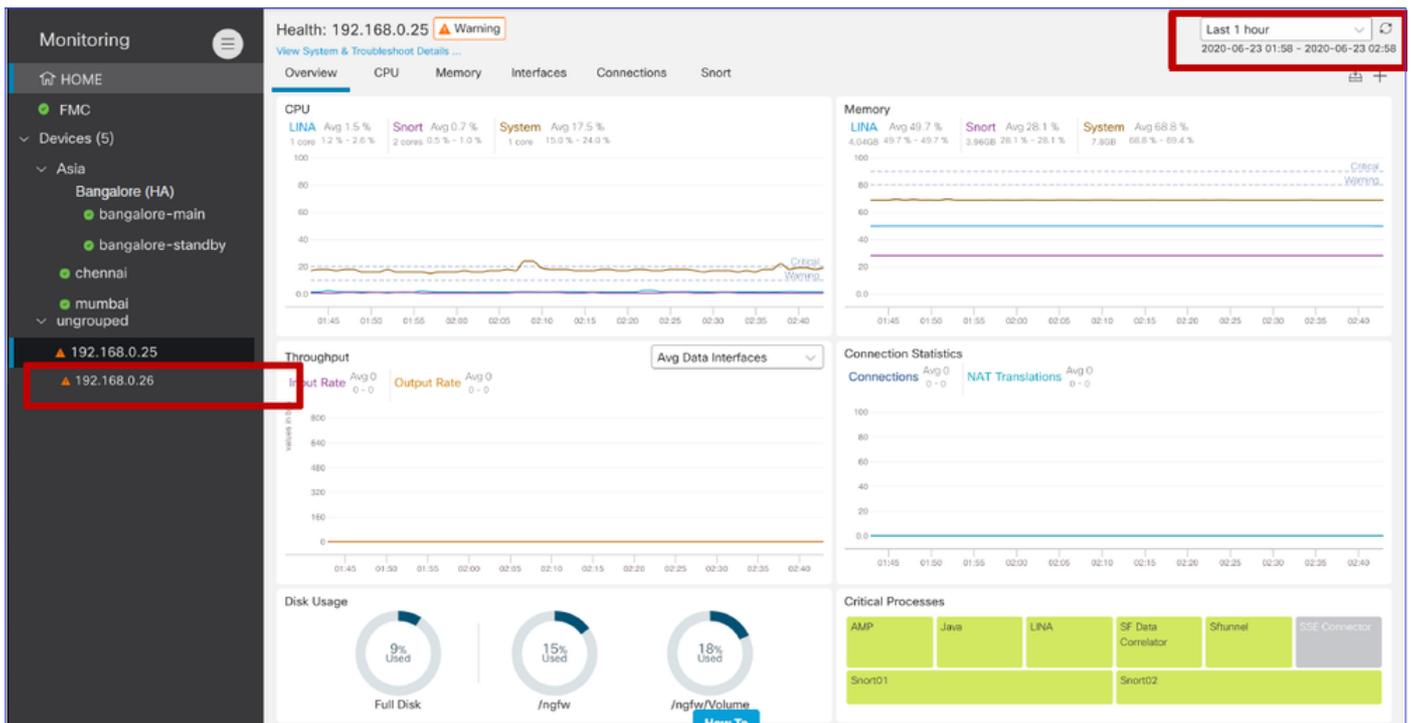
Interface do usuário do FMC: o monitoramento de integridade do FMC está inalterado

A página de saúde do FMC ainda é a página herdada. A nova IU é suportada apenas para FTD com 6.7+



IU do FMC: Novo! Painéis de dispositivos

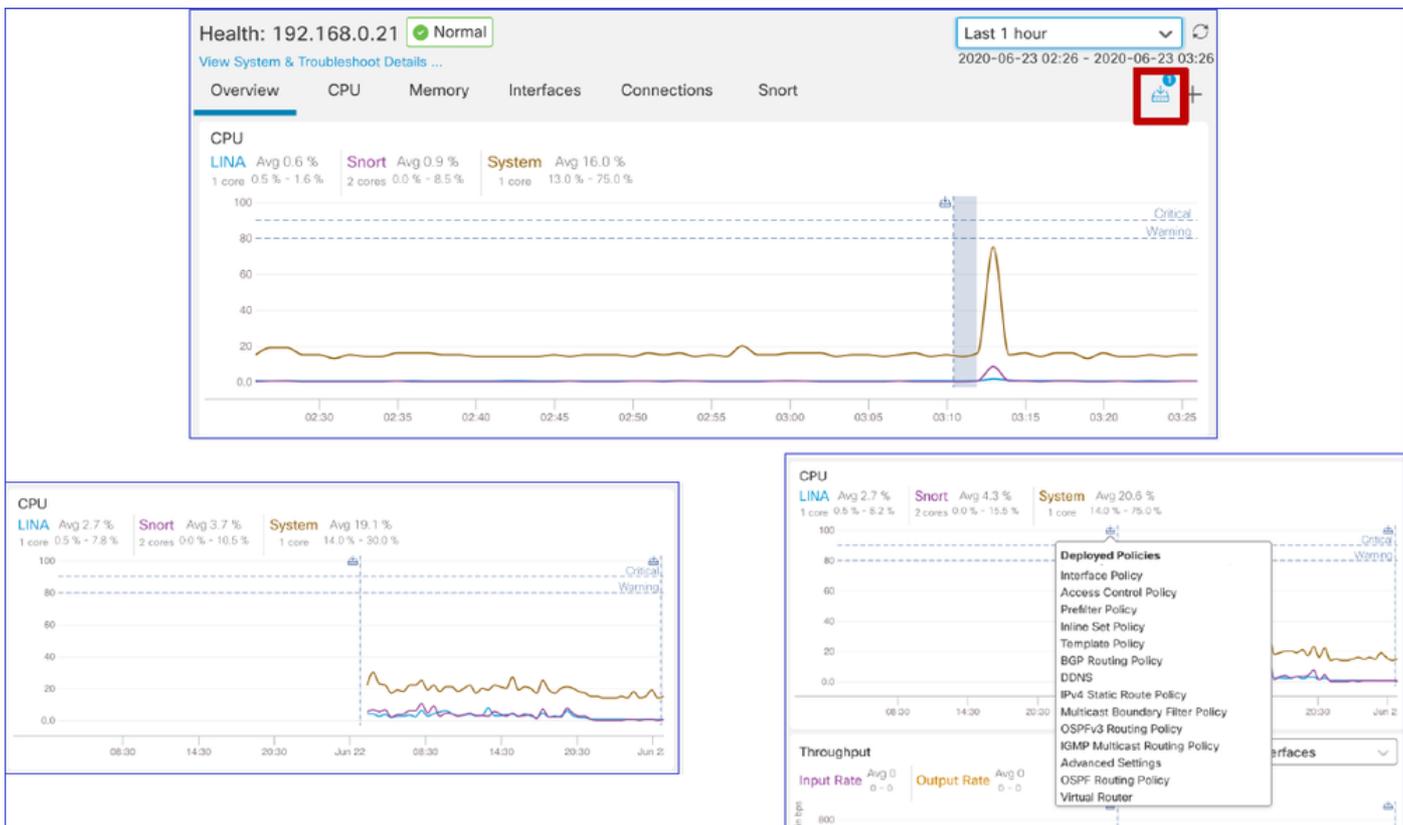
- Clique no nome do dispositivo no painel esquerdo para acessar a página de visão geral da integridade do dispositivo.
- A visão geral da integridade tem todos os gráficos de tendência de métricas de integridade principais.
- Vários intervalos de tempo estão disponíveis (o padrão é a última hora)
- Atualizar automaticamente para recarregar o gráfico



Interface do usuário do FMC: sobreposição de dados de implantação

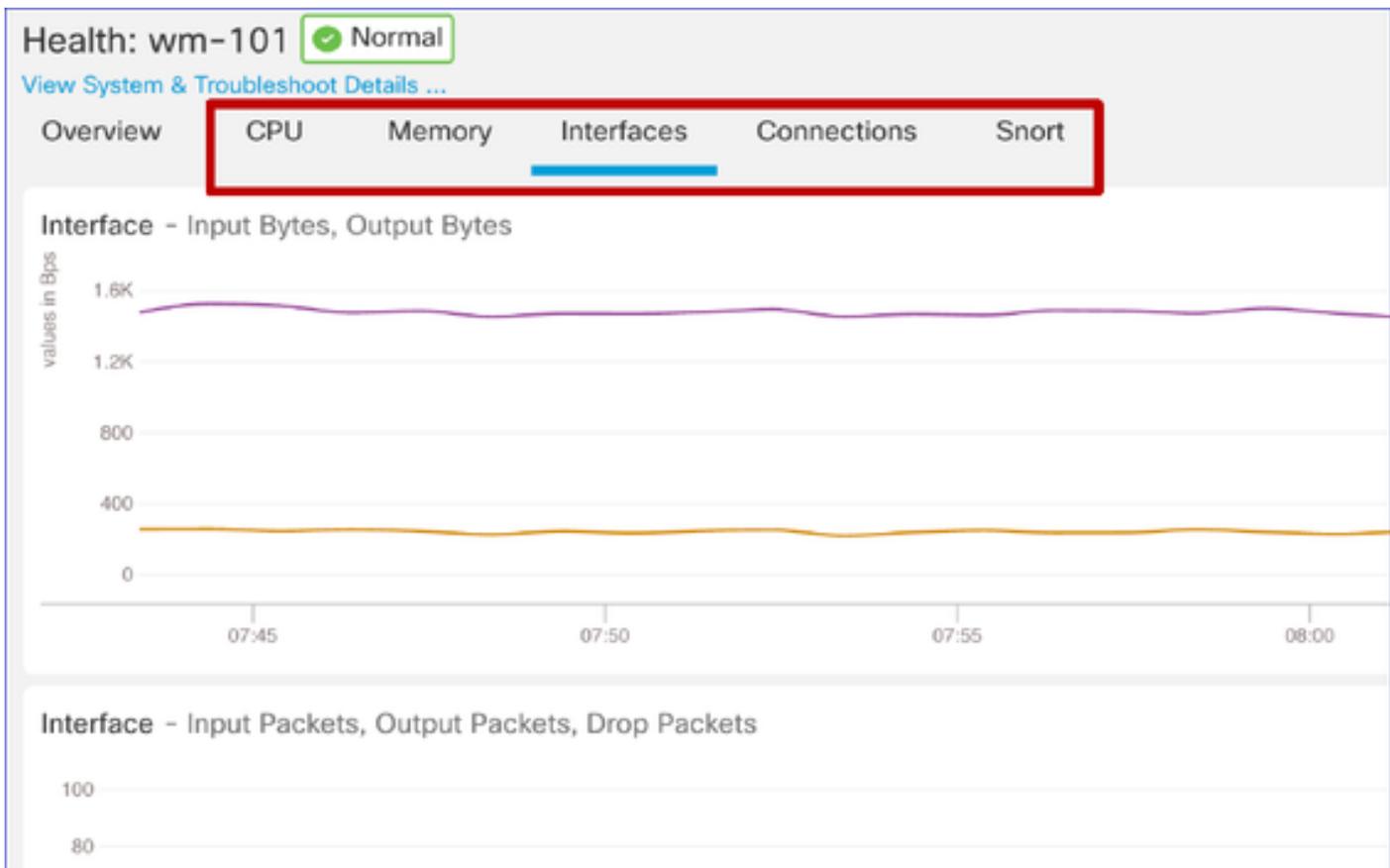
Clique no ícone de implantação para mostrar os detalhes da sobreposição de implantação no gráfico com o intervalo de tempo selecionado

- O ícone indica o número de disponibilizações durante o intervalo de tempo selecionado
- A faixa aparece para indicar a hora de início e término da implantação.
- No caso de várias implantações, várias bandas/linhas são exibidas
- Clique no ícone na parte superior da linha pontilhada para mostrar os detalhes

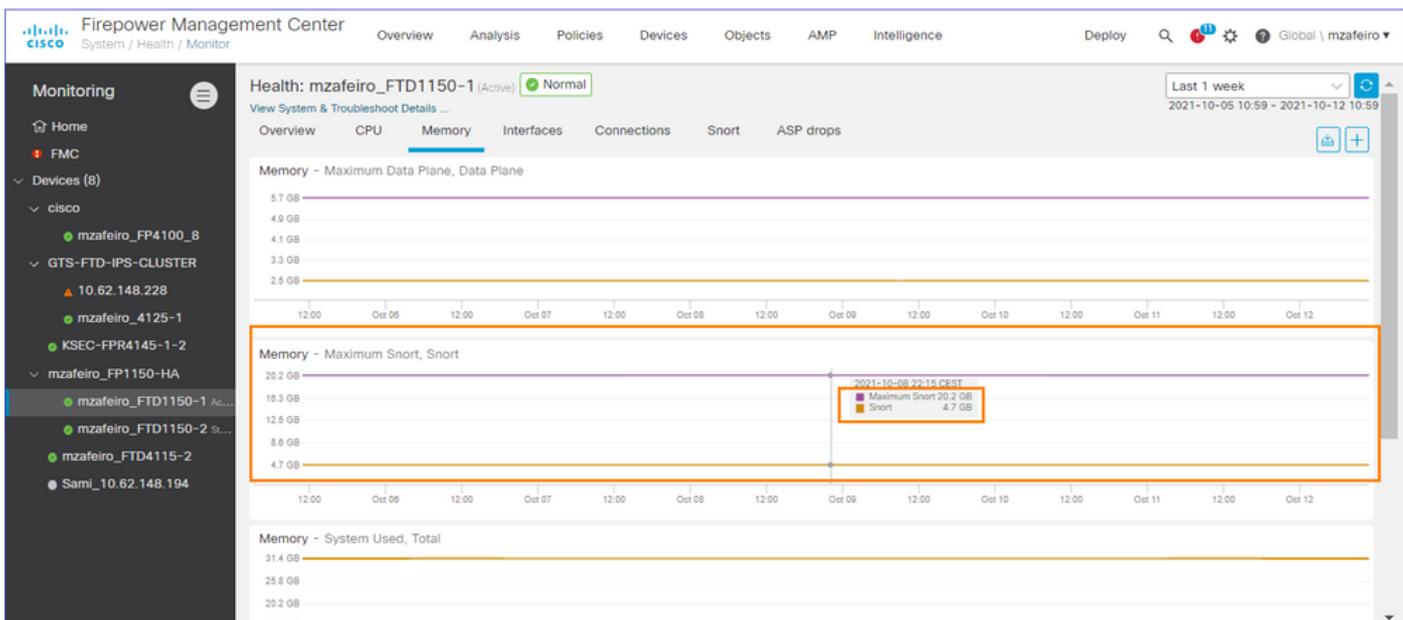


Interface do usuário do FMC: painéis de dispositivos pré-criados

- Há painéis de integridade pré-criados presentes na interface do usuário do FMC.
- Esses painéis pré-criados vêm com métricas relacionadas agrupadas.
- O painel de controle da interface tem um gráfico de tendências para todas as métricas relacionadas à interface, como bytes de entrada/saída, pacotes e tamanho médio de pacote para interfaces diferentes.



Memória Snort FTD - De onde ela se origina?

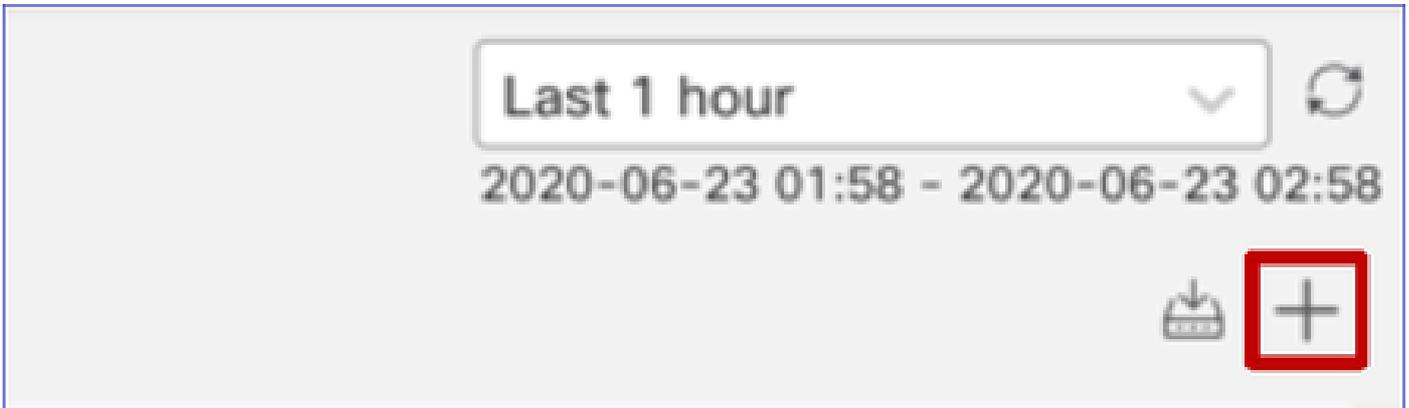


Interface do usuário do FMC: painéis personalizados podem ser criados

Os usuários podem criar seu próprio painel personalizado

- Além dos painéis predefinidos, um usuário também pode criar painéis personalizados.
- Em um painel personalizado, qualquer número de métricas pode ser adicionado.

- Normalmente, um painel personalizado seria criado se as métricas de diferentes grupos de métricas pudessem ser correlacionadas para chegar à causa raiz de um problema.
- Em caso de alta utilização da CPU de Lina, é possível ver a entrada de CPS (Connection Per Second, Conexão por segundo), estatísticas de interface (e assim por diante), o que pode fazer com que a CPU fique alta.



Interface do usuário do FMC: crie um painel personalizado

Diálogo Correlacionar Métricas

- Quando um usuário clica em "+" para criar um painel personalizado, a janela Correlacionar Métricas é aberta.
- Um usuário pode adicionar diferentes métricas que deseja monitorar em conjunto.

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 ▼	Snort ✕	✕ ▼	
Interface ▼	Input Packets ✕	✕ ▼	
Deployed Configuration ▼	Number of rules ✕	✕ ▼	
Deployed Configuration ▼	Number of ACEs ✕	✕ ▼	

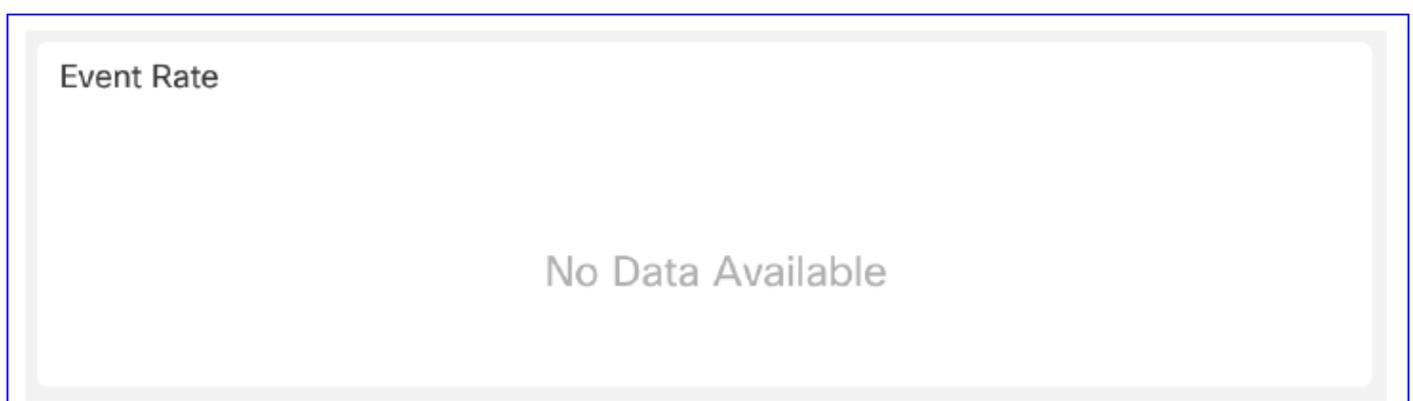
[Add Metrics](#)

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

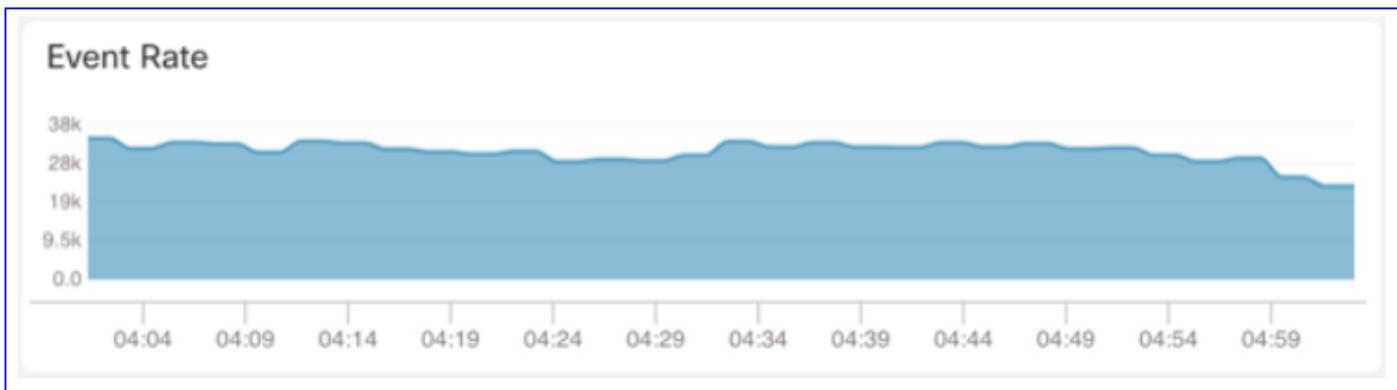
Coletando dados de (dispositivo) - GUI

Dados para um intervalo de tempo exibido na GUI

Quando o Health Monitor não tem dados para o intervalo de tempo selecionado, a GUI mostra 'No Data Available' no painel:



No caso dos dados disponíveis, o gráfico aparece da seguinte forma:



Usar as guias Console do navegador e Rede

Log do console do navegador e log de chamadas da rede

- Neste exemplo, o console do desenvolvedor do navegador Chrome é mostrado
- Em caso de erro, os detalhes da exceção são mostrados no registro do console

The image shows a screenshot of the Firepower Management Center (FMC) dashboard and the Chrome DevTools console. The FMC dashboard displays various monitoring metrics for a system, including CPU usage (Data Plane, Snort, System), Memory usage (Data Plane, Snort, System), Throughput (Input Rate, Output Rate), and Connection Statistics (Connections, NAT Translations). The Chrome DevTools console shows a stack trace for an error, indicating a runtime error in the application code.

Exemplo de Log do Console do Navegador

Console Tab

Exception details



Referências

[Monitoramento de integridade do FMC - 6.7](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.