# Atualizar FP - Monitoramento de integridade do dispositivo

## Contents

<u>Introdução</u>
Informações de fundo
<u>Visão geral do recurso</u>
<u>Detalhes do recurso 7.0</u>
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.

	Q Deploy	💕 🌣 🔕 admin 🔻
Configuration	Logging	Monitoring
Users	Stealthwatch Logging	Audit
Domains		Syslog
Integration	Health	Statistics
Updates	Monitor	
	Policy	Tools
Licenses	Events	Backup/Restore
Smart Licenses	Blacklist	Scheduling
Classic Licenses	Monitor Alerts	Import/Export
		Data Purge
l		

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

CISCO FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	0	۵	<b>Ø</b> s	yed •
Monitoring		Health S 4 total FMC pev Devic > • FM > • FM > • FM > • 19 > • 19	Ac_Active 2.168.0.217	0 warnings	1 normal	1 disabled	C. Filter us	ing device	: nam	C			)

- 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

Firepower Manage System / Health / Monitor	ement Cer	nter ov	erview	Analysis	Policies	Devices	Objects	AMP Intelligence	Deploy 🔍 🥝 🌣 🕼	syed •
Monitoring () 얇 Home	Health: F View System Overview	MC_Active & Troubleshoot Process	e \rm Critica Details	1					Select 2020-12-08 04:04 - 2020-1:	2-08 05:04
	High Availa	ability					Manage HA	Event Rate		
<ul> <li>Standby FMC</li> <li>Devices (2)</li> <li>192.168.0.216</li> <li>192.158.0.217</li> </ul>	Primar	ocal y- Active	Last s A Degraded	Degraded ync: a few seco I- Synchronizat	onds ago tion incomplete	e Second	ary- Standby	38k 20k 10k 95k 020 04:04 04:09 04:14 04:19 04:24 0	429 0434 0439 0444 0449 0454	04:59
@ 152.100.0.217	Process H	ealth		(	Critical Proce	esses A	II Processes	Event Capacity	0	onfigure
	ActionQ	DCCSM	ESS	Msg Service	Peri MsgHandler	Pruner	RabbitMQ	Connection 59 days 3 brs 14 mins Intrusion No Events	526 0/11	.79K/1M M
	SFDC Notifier	SF Data Correlator	Sync D	Tomcat	Provisioning Process	ADI	Disk Manager	Security Intelligence 57 days 3 hrs 13 mins	100	K/1M
	Mojo M	Monet DB	Mongo DB MySQL		DB Run HM	SFIP Proxy	SF Mgr	Connection Summary No Events Malware No Events	0/11	0/1M 0/2M
	sftunnel	SLA	5	Sybase Arbiter	Symmetric	c Syb	ase DB	Discovery No Events	0/11	M
	CPU 100% 75% 50% 04:04 04:04 Interface - 86 44.3K	04:09 04:14 Input Rate	04:19 04:24 Output Ra	0429 043- te	4 04:39 04:	Avg CP	U ~	Memory - Used 100% 75% 50% 25% 0% 0% 0% 0% 0% 0% 0% 0% 0% 0	129 0134 0139 0144 0149 0154 Critical Partitions	04.59
	22.2K 11.1K 0 04:04	04:09 04:14	04:19 04:24	04:29 04:3	4 04:39 04:	54 04:10	D4:54 04:59	10%	13% Used /dev/sda7	

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

High Availability		Configure
Local Primary- Activ	e Degraded Last sync: a few seconds ago ▲ Degraded- Synchronization incomplete	Remote         Secondary- Standby         FMC_Standby - Critical         Alerts:       2       0       0 21         Top 5 Alerts         File system integrity check         FMC HA Status         Host Limit         Classic License Expiration Monitor         AMP for Endpoints Status         View all alerts

#### 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

Health: Fl View System 8 Overview	MC OCrit Troubleshoo Process	ical t Details						Last 1 2021-02	hour -22 06:32 - 2021-02-22 07	07:32
Process He	alth	ECC	Mag Sapring	Crit	tical Proce	sses A	II Processes	Event Capacity Connection 3 days 16 hrs 3 mins	Configur 1/1M	Jre ^
SF Data	Sync D	Tomcat	Provisioning	MsgHandler ADI	Disk	Mojo	Notifier Monet DB	Intrusion No Events File No Events Security Intelligence No Events	0/1M 0/1M 0/1M	
Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Sftunnel	SLA	Sybase Arbiter	Connection Summary No Events Malware No Events Discourse	0/1M 0/2M	
Symmetric	Symmetric Sybase DB							User No Events	0/1M 0/1M	•
CPU Data col shown.	lection for C	PU module	e is disabled No Data	in the healt	th policy, p	Avg CP	U v	Event Rate 5 0k 3.8k 2.5k 1.3k 0.0 06:35 06:40 06:45 06:55 07:00 07:05 07:10 07	15 07:20 07:25 07:30	0

Painel do FMC: capacidade de eventos

Estado de Consumo da Capacidade do Evento Normal

Normal:				
Connection	182 days 4 hrs 23 m	ins		5.6 M / 10 M
Connection	182 days 4 hrs 23 mi	ns		5.6 M / 10 M
	Jun 12, 2020 7:00 PM Oldest Event	3.6k/min Incoming Rate	56458978/100000000 Capacity	
Overflow	w:			
Connection	18h			11.6 M / 10 M
	2020-09-18 14:28:30			_ \
Connection	18h			11.6 M / 10 M
	18 hours Retention Duration	3.6k/min Incoming Rate	116245455/10000000 Capacity 🛆 🔫	

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							ical Proc	esses A	All Processes		
ActionQ	DCCSM	ESS	Msg Service	Perl MsgHandler	Pruner		RabbitMQ	SFDC Notifier	SF Data Correlator		
Sync D	Tomcat	Provisioning Process	ADI	Disk Mojo Manager		Monet DB		Mongo DB	MySQL DE		
Run HM	SFIP Prox	y SF Mgr	Sftunne	I SLA		Syba Arbite	se er	Symmetric	Sybase DB		

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

- Estado atual
- Uso da CPU
- Utilização de memória

Process Health		Critica	al Processes	All Processes
Process status at: Dec 14, 2020 3:2	2 AM			
Process *	Status	CPU (%)	Mem U	sed
ActionQ	Running	0	66	5.23KB
CSD App	Waiting	0		0
CSM Event Server	Running	0.6	18	32.1KB
CloudAgent	Running	0.9	12	2.03KB
DCCSM	Running	0	104	.49KB
ESS	Running	0.1	448	3.26KB
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

Disk Usage Entire Disk	Critical Partitions
9%	12%
Used	Used

#### 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

CISCO Edit Overview Analy	sis Policies	Devices	Objects	AMP	Intelligence	Deplo	/ Q	0	¢	0	admin 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Poli	cy: Initial_H	ealth_Polic	y 2021-	01-29 04:40:4	19					Alerts
AMP For Endpoints Status AMP for Firepower Status ASP Drop	Po	Policy Name icy Description	Initial_Hea	alth_Policy Ith Policy	2021-01-291						
Advanced Snort Statistics Appliance Heartbeat	Legacy Ru Run Time	n Time Interva (mins) Interval (mins)	5								
Automatic Application Bypass Status Backlog Status CPU Usage (per core)	Note : Changes monitoring proc	; to Run Time Int cess.	ierval will restar	t the health							
CPU Usage Data Plane CPU Usage Snort CPU Usage System					Gancel	Save Policy and Exi					
Card Reset Chassis Status FTD Cluster/Failover Status											
Configuration Database Connection Statistics											
Critical Process Statistics Deployed Configuration Statistics Disk Status											

#### 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

CISCO Edit Overview Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	¢	۵	0	syed •
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Polic [en_US/adn	:y: Initial_H nin:policy_l	ealth_Polic ast_modifie	y 2020-1 ed])	12-08 08:49:46	6 (Last Modified:					Alerts
AMP For Endpoints Status AMP for Firepower Status ASP Drop	Poli	Policy Name cy Description	Initial_Hea	alth_Policy	2020-12-08 (						
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status		Description	Monitors CPI cores, thresh applicable to	U usage on old set here all the core	all the ⊵ will be s						
Backlog Status CPU Usage (per core)	Critica	al Threshold %	90	л							
CPU Usage Data Plane	Warnin	g Threshold %	80								
CPU Usage System Card Reset					Cancel	Save Policy and Exit					
Chassis Status FTD Cluster/Failover Status											
Configuration Database											
Critical Process Statistics											
Deployed Configuration Statistics											
Disk Usage Event Stream Status FMC Access Configuration Changes											

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

Health: FN View System 8 Overview	Crit Troubleshoo Process	ical t Details	S	Last 1 hour C 2021-02-22 07:07 - 2021-02-22 08:07
Process Hea	alth		Critical Processes All Processes Event Capacity	Configure
ActionQ	DCCSM	ESS	Add Dashboard	1/1M ^
SF Data Correlator	Sync D	Tomca	Name*	0/1M 0/1M
Mongo DB	MySQL DB	Run H	my_custom_dashboard 5	0/1M 0/2M
Symmetric			Chosen metrics will be displayed as portlets in the dashboard.	0/1M
CPU			Add Metrics	
			Cancel Add Dashboard	

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
СРU	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.

Monitoring 😑	Health Alerts
ល់ HOME	7 total 1 critical 2 warnings 5 normal 0 disabled Search a device X V
<ul> <li>FMC</li> <li>Devices (5)</li> <li>Asia</li> </ul>	FMC Asia ungrouped 192.168.0.26 - Warning
<ul> <li>Bangalore (HA)</li> <li>bangalore-main</li> </ul>	Device Alerts: 9 0 2 0 21
bangalore-standby	FMC     CPU Usage     CPU usad by system
chennai	bangalore-main     Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalore-standby     bundle Link Mismatch Alarms     Local Malware Analysis
A 192.168.0.25	> Clickto view more distails
A 192.168.0.26	> 🔷 mumbai
	> 192.168.0.25
	> 192.168.0.26

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

>	A 192.168.0.25	
~	A 192.168.0.26	
	▲ CPU Usage Using CPU03 16%	Jun 23, 2020 2:54 AM
	<ul> <li>Automatic Application Bypass Status</li> <li>No applications were bypassed</li> </ul>	Jun 23, 2020 2:54 AM
	<ul> <li>Cluster/Failover Status</li> <li>Process is running correctly</li> </ul>	Jun 23, 2020 2:54 AM
	<ul> <li>Configuration Database</li> <li>Does not apply to this platform</li> </ul>	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

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+

Monitoring						
FMC	Health	Monitor				
· Devices (4)		Appliance				Module Status Summary
0 1140	•	vime-10	Generate Troubleshooting Files			
			Advanced Troubleshooting		Normal (56.0	Coulde Could
	Alert D	etail (vfmc-10)				
		Alert		Time	Description	
	•	Process Status		2020-06-18 08:50:44	All processes are running correctly	
	0	AMP for Endpoints Status		2020-06-18 08:50:44	Process is running correctly	
	0	AMP for Firepower Status		2020-06-18 08:50:44	Successfully connected to cloud	

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

Monitoring 📄	Health: 192.168.0.25 & Warning View System & Troubleshoot Details Overview CPU Memory Interfaces Connections Snort	Last 1 hour シーク 2020-06-23 01:58 - 2020-06-23 02:58 さーナ
<ul> <li>FMC</li> <li>Devices (5)</li> <li>Asia</li> <li>Bangalore (HA)</li> <li>bangalore-main</li> <li>bangalore-standby</li> <li>chennai</li> </ul>	CPU         Snort         Avg 0.7 %         System         Avg 17.5 %         I come 12 % - 2.6 %         2 come 0.5 % - 1.0 %         I come 15.0 % - 24.0 %         I come 15.0 % - 24.0 %         I come 0.5 % - 1.0 %         I come 0.5 %         I com	Memory         Sport         Avg 28.1 %         System         Avg 68.8 %         2,000         49.7 %         3.9908 28.1 % - 28.1 %         System         Avg 68.8 %         2,000         68.5 %         2.000         68.5 %         2.000         68.5 %         2.000         69.6 %         2.000         69.6 %         Vertrain         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %         60.6 %
● mumbai ✓ ungrouped	0.0	0.0 01:45 01:50 01:55 02:00 02:05 02:10 02:15 02:20 02:25 02:30 02:35 02:40
▲ 192.168.0.25 ▲ 192.168.0.26	Throughput Avg Data Interfaces	Connection Statistics Connections Aug 0 0 - 0
	800 440 440 320 146 0 0 0 0 0 0 0 0 0 0 0 0 0	100 80 40 20 0.0 01:45 01:50 01:55 02:05 02:10 02:15 02:20 02:25 02:30 02:35 02:49
	Disk Usage	AMP         Java         LINA         SF Data Correlator         Shumel         SSE Connector           Snort01         Snort02         Snort02         Snort02         Snort02         Snort02

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

	Health: 192.168.0.21 Normal View System & Troubleshoot Details Overview CPU Memory Interfaces Connections S	Last 1 hour → ♡ 2020-06-23 02:26 - 2020-06-23 03:26
	CPU         Snort         Avg 0.9 %         System         Avg 16.0 %           1 core         0.5 % - 1.6 %         2 cores         0.0 % - 8.5 %         1 core         13.0 % - 75.0 %           100         00         00         00         00         00         00           00	Critical Werong. 03:00 03:05 03:10 03:15 03:20 03:25
CPU LINA Avg 2.7 % Snort 1 1 core 0.5 % -7.8 % 2 cores 0 100 	Avg 3.7 % 0 % - 10.5 % 1 core 14.0 % - 30.0 %	CPU       Short       Avg 4.3 %       System       Avg 20.6 %         1 core       0.95 × 8.2 %       2 cores       0.95 × 13.5 %       1 core       14.0 % × 75.0 %         100       #       Order       #       Order       Order         00       #       Order       #       Order       Order         00       #       Order       #       Order       Order         00       #       Order       #       Order       Order       Order         00       #       Order       Interface Policy       Order       Order       Order       Order       Order         00       #       Order       BGP Routing Policy       OSPF/3 Routing Policy       Input Rate Avg 0       OSPF/3 Routing Policy       OSPF/3 Routing Policy       OSPF/3 Routing Policy       Input Rate Avg 0       OSPF/3 Routing Policy       OSPF/3 Routing Policy       Input Routing Pol

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.

Hea View	alth: wm System & 1	1-101 📀	Normal Details				
Ov	erview	CPU	Memory	Interfaces	Connections	Snort	
Int g	erface - Ir	nput Bytes, (	Output Bytes				
in B	1.6K						
values	1.2K						
	800						
	400						
	0						
-		07:45		07:50	07	:55	08:00
Int	erface - Ir	nput Packets	s, Output Pack	ets, Drop Pack	ets		
10	0						
4	30						

#### Memória Snort FTD - De onde ela se origina?

Firepower Manage System / Health / Monitor	ement Cente	er <sub>Overview</sub>	Analysis	Policies	s Device	rs Obje	cts AM	IP Inte	lligence		Deploy	۹ (	<b>6</b> ¢	Ø Global \ mzafeiro ▼
Monitoring	Health: mz	afeiro_FTD11	150-1 (Active)	Normal								Last 2021	t 1 week	✓ ○ ▲ 59 - 2021-10-12 10:59
බ Home	Overview	CPU M	lemory Inte	erfaces (	Connections	Snort	ASP dro	ops						<u>ش</u> (+)
FMC	Memory - N	faximum Data Pla	ane, Data Plane	•										
V Devices (8)	5.7 G8													
V CISCO	4.9 GB													
	4.1 GB													
• 10.62.148.228	2.5 GB													
a mzafeiro 4125-1	12:00	Oct 08	12:00	Oct 07	12:00	Oct 08	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12
KSEC-FPR4145-1-2														
✓ mzafeiro FP1150-HA	20.2 GB	faximum Snort, S	Snort											
mzafeiro_FTD1150-1 Ac	16.3 GB							2021-10- Maxim	-08 22:15 CEST sum Snort 20.2 Gi	3				
mzafeiro_FTD1150-2 s	12.5 GB							anon	4.7 0	2				
mzafeiro_FTD4115-2	8.6 GB													
Sami_10.62.148.194	4.7 00					1		1				1		
	12:00	Oct 08	12:00	Oct 07	12:00	Oct 08	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12
	Memory - S	ystem Used, Tot	al											
	31.4 GB													
	20.2 GB													
	144.08													*

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			$\sim$			
Hide Details Dashboard Name*						
Correlation-CPU-Snort						
Metrics Chosen metrics will be displaye	d as portlets in the dashboard. Snort X	× ~	Ŧ			
Interface $\lor$	Input Packets X	× ~	) <b>ə</b>			
Deployed Configuration $\lor$	Number of rules X	× ~	•			
Deployed Configuration $\sim$	Number of ACEs X	X ~				
Add Metrics			47			
		Cancel Ad	d			

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:

Event Rate	
	No Data Available

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

Gisco System / Health / Monitor	ment Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy 9, 🥏 🌮 🍘 syed	¥
Monitoring The Home FMC FMC - Active FMC - Standby Devices (2) 0 192.168.0.219	Overview         CPU         Memory         Interfaces         Connections         Snort         ASP drops           CPU         Data Plane Aug 0%         Snort Avg 1%         System Avg 15%         Data Plane Aug 26%         Snort Avg 21%         System Avg 45%           100%         2 cores 0% - 1%         System Avg 15%         1 core         0% - 07%         3.9608 21% - 21%         System Avg 45%           20%         -         -         -         -         -         -           0%         -         -         -         -         -         -           0%         -	5
✓ FTD-HA	Dec 13 Dec 14 00:59 01:29 01:59 02:29 02:59 03:29 Dec 13 Dec 14 00:59 01:29 01:59 02:29 02:59 03:	:29
9 192.168.0.216	Throughput Avg - all interfaces Connection Statistics	
Image: Console     Source       Image: Consource     Source       Image: Cons	Input Rate         Output Rate         2000pa - 2.37ktps           0         2.56         1.36         1	23 ×
<pre>in MessageFrovider (at ToastProvider) in ToastProvider (at Provider); in ReatureFlagProvider [st] n EnsureFlagProvider [at Provider]; in EnsurtNodeFrovider [at Provider] in EnseprationProvider [at Provider] in ThemeProvider (at Provider) in EnseProvider (at LocaleProvider) in ConnectFunction (at Provider) in ConnectFunction (at Provider) in ConnectFunction (at Provider) in ReactBueryCacheProvider [at Provider] in ReactBueryCacheProvider [at Provider] in Provider [at application]; in StrictNode [at application];</pre>	<pre>(100r.js:00) (100r.js:00) (der.js:33) (der.js:33) (der.js:32) nmectFunction) (js:31) der.js:29) Nuer(CacheProvider.js:13) der.js:28) 36) 36) 36] 3135)</pre>	1
>		

Exemplo de Log do Console do Navegador

Console Tab Exception details	5						
Elements Console Sources Network Performance Memory Application Securit	ty Lighthouse Redux » 🛛 3 🗛 1 🔅 🗄 🗙						
🕩 🛇 top 🔻 🧿 Filter Default levels 🔻	\$						
▼ Validation using FMC HA State schema failed with 2 error(s) validator.js:75							
<pre></pre>							
<pre></pre>							
▲ > Details > {data: {}, error: {}, schema: {}}							
⊘ ►► F {message: "validation failed", errors: Array(2), validation: true, ajv: true}							
BaseLineChart - Render BaseLineChart.js:376							
Baseline chart props changed BaselineChart.js:163							
undefined 0 100 100 undefined > [{}] "area" undefined > (2) [{_}, {}] > {type: "UTC_TIME", range: e} "percent" undefined undefined 5							
	- · · · · · · · · ·						

## 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.