# Aggiorna FP - Monitoraggio stato dispositivo

### Sommario

ntroduzione	
nformazioni sullo sfondo	
Panoramica delle funzionalità	
Feature Details 7.0	
FTD: metriche introdotte nel FP 7.0	
Feature Details 6.7	

### Introduzione

Questo documento descrive la nuova funzione di monitoraggio dello stato dei dispositivi aggiunta nelle versioni 6.7 e 7.0.

### Informazioni sullo sfondo

Il problema:

Il sistema di monitoraggio dello stato fornisce visibilità sulle prestazioni del dispositivo per il debug reattivo e le azioni proattive.

La visibilità e l'analisi complete si ottengono mediante:

- · Grafici di andamento per le metriche chiave
- Sovrapposizione evento
- Dashboard personalizzabili
- Architettura unificata di monitoraggio dello stato: vedere gli stessi dati per tutti i responsabili
- Numerose nuove metriche ed estendibilità delle metriche per aggiungerne altre

Novità della release 7.0

Novità o differenze rispetto al 7° PQ

- Dashboard FMC con supporto HA
- Oltre 110 nuove metriche per FTD
- · Avviso di integrità per lo scenario di separazione del cervello FTD
- Intervallo di tempo di esecuzione personalizzato per le metriche di integrità più recenti

Vantaggi

- Consente di eseguire il debug del sistema grazie alla possibilità di correlare i dati di diversi sottosistemi e risorse sul dispositivo
- · Visibilità di varie metriche delle prestazioni del sistema

• Pianificazione della capacità

Novità della versione 6.7

Nuovo o diverso rispetto alla release immediatamente precedente (di alto livello):

- Nuova interfaccia utente per il monitoraggio dello stato dei dispositivi in FMC
- FTD Device REST API: API device-metric: molte nuove metriche aggiunte
- API FMC: nuove API: avvisi di integrità, metriche di integrità e dettagli di distribuzione
- Panoramica di mercato di alto livello, applicazioni reali
- Consente di eseguire il debug del sistema grazie alla possibilità di correlare i dati di diversi sottosistemi e risorse sul dispositivo
- Visibilità
- Pianificazione della capacità

### Panoramica delle funzionalità

#### Come funziona

- Monitoraggio dello stato dei dispositivi in FP 7.0
- Nuovo dashboard di integrità per FMC che fornisce grafici di tendenza, sovrapposizioni e dashboard personalizzati
- Nuove metriche FTD disponibili nei dashboard FTD
- Più di 110 metriche che coprono 12 categorie
- API FTD: rende le metriche disponibili per l'esecuzione di query da parte di entità esterne

#### Sotto il cofano,

Raccoglie l'integrità di un dispositivo con Telegraf (un framework di raccolta di metriche open-source)

#### Note aggiuntive

Sono disponibili dati di monitoraggio dello stato

- Nel Dashboard stato di FMC, accessibile dal menu di sistema (Sistema > Integrità > Monitor)
- Dall'API REST di FMC
- Quando il dispositivo è gestito da FDM, tramite l'API REST del dispositivo FTD

Alcune metriche (sia FMC che FTD) sono disabilitate per impostazione predefinita

• Per visualizzare alcune metriche, è necessario abilitare e distribuire i moduli di integrità nei criteri di integrità.

Attuazione dei miglioramenti richiesti dal 6.7° PQ

- · Aggiornamento automatico per impostazione predefinita
- Filtra con intervallo di tempo personalizzato nel dashboard
- · Selezionare le interfacce in base al nome definito dall'utente (nonché al nome dell'interfaccia

fisica) nel selettore di interfaccia

• Dashboard del dispositivo per l'avvio incrociato dalla pagina 'Home' di Health Monitor

Monitoraggio dello stato dei dispositivi in FP 6.7

- Nuova interfaccia utente di FMC che fornisce grafici di tendenza, sovrapposizioni e dashboard personalizzati.
- API FTD: rende disponibili le stesse metriche per eseguire query in base a entità esterne.

Riepilogo delle limitazioni:

- La funzionalità non è supportata nella GUI o nel CDO di FDM
- Il monitoraggio di FMC stesso nella nuova interfaccia utente di monitoraggio dello stato non è supportato.
- Gli intervalli di polling non sono configurabili. Non è possibile configurare intervalli di polling diversi per dispositivi diversi. Tutte le richieste vengono sottoposte a polling a intervalli fissi di un minuto.

Esempi di distribuzione

- Nessuna distribuzione specifica necessaria per testare la funzionalità. È sufficiente aggiornare FMC e il dispositivo a FP 6.7.
- I dati di monitoraggio dello stato sono disponibili nel dashboard di stato del CCP, accessibile dalla scheda Sistema.



Prerequisiti e piattaforme supportate

Minimo piattaforme software e hardware supportate

Versione minima di Gestione supportata	Dispositivi gestiti	Versione minima dispositivo gestito supportato richiesta	Note
CCP 6.7	FTD 6,7	FXOS 2.9.1 FTD 6,7	Supportato solo su FTD
API REST dispositivo FTD	FTD 6,7	FXOS 2.9.1 FTD 6,7	Solo API REST dispositivo FTD (non FDM o CDO GUI)

Interoperabilità

Nessun requisito specifico di interoperabilità.

### Feature Details 7.0

Interfaccia utente FMC: supporto autonomo e HA

Navigazione nelle pagine di monitoraggio dello stato

CISCO FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹ 🔮	¢	0	syed 🕶
Monitoring The Home FMC Active FMC Standby FMC Devices (2) 192.168.0.21 9 192.168.0.21	(☐) ; 6 7	Health S	Caritical 2 critical Vices MC_Active MC_Standby 22.168.0.217	0 warnings	1 normal	1 disabled	C. Filter u	sing device	name			

- FMC autonomo visualizzato come nodo singolo
- FMC HA visualizzato come coppia di nodi
- Ogni CCP è indicato con lo stato di salute

- FMC HA è indicato in doppio esagono.
- Nella tabella degli allarmi sono elencate anche le periferiche attive e in standby di FMC.

#### Dashboard FMC

Dashboard di monitoraggio dello stato di FMC in 7.0

Firepower Manage System / Health / Monitor	ement Cente	Overview	v Analysis	Policies	Devices	Objects	AMP Intelligence	Deploy 🔍 🥝 🏠 🔞 syed 🔻
Monitoring (書) 없 Home	Health: FM0 View System & T Overview	C_Active roubleshoot Detail Process	Critical					Select V C 2020-12-08 04:04 - 2020-12-08 05:04
<ul> <li>FMC</li> <li>Active FMC</li> <li>Standby FMC</li> <li>Devices (2)</li> <li>192.168.0.216</li> </ul>	High Availabil Loca	Active A D	Degraded Last sync: a few sec egraded- Synchronizi	ands ago ation incomplete	F Second	Manage HA temote	Event Rate	01.30 01.41 01.49 01.54 01.59
• 192.168.0.217	Process Healt	th DCCSM ESS	Msg Service	Critical Proce	Prunor	All Processes RabbitMQ	Event Capacity Connection 59 days 3 Ars 14 mins Intrusion 40 Events File 210 days 3 Ars 13 mins	Configure 526.79K/1M 0/1M 1.29M/1M
	SEDC Since Section 2015 SEDC Section 2015 SEDC Section 2015 SECTION 20	SF Data Sync Correlator Monet DB Mon SLA	go DB MySQL DB Sybase Arbiter	Provisioning Process Run HM Symmetrie	SFIP Proxy	Disk Manager SF Mgr vase DB	Security Intelligence 57 days 3 hrs 13 mins Connection Summary No Events Malware No Events Discovery No Events User No Events	100K/1M 0/1M 0/2M 0/1M 0/1M
	CPU 100% 75% 50% 0% 04.04 04.04 04.04	09 04:14 04:19	0424 0429 04	34 04:39 04	Avg CF	2U ~	Memory - Used 100% 50% 25% 25% 0% 0%	04/34 04/39 04/44 04/49 04/54 04/59
	Interface - In 64.3K 133.2K 22.2K 11.1K 0 04.04 04	09 04:14 04:19	put Rate	34 04:39 04:	44 D4:19	De:54 04:59	Disk Usage Entire Disk	Critical Partitions

Visualizzazione di riepilogo di:

- Alta disponibilità
- · Velocità e capacità degli eventi
- Integrità del processo
- CPU
- Memoria
- Interfaccia
- Disco

Questo dashboard è disponibile sia per i CCP attivi che per quelli in standby. L'utente può creare dashboard personalizzati per monitorare le metriche scelte.

Dashboard FMC: pannello HA FMC

High Availability		Configure
Local Primary- Active	Degraded Last sync: a few seconds ago Degraded- Synchronization incomplete	Remote Secondary- Standby FMC_Standby - Critical Alerts: 2 4 0 21 Top 5 Alerts File system integrity check FMC HA Status Host Limit Classic License Expiration Monitor AMP for Endpoints Status

#### Il pannello HA mostra

- Stato HA corrente
- Attivo/Standby
- Ora ultima sincronizzazione
- Integrità del dispositivo

Dashboard FMC: velocità e capacità degli eventi

Frequenza eventi

- · Velocità evento massima come linea di base
- Frequenza eventi complessiva ricevuta da FMC

#### Capacità evento

- Consumo corrente per categorie di eventi
- Tempo di conservazione degli eventi
- Corrente rispetto a Massima

#### capacità evento

· Indicatore di overflow della capacità

He Viev O	alth: FN v System & verview	MC Orit Troubleshoo Process	tical ot Details s											Last 2021	1 hour	r 06:32 - 2	2021-02	-22 07:32
Pro	ocess He	alth			Crit	tical Proce	sses A	II Processes	Event Capacity	-							Co	nfigure
	1.100	DOODL	500	Mar Cardina	Deal	Develop	Destable	0500	Connection	3 days 16 hrs 3 m	ins						1/1M	Ê
A	ctionQ	DCCSM	655	Msg Service	MsgHandler	Pruner	RabbitMQ	Notifier	Intrusion	No Events						(	0/1M	
	C Data	0.000	Townsh	Descisioning	ADI	Disk	Main	Marat DD	File	No Events							0/1M	
C	errelator	Sync D	Tomcat	Process	ADI	Manager	MOJO	Monet DB	Security Intelligence	No Events						(	0/1M	
		14.001.00	Durality	0510.0	05.14-2	Othersel	01.4	C. hund	Connection Summary	No Events							0/1M	
~	iongo DB	MySQL DB	KUN HM	SHIP Proxy	SH Mgr	Situnnei	SLA	Arbiter	Malware	No Events							0/2M	
s	ymmetric		1		Sybase DB			1	Discovery	No Events							0/1M	
									User	No Events							0/1M	-
_										-								
CE	U						Avg CPI	u ~	Event Rate									
0.	Data coll	lection for C	PLLmodul	e is disabled	in the healt	h policy p	artial or no	data may be	5.0k									
▲	shown.		or or module	6 15 01500160	in the near	in policy, p		data may be	3.8k									
	01101111								2.5k									
									1.3k									_
									0.0									
				No Data	Available	9			06:35 06:40	06:45 06:50	06:55	07:00	07:05	07:10	07:15	07:20	07:25	07:30

#### Dashboard FMC: capacità evento

#### Stato consumo capacità evento normale

Normal:				
Connection	182 days 4 hrs 23 mi	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	v:			
Connection	18h			11.6 M / 10 M
	2020-09-18 14:28:30			_ \
Connection	18h 18 hours	3.6k/min	116245455/100000000	11.6 M / 10 M
	Retention Duration	Incoming Rate	Capacity 🔺 🔫	

Scenario di overflow, quando gli eventi vengono archiviati oltre la capacità massima configurata.

- Il testo in grassetto indica un riversamento
- Un'icona di avvertenza evidenzia l'overflow della capacità

Dashboard di FMC: pannello Processo di FMC

Il pannello Processi critici mostra

- Elabora stato corrente
- Conteggio riavvii processo

rocess H	ealth					Critic	cal Proc	esses A	All Processe
ActionQ	tionQ DCCSM ESS		Msg Service	Perl MsgHandler	Pruner	R	RabbitMQ	SFDC Notifier	SF Data Correlator
Sync D	Tomcat	Provisioning Process	ADI	Disk Manager		Mojo Monet		Mongo DB	MySQL DB
Run HM SFIP Proxy SF M		y SF Mgr	Sftunne	Sftunnel SLA		Sybase Arbiter		Symmetric	Sybase DB

Il pannello dei processi mostra queste metriche per tutti i processi "pmconfig":

- Stato corrente
- Utilizzo CPU
- Utilizzo memoria

Process Health		Critica	al Processes	All Processes
Process status at: Dec 14, 2020 3:	22 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 4			3.26KB
Event DS	Running	0	34	1.59KB

#### Dashboard FMC: CPU FMC

Il pannello CPU mostra

- CPU media (predefinita)
- Tutti i core





#### Dashboard di FMC: altri pannelli

Il pannello Memoria mostra l'utilizzo complessivo della memoria su FMC



#### Il pannello Interfaccia mostra la velocità di ingresso/uscita della media di tutte le interfacce



#### Il pannello Disco mostra

- Intera capacità del disco
- · Capacità di partizione critica in cui sono archiviati i dati FMC

Disk Usage	
Entire Disk	Critical Partitions
9% Used	12% Used
	/dev/sda7

Intervallo di tempo di esecuzione

- L'intervallo di tempo di esecuzione per il vecchio modulo di integrità viene rinominato come 'Intervallo di tempo di esecuzione legacy'
- 'Run Time Interval' è destinato ai nuovi moduli di integrità basati su Telegraf
- · Impostazione globale, ha effetto su tutti i dispositivi

CISCO Edit Overview Analy	vsis Policies	Devices	Objects	AMP	Intelligence	Deplo	/ Q	0	¢	0	admin 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status	Editing Poli	icy: Initial_H	ealth_Polic	y 2021-	01-29 04:40:	49					Alerts
AMP For Endpoints Status AMP for Firepower Status ASP Drap	Po	Policy Name licy Description	Initial_He	alth_Policy	2021-01-29 (						
Advanced Snort Statistics Appliance Heartbeat Automatic Application Bypass Status	Legacy Ri Run Time Note : Change:	un Time Interva (mins) e Interval (mins) s to Run Time Im	5 ) 1 terval will resta	t the health							
Backlog Status CPU Usage (per core) CPU Usage Data Plane	monitoring pro	cess.									
CPU Usage Snort CPU Usage System Card Reset	-				Gancel	Save Policy and Exi					
Chassis Status FTD Cluster/Failover Status Configuration Database											
Connection Statistics Critical Process Statistics Deployed Configuration Statistics											
Disk Status											

Metriche disponibili

Metriche disponibili per dashboard personalizzati

• Se un utente desidera creare un dashboard personalizzato, queste diapositive sono una guida alle metriche disponibili.

• È necessario abilitare alcune metriche nei criteri di integrità prima di poterle utilizzare in un dashboard di integrità personalizzato

CISCO Edit Overview Analysis	Policies	Devices	Objects	AMP	Intelligence	De	ploy	۹	69	۵	0	syed •
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status AMP For Endopints Status	Editing Polic [en_US/adn	:y: Initial_He nin:policy_la	ealth_Policy ast_modifie	/ 2020-1 d])	2-08 08:49:46	; (Last Modified:						Alerts
AMP for Firepower Status ASP Drop	Polie	Policy Name cy Description	Initial_Hea	th Policy	2020-12-08 (							
Appliance Heartbeat		Description	Monitors CPU cores, thresh applicable to	J usage on old set here all the core	all the will be s							
Backlog Status	Critica	Enabled al Threshold %	● On ○ O 90	λŧ								
CPU Usage Data Plane CPU Usage Snort	Warnin	g Threshold %	80									
CPU Usage System Card Reset					Cancel	Save Policy and E	xit					
Chassis Status FTD Cluster/Failover Status												
Configuration Database Connection Statistics												
Critical Process Statistics Deployed Configuration Statistics												
Disk Status Disk Usage												
Event Stream Status FMC Access Configuration Changes												

#### Interfaccia utente FMC: dashboard personalizzato FMC

Nuove categorie di metriche di monitoraggio FMC in 7.0

- CPU
- Memoria
- Interfaccia
- Disco
- Evento
- Processo
- RabbitMQ
- Sybase
- MySQL

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

Interfaccia utente FMC: Metriche FMC

40 metriche aggiunte tra diverse categorie (disponibili nel dashboard personalizzato). Per abilitare le metriche disabilitate, abilitare il modulo di integrità corrispondente nel criterio di integrità associato (Sistema > Integrità > Criteri).

Nome gruppo di metriche	Attivato per impostazione predefinita	Descrizione
CPU	No	Controlla la CPU FMC
Memoria	Sì	Monitoraggio della memoria FMC
Disco	Sì	Monitoraggio dell'utilizzo del disco della console Gestione risorse
Interfaccia	Sì	Monitor FMC Interface
Processo	Sì	Monitoraggio dei processi FMC
Evento	Sì	Frequenza eventi monitor
MySQL	No	Controlla MySQL

RabbitMQ	No	Monitor RabbitMQ
Sybase	No	Monitor Sybase

### FTD: metriche introdotte nel FP 7.0

Abilitato per impostazione predefinita: le metriche vengono raccolte per impostazione predefinita. Per abilitare le metriche disabilitate, abilitare il modulo di integrità corrispondente nel criterio di integrità associato (Sistema > Integrità > Criteri).

Nome gruppo di metriche	Attivato per impostazione predefinita	Descrizione	Piattaforma
Stato dello chassis	Sì	Esegue il monitoraggio di diversi parametri dello chassis, quali la velocità della ventola e la temperatura.	Applicabile solo alle piattaforme FPR2100 e FPR1000
Funzionalità Flow Offload	Sì	Monitoraggio delle statistiche di offload del flusso hardware	Applicabile a FPR9300 e piattaforme FPR4100
Cadute ASP	Sì	Monitoraggio delle perdite di pacchetti lina	Tutto
Conteggio visite	No	Monitoraggio dei conteggi delle corrispondenze per le regole dei criteri di controllo di accesso	Tutto
Stato AMP Threat Grid	Sì	Monitoraggio della connettività ad AMP ThreatGrid	Tutto
Stato connettività AMP	No	Monitoraggio della connettività cloud AMP da FTD	Tutto

Stato connettore SSE	No	Monitoraggio della connettività cloud SSE dall'FTD	Tutto
Stato NTP	No	Controlla i parametri di sincronizzazione dell'orologio NTP su FTD	Tutto
Statistiche VPN	Sì	Monitoraggio delle statistiche del tunnel VPN da sito a sito e da sito	Tutto
Statistiche ciclo di lavorazione	Sì	Monitoraggio delle perdite di pacchetti lina	Tutto
Statistiche prestazioni Snort 3	Sì	Esegue il monitoraggio di alcune statistiche sulle prestazioni di Snort3 (perfstats)	Tutto
Contatori xTLS	No	Monitoraggio dei flussi xTLS/SSL, della memoria e dell'efficacia della cache	Tutto

#### API REST, Syslog, SNMP

Nella versione 7.0 non sono state introdotte nuove API REST FMC o FTD. Le API REST esistenti supportano le nuove metriche aggiunte nella versione 7.0.

Syslog e SNMP

Syslog

Nessuna modifica nel syslog per Health Monitor

#### SNMP

• TOI separato per "SNMP Device Health Monitoring"

Integrazione di SAL/CTR/prodotti di terze parti

• TOI separato per il supporto di 'Azure Application Insights'

- Nessuna modifica specifica apportata per supportare l'integrazione del monitoraggio dello stato con SAL/CTR/SecureX
- L'API REST può essere utilizzata per l'integrazione con terze parti

Tecnologia software

### Feature Details 6.7

Nuovo monitoraggio dello stato NGFW per stato e prestazioni FTD

#### Aiuta gli utenti con

- Debug reattivo, ad esempio l'analisi della causa principale del problema dopo che si è verificato
- Azioni proattive, quali il monitoraggio dei livelli di utilizzo e saturazione, per identificare potenziali problemi di capacità e, di conseguenza, aiutare gli utenti a migliorare la capacità o a refactoring.

#### Caratteristiche

- Grafici di andamento: i grafici di andamento consentono di rilevare con estrema facilità le anomalie e di determinare la causa principale dei problemi. Con l'ispezione visiva è possibile individuare le tendenze e tracciare le correlazioni tra diverse metriche per trovare la relazione causale tra di esse.
- Sovrapposizioni di eventi: le sovrapposizioni di eventi mostrano informazioni importanti, quali la distribuzione della configurazione e gli aggiornamenti SRU nei grafici di andamento per indicare le relazioni causali.
- Dashboard personalizzabili: gli utenti possono creare i propri dashboard per raggruppare le metriche che desiderano visualizzare in un'unica pagina.
- Architettura di monitoraggio dello stato unificato: singolo punto di raccolta ed esportazione per le metriche, indipendentemente dal responsabile "interessato" alle metriche. Le API FTD e il CCP utilizzano i dati dello stesso agente di raccolta metriche.
- Estendibilità delle metriche: uno degli obiettivi dell'architettura per la piattaforma era quello di poter aggiungere facilmente nuove metriche. Ciò è possibile utilizzando gli strumenti di raccolta e archiviazione delle metriche Open Source e con dashboard personalizzabili.

#### **GUI FMC**

Interfaccia utente di FMC: Passa a Stato integrità

Su FMC, fare clic sull'icona Sistema > Integrità > Monitor per passare alla pagina Stato di integrità.



Interfaccia utente FMC: pagina Nuovo stato integrità

La pagina Stato di integrità consente di visualizzare una panoramica dello stato di tutti i dispositivi gestiti dal CCP, incluso lo stato del CCP.

- I dispositivi sono raggruppati in base al gruppo/ha/cluster.
- Un punto a sinistra del dispositivo ne indica lo stato
- Verde nessun allarme
- · Arancione almeno un avviso di integrità
- Rosso almeno un allarme sanitario critico
- Il riepilogo dello stato viene visualizzato quando si passa il mouse sull'esagono che rappresenta lo stato di salute del dispositivo.
- Le soglie di avvertenza e critica possono essere configurate nei criteri di integrità, nello stesso modo in cui sono state configurate prima del 6.7.

Monitoring 😑	Health Alerts
ගි 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> <li>Bangalore (HA)</li> <li>bangalore-main</li> </ul>	FMC     Asia     ungrouped       Image: Device     192.168.0.26 - Warning       Alerts: 1 0     A 2     0 21       Top 5 Alerts
bangalore-standby	FMC     GPU Usage     CPU used by system
chennai	o bangalore-main     o Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalore-standby     Local Malware Analysis     Local Malware Analysis
A 192,168,0,25	Clickto view more details
A 192.168.0.26	> 🧿 mumbai
	> 🛕 192.168.0.25
	> ▲ 192.168.0.26

Interfaccia utente di FMC: eventi di integrità del dispositivo

Fare clic sul dispositivo nel pannello inferiore per visualizzare gli eventi di stato associati al dispositivo. Gli avvisi vengono ordinati in base allo stato di salute (gravità).

#### Pagina Monitoraggio stato

>	▲ 192.168.0.25	
~	▲ 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
	Cluster/Failover Status     Process is running correctly	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

Interfaccia utente FMC: monitoraggio stato FMC non modificato

La pagina dello stato di salute di FMC è ancora la pagina legacy. La nuova interfaccia utente è supportata solo per FTD con 6.7+

Monitoring	Health	Monitor				
e 1140 e wm-101	•	Appliance vfmc-10	Generate Troubleshooting Files Advanced Troubleshooting			Module Status Summary Double Nermal (56.005)
	Alert D	etail (vfmc-10)				
		Alert		Time	Description	
	•	Process Status		2020-06-18 08:50:44	All processes are runn	ning correctly
	•	AMP for Endpoints Status		2020-06-18 08:50:44	Process is running con	rectly
	•	AMP for Firepower Status		2020-06-18 08:50:44	Successfully connecte	ed to cloud

FMC UI: Novità! Dashboard dispositivi

- Fare clic sul nome del dispositivo nel riquadro di sinistra per accedere alla pagina di panoramica dello stato del dispositivo.
- La panoramica dello stato contiene tutti i grafici delle tendenze delle metriche dello stato chiave.
- Sono disponibili vari intervalli di tempo (il valore predefinito è 1 ora)
- · Aggiornamento automatico per ricaricare il grafico

Monitoring	Health: 192.168.0.25 A Warning View System & Troubleshoot Details	Last 1 hour V 0 2020-06-23 01:58 - 2020-06-23 02:58
từ home	Overview CPU Memory Interfaces Connections Snort	± +
FMC	CPU	Memory
<ul> <li>Devices (5)</li> </ul>	LINA Avg 1.5 % Snort Avg 0.7 % System Avg 17.5 % 1 core 12 % - 2.6 % 2 cores 0.5 % - 1.0 % 1 core 15.0 % - 24.0 %	LINA Avg 49.7 % Snort Avg 28.1 % System Avg 68.8 % 4.0468 49.7 % - 49.7 % 3.9668 28.1 % - 28.1 % 7.808 66.8 % - 69.4 %
✓ Asia	100	100 Cillor
Bangalore (HA)	80	80
💩 bangalore-main	60	60
bangalore-standby	40	40
chennai	20Wampa	20
⊚ mumbai ∽ ungrouped	0.0 01.45 01.50 et.56 02.90 02.05 62.10 02.15 02.20 02.25 02.39 62.35 02.40	0.0 01.45 01.50 01.55 02.00 02.05 02.10 02.15 02.20 02.25 02.00 02.25 02.40
▲ 192.168.0.25	Throughput Avg Data Interfaces V	Connection Statistics
▲ 192.168.0.26	In sut Rate Aug 0 0 - 0 Output Rate Aug 0 0 - 0	Connections Avg 0 0 + 0 NAT Translations Avg 0 0 + 0
	2 800 2	100
	640	80
	480	60 40
	320	20
	160	0.0
	01.45 01.50 01.55 02.00 02.95 02.10 02.15 02.20 02.25 02.30 02.35 02.40	01:45 01:50 01:55 02:00 02:05 02:10 02:15 02:20 02:25 02:30 02:25 02:40
	Disk Usage	Critical Processes
	9% Used Used Used	AMP Java LINA SF Data Correlator Snort01 Snort02
	Full Disk /ngfw /ngfw/Volume	

Interfaccia utente di FMC: overlay dei dati di distribuzione

Fare clic sull'icona di distribuzione per visualizzare i dettagli della sovrapposizione di distribuzione nel grafico relativo all'intervallo di tempo selezionato

- Icona indica il numero di distribuzioni durante l'intervallo di tempo selezionato
- Viene visualizzata una banda che indica l'ora di inizio e di fine della distribuzione.
- In caso di distribuzioni multiple, vengono visualizzate più bande/linee
- Fare clic sull'icona sopra la linea tratteggiata per visualizzare i dettagli



Interfaccia utente di FMC: dashboard predefiniti del dispositivo

- Nell'interfaccia utente di FMC sono presenti dashboard predefiniti per l'integrità.
- Questi dashboard predefiniti vengono forniti con le metriche correlate raggruppate insieme.
- Il dashboard dell'interfaccia dispone di un grafico di andamento per tutte le metriche relative all'interfaccia, ad esempio byte di input/output, pacchetti e dimensioni medie dei pacchetti per diverse interfacce.

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						

#### FTD Snort Memory - Da dove ha origine?

Firepower Manage System / Health / Monitor	ent Center Overview Analysis	Policies Devices C	bjects AMP Intelligence	Deploy	🔍 🚱 🔅 🔞 Global \ mzafeiro 🔻
Monitoring 😑	Health: mzafeiro_FTD1150-1 (Active)	Normal			Last 1 week
යි Home	Overview CPU Memory Interfa	ces Connections Sno	rt ASP drops		af
FMC					
<ul> <li>Devices (8)</li> </ul>	Memory - Maximum Data Plane, Data Plane				
√ cisco	5.7 GB				
mzafeiro_FP4100_8	4.1 GB				
✓ GTS-FTD-IPS-CLUSTER	3.3 GB				
A 10.62.148.228	2.5 GB				
mzafeiro_4125-1	12:00 Oct 05 12:00 Oct	07 12:00 Oct 08	12:00 Oct 09 12:00	Oct 10 12:00	Oet 11 12:00 Oet 12
KSEC-FPR4145-1-2	Memory - Maximum Sport Sport				
v mzafeiro_FP1150-HA	20.2 GB		0001-10-02 00:15 0	COT	
mzafeiro_FTD1150-1 Ac	16.3 GB		Maximum Snort 20	22 GB 4.7 GB	
mzafeiro_FTD1150-2 st	12.5 GB		-		
mzafeiro_FTD4115-2	8.6 GB				
Sami_10.62.148.194	1.1 08		1		
	12:00 Oct 08 12:00 Oct	07 12:00 Oct 08	12:00 Oct 09 12:00	Oct 10 12:00 0	Oet 11 12:00 Oet 12
	Memory - System Used, Total				
	31.4 GB				
	25.8 GB				
	20.2 GB				•

Interfaccia utente di FMC: è possibile creare dashboard personalizzati

Gli utenti possono creare un dashboard personalizzato

- Oltre ai dashboard predefiniti, un utente può anche creare dashboard personalizzati.
- Nel dashboard personalizzato è possibile aggiungere un numero qualsiasi di metriche.

- In genere, un dashboard personalizzato viene creato se le metriche di diversi gruppi di metriche possono essere correlate per ottenere la causa principale di un problema.
- In caso di CPU Lina elevata, è possibile visualizzare le connessioni in ingresso al secondo (CPS), le statistiche dell'interfaccia (e così via) che possono causare un aumento della CPU.



Interfaccia utente di FMC: creazione di un dashboard personalizzato

Finestra di dialogo Correla metriche

- Quando un utente fa clic su "+" per creare un dashboard personalizzato, viene visualizzata la finestra Correla metriche.
- Un utente può aggiungere diverse metriche che desidera monitorare insieme.

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 displayed	d as portlets in the dashboard.	× ~	Ŵ						
Interface v	Input Packets X	× ~	ŵ						
Deployed Configuration $\lor$	Number of rules X	× ~	Ŧ						
Deployed Configuration $\sim$	Number of ACEs X	X ~	Ŵ						
Add Metrics									
	c	ancel Add							

Raccolta dati da (dispositivo) - GUI

Dati per un intervallo di tempo visualizzati nella GUI

Se il Monitor per la salute non dispone di dati per l'intervallo di tempo selezionato, l'interfaccia grafica mostra 'Nessun dato disponibile' nel pannello del dashboard:

Event Rate	
	No Data Available



Nel caso di dati disponibili, il grafico è il seguente:

Utilizzare le schede Console e Rete del browser

Registro console browser e registro chiamate di rete

- In questo esempio, viene mostrata la console di sviluppo del browser Chrome
- In caso di errore, i dettagli dell'eccezione vengono visualizzati nel log della console

Gisco System / Health / Monitor	nent Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🤉 🌘	👂 🔅 😰 syed 🔻
Monitoring 😑	Overview CPU Memory Interfaces Connections Snort ASP drops	<b>(</b> +)
127 Home ✓ FMC ■ FMC - Active ■ FMC - Standby ✓ Devices (2) ■ 192.168.0.219 ✓ FTD-HA	CPU         Data Plane Aug 0%         Snort Aug 1%         System Aug 15%         Data Plane Aug 76%         Snort Aug 21%         System 3.0258           100%         2 cores 0% - 1%         1 core 0% - 37%         100%         3.0258         70% - 70%         3.9668 21% - 21%         7.868           90%         2 cores 1% - 1%         0 core 0% - 37%         0%         0%         50%         26%         0%	n Avg 45% 43% - 42%
9 192.168.0.216	Consulta Stalate	
192. 168.0.217	Input Rate         Avg 1.34Kbps d398bps - 2.24Kbps         Output Rate         Avg 2.03Kbps d005bps - 2.37kbps         Connections         Avg 2.4 Avg 44         NAT Translations         Avg 0 00           2.5K         ax         Avg 2.03Kbps         0.00000000000000000000000000000000000	02.29 02.59 03.28 ♀ 5 ■ 354 ☆ ⋮ ×
Image: Solution of the soluti		
● >> {type: "unknown"}		index.js:1
>		

Esempio di registro della console del browser

Console Tab	Exception details		
Elements Console Sources Network Performance	Memory pplication Security Lighthouse Redux » 🛛 🛛 🖄 🕹 1 🔯 🗄 🗙		
🕨 🛇 top 🔻 💿 Filter	Default levels 🔻		
v Validation using FMC HA State schema failed with 2 error(s) validator.js:75			
<pre>&gt; bdata.remote.status[2] = null should be string,number (per #/definitions/Status/properties/status/items/type)</pre>			
<pre>© bdata.remote.status[3] = null should be string,number (per #/definitions/Status/properties/status/items/type)</pre>			
▲ > Details > {data: {_}, error: {_}, schema: {_}}			
② ▶▶ {message: "validation failed", errors: Array(2), validation: true, ajv: true}			
BaseLineChart - Render			
Baseline chart props changed BaseLineChart.js:163			
undefined 0 100 100 undefined > [{-}] "area" undefined > (2) [{-}, {}] > {type: "UTC_TIME", range: e} "percent" undefined undefined 5			
the second second			

## Riferimenti

Monitoraggio dello stato del CCP - 6.7

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).