

# Aggiorna FP - Monitoraggio stato dispositivo

## Sommario

---

[Introduzione](#)

[Informazioni 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 estensibilità 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

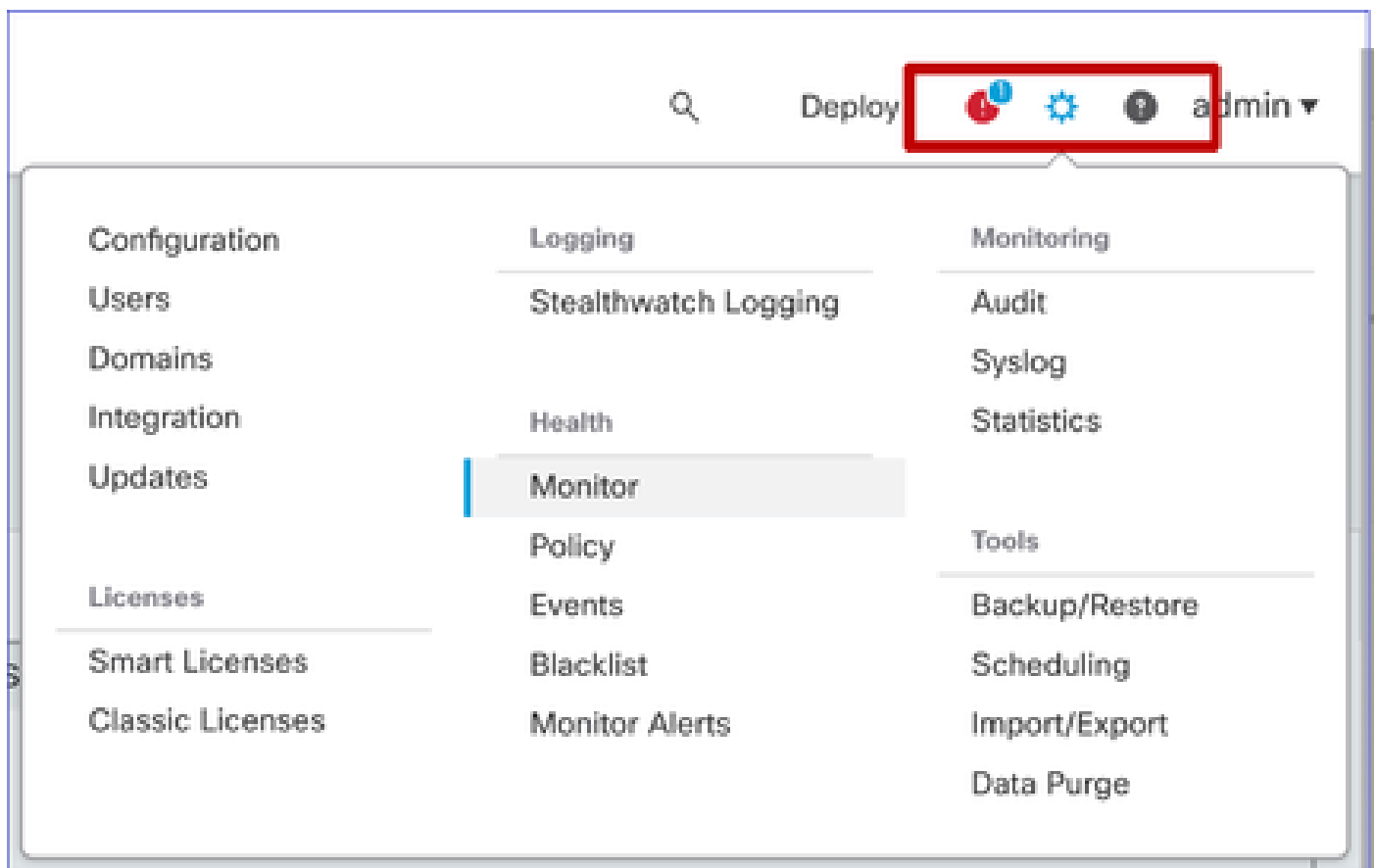
- Nuova interfaccia utente di FMC che fornisce grafici di tendenza, sovrapposizioni e dashboard personalizzati.
- API FTD: rende disponibili le stesse metriche per eseguire query in base a entità esterne.

#### 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)

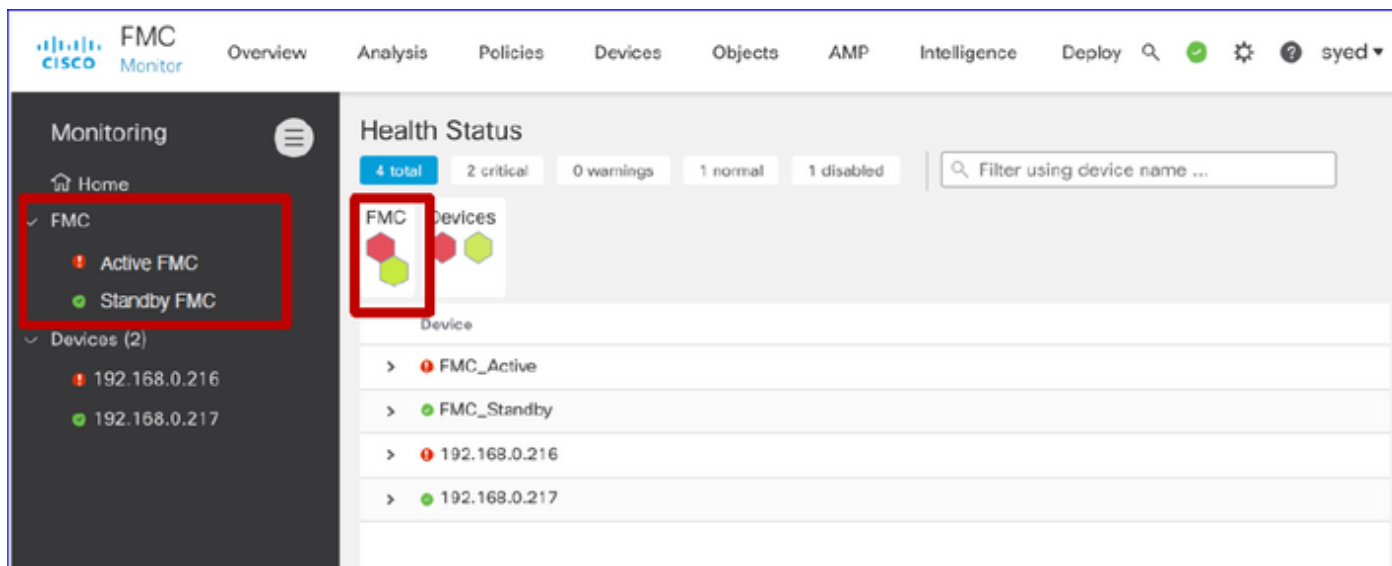
## Interoperabilità

Nessun requisito specifico di interoperabilità.

## Feature Details 7.0

Interfaccia utente FMC: supporto autonomo e HA

Navigazione nelle pagine di monitoraggio dello stato



The screenshot displays the Cisco FMC Monitor 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 two sections: 'Monitoring' on the left and 'Health Status' on the right. In the 'Monitoring' section, 'FMC' is selected, showing 'Active FMC' (red) and 'Standby FMC' (green). Below it, two devices are listed: '192.168.0.216' (red) and '192.168.0.217' (green). In the 'Health Status' section, a summary shows '4 total' (2 critical, 0 warnings, 1 normal, 1 disabled). A search bar is present with the text 'Filter using device name ...'. Below the summary, a table lists the devices: 'FMC\_Active' (red), 'FMC\_Standby' (green), '192.168.0.216' (red), and '192.168.0.217' (green).

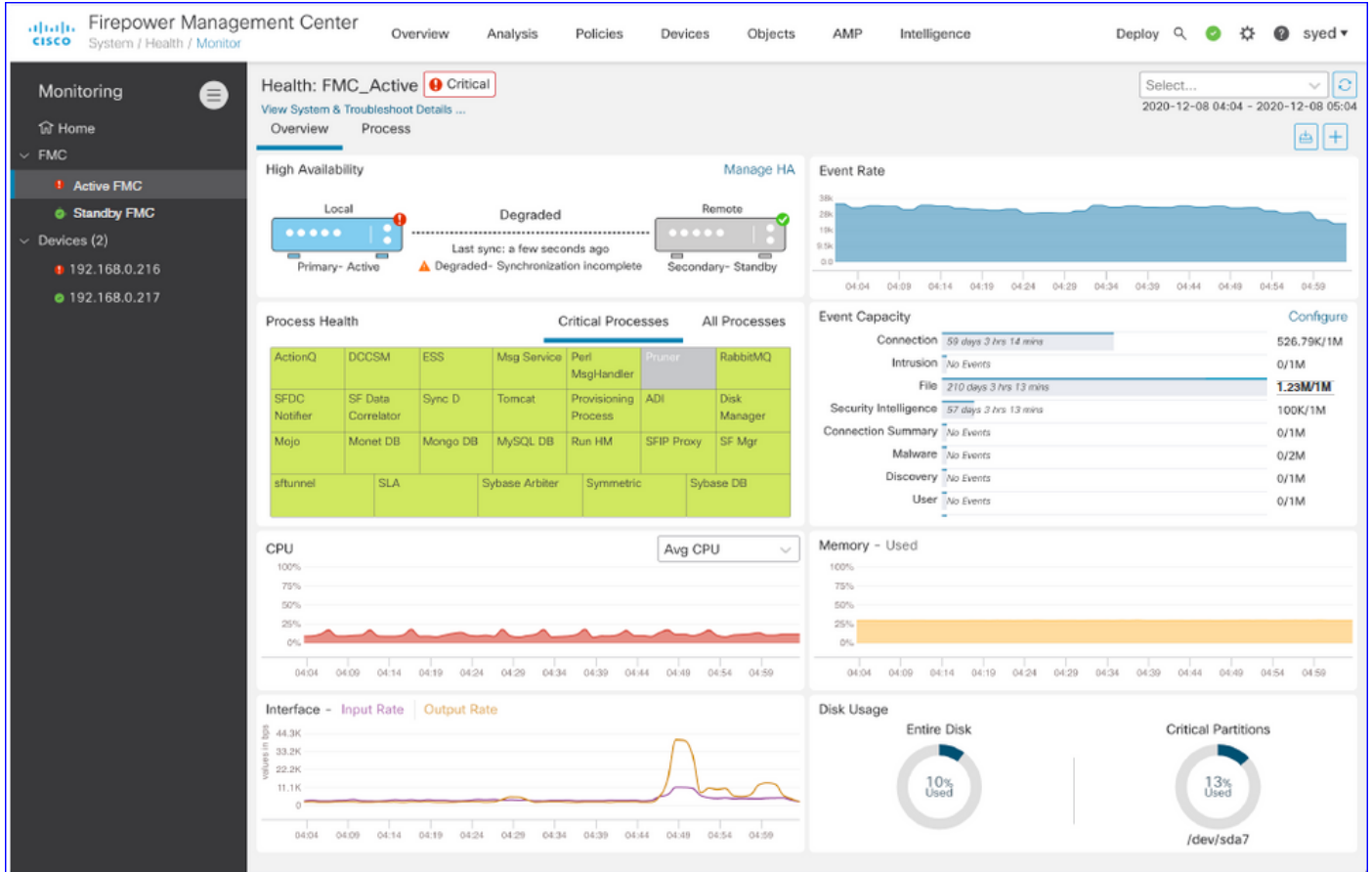
- FMC autonomo visualizzato come nodo singolo
- FMC HA visualizzato come coppia di nodi
- Ogni CCP è indicato con lo stato di salute

## Stato integrità

- 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

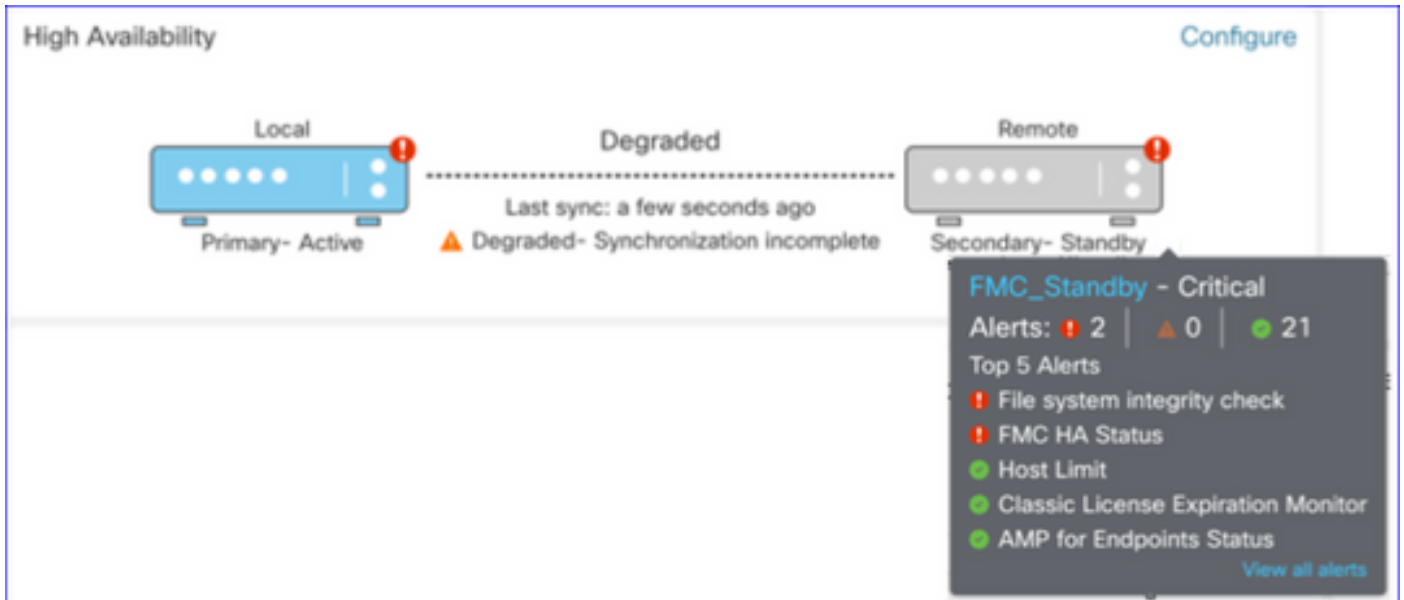


### Visualizzazione di riepilogo di:

- 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



Il pannello HA mostra

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

Dashboard FMC: velocità e capacità degli eventi

Frequenza eventi

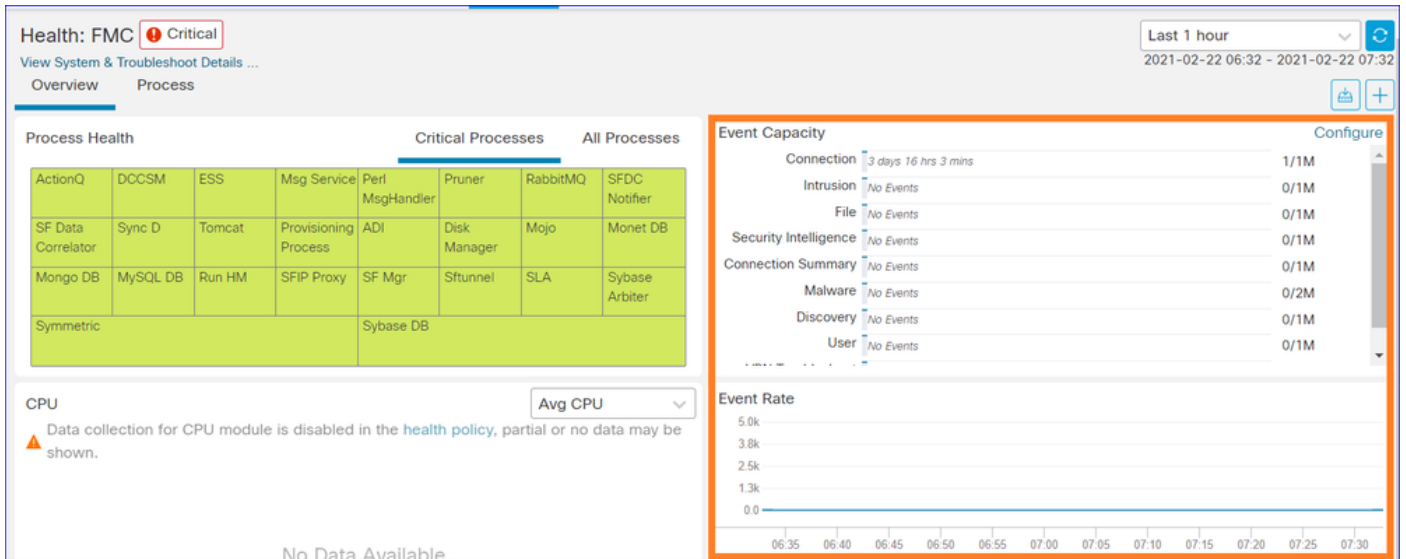
- Velocità evento massima come linea di base
- Frequenza eventi complessiva ricevuta da FMC

Capacità evento

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

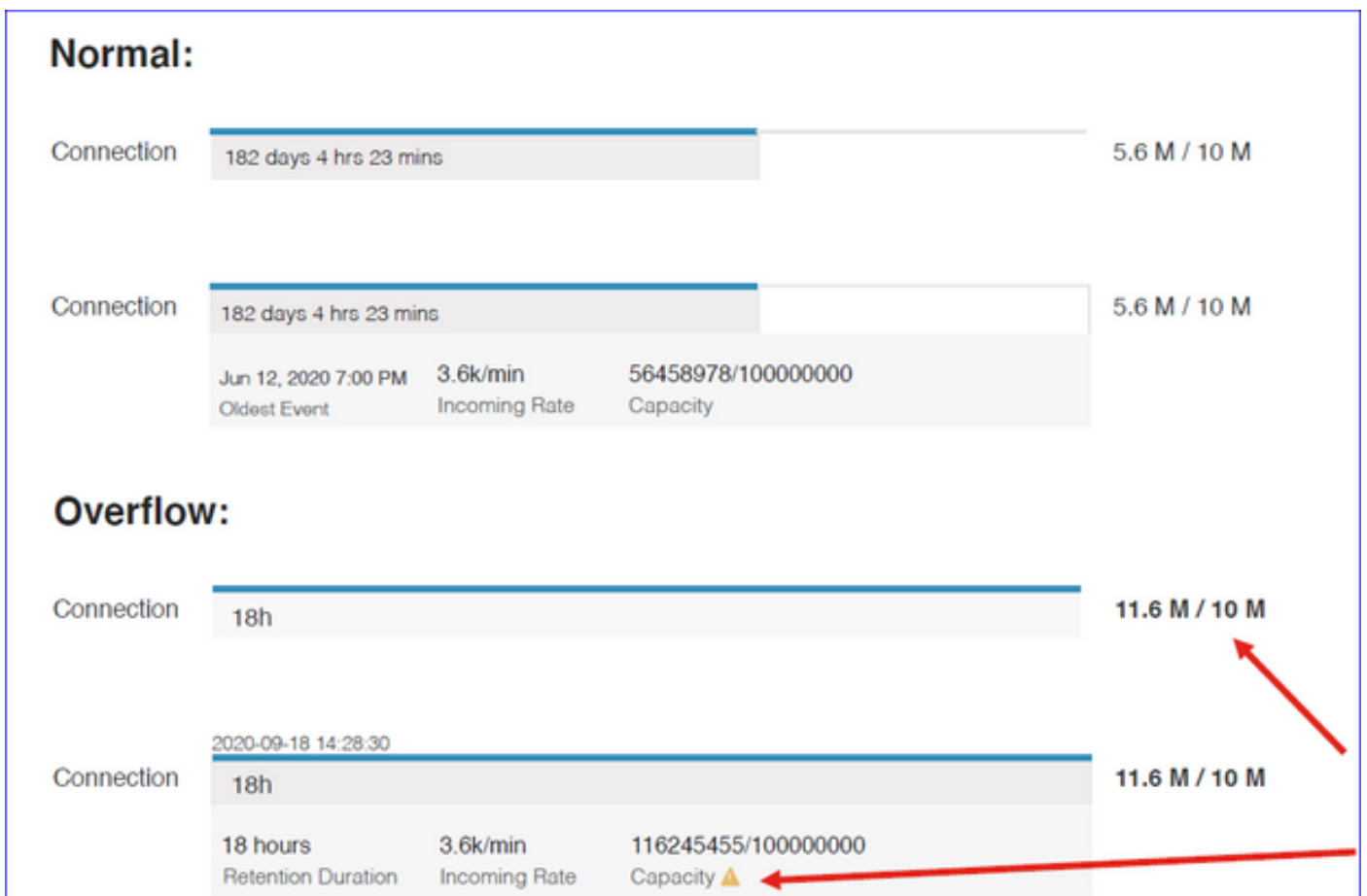
capacità evento

- Indicatore di overflow della capacità



Dashboard FMC: capacità evento

Stato consumo capacità evento normale



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

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	

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

- Stato corrente
- Utilizzo CPU
- Utilizzo memoria

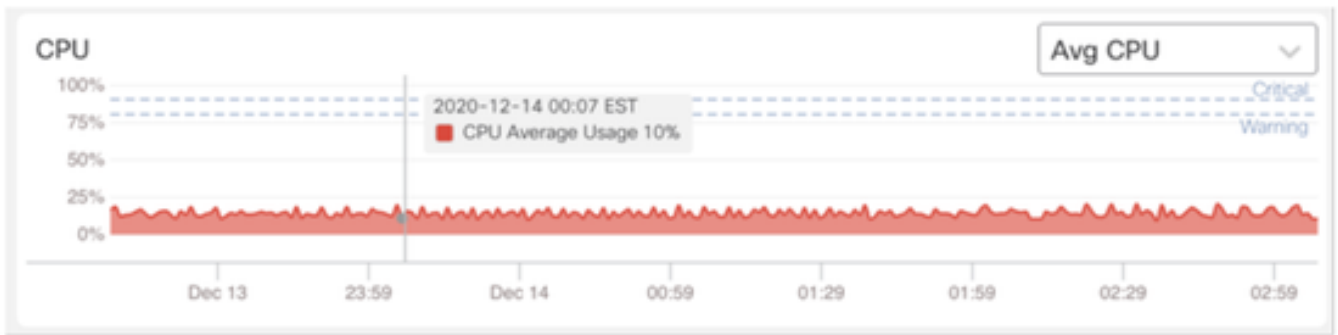
Process Health		Critical Processes		All Processes
Process status at: Dec 14, 2020 3:22 AM				
Process *	Status	CPU (%)	Mem Used	
ActionQ	Running	0	66.23KB	
CSD App	Waiting	0	0	
CSM Event Server	Running	0.6	182.1KB	
CloudAgent	Running	0.9	12.03KB	
DCCSM	Running	0	104.49KB	
ESS	Running	0.1	448.26KB	
Event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

Dashboard FMC: CPU FMC

Il pannello CPU mostra

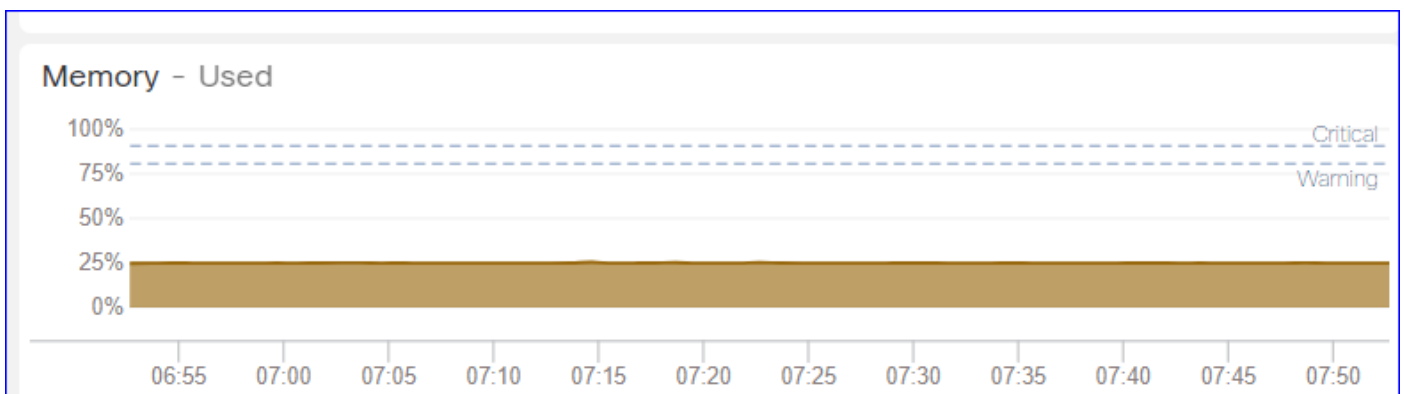
- CPU media (predefinita)
- Tutti i core



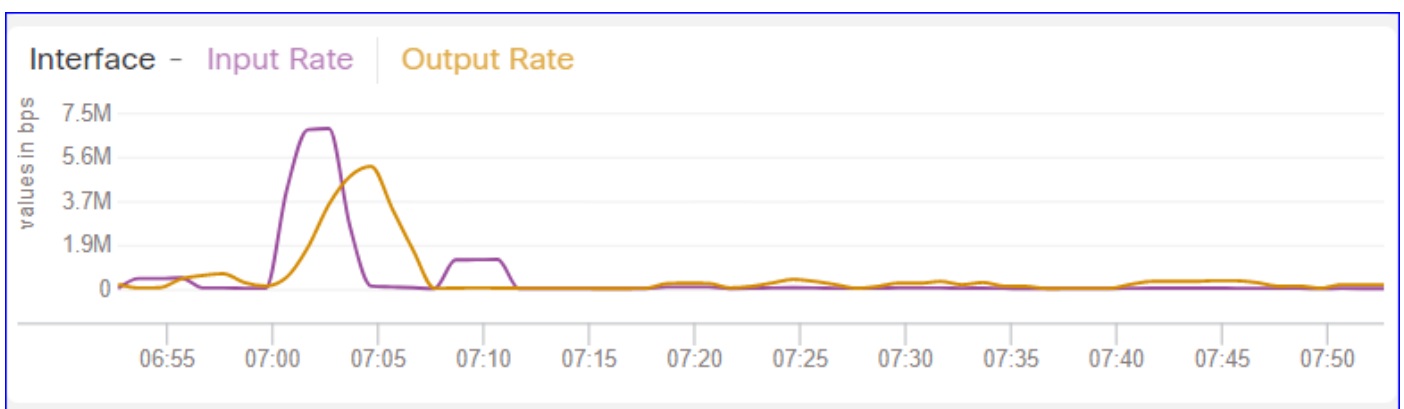


Dashboard di FMC: altri pannelli

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

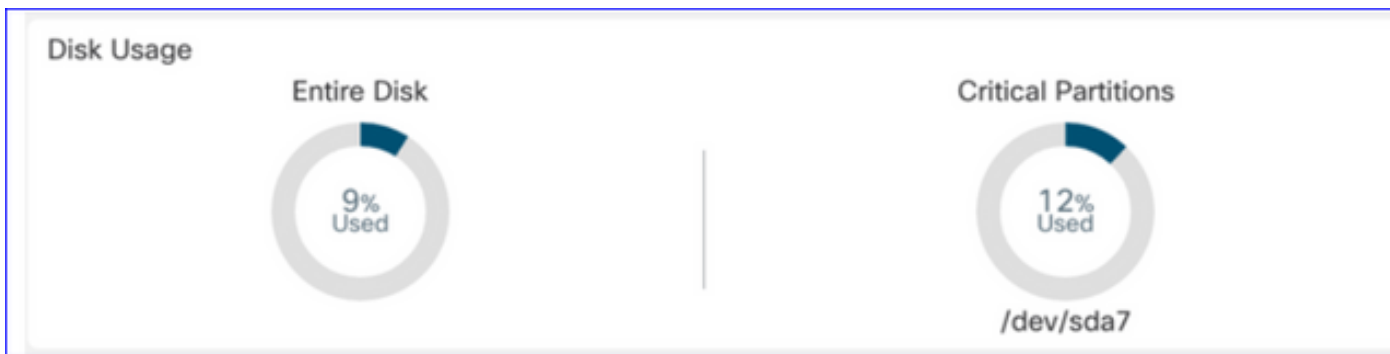


Il pannello Interfaccia mostra la velocità di ingresso/uscita della media di tutte le interfacce



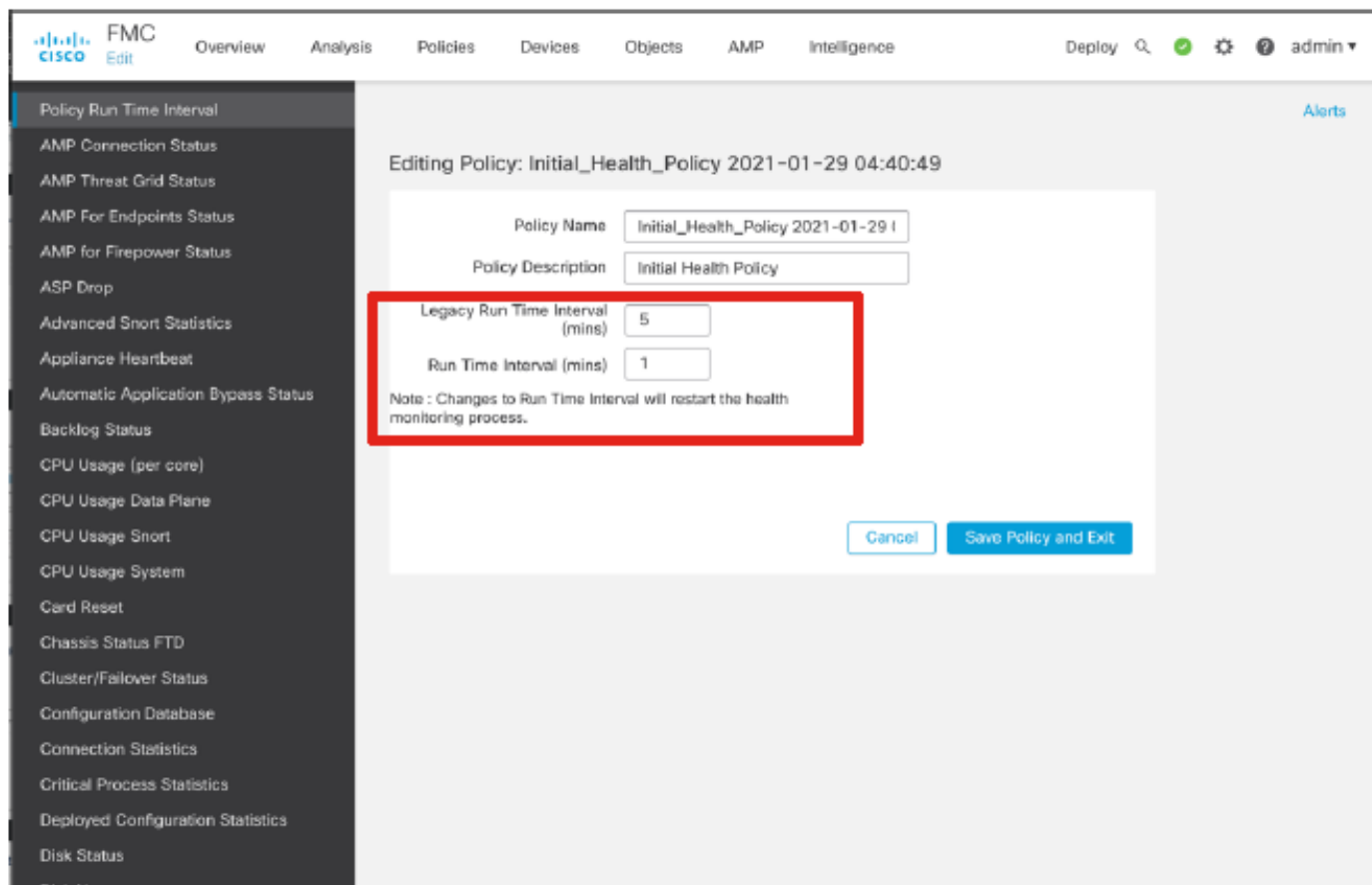
Il pannello Disco mostra

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



### 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

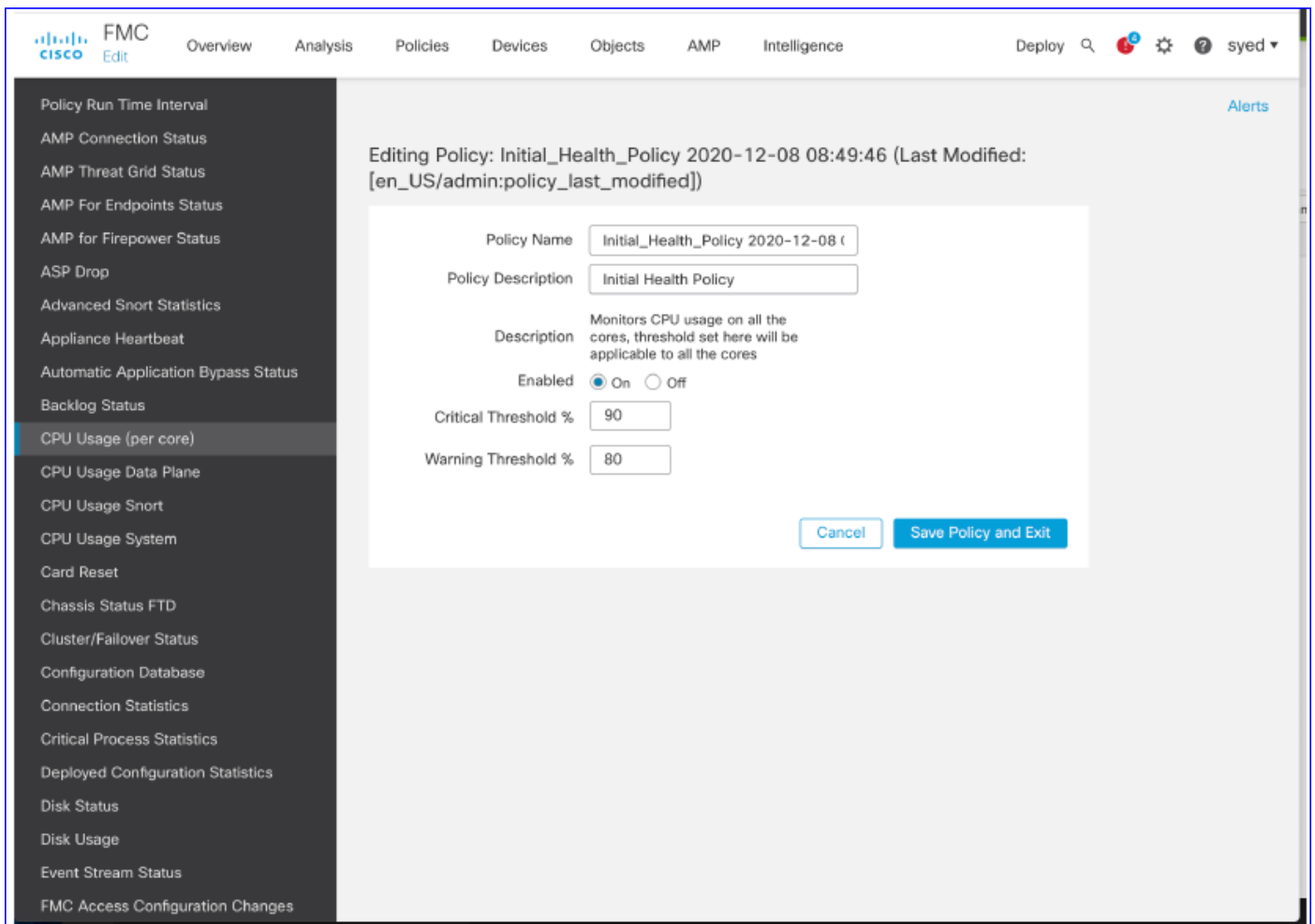


### Metriche disponibili

#### Metriche disponibili per dashboard personalizzati

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

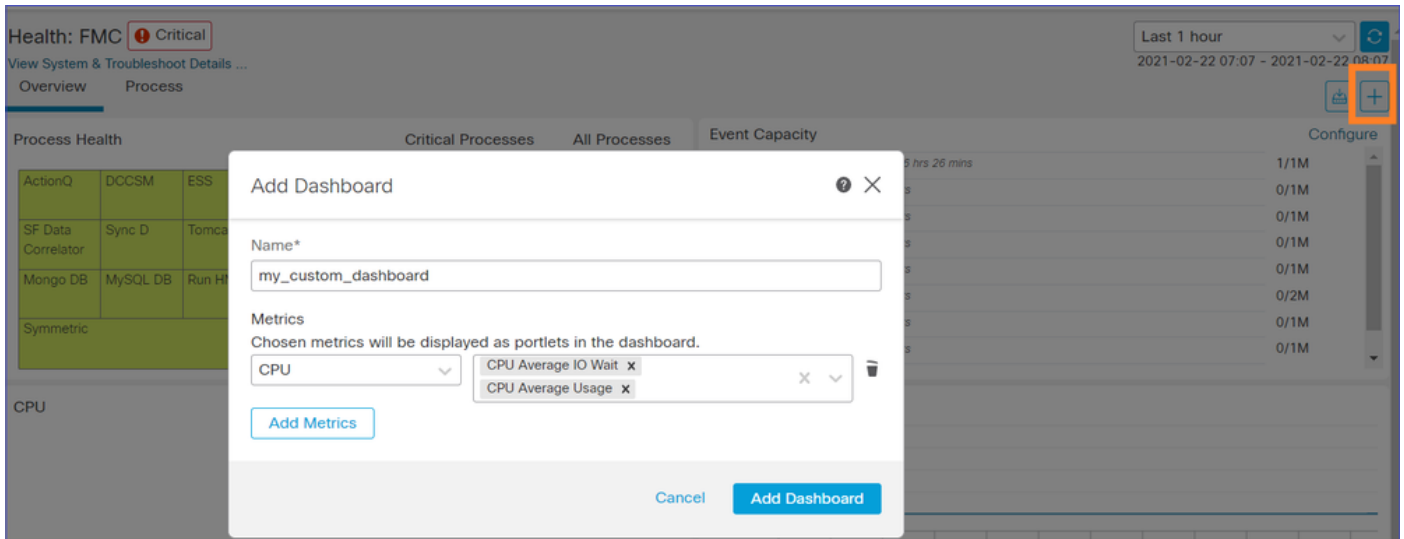
- È necessario abilitare alcune metriche nei criteri di integrità prima di poterle utilizzare in un dashboard di integrità personalizzato



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



## 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 linea	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.

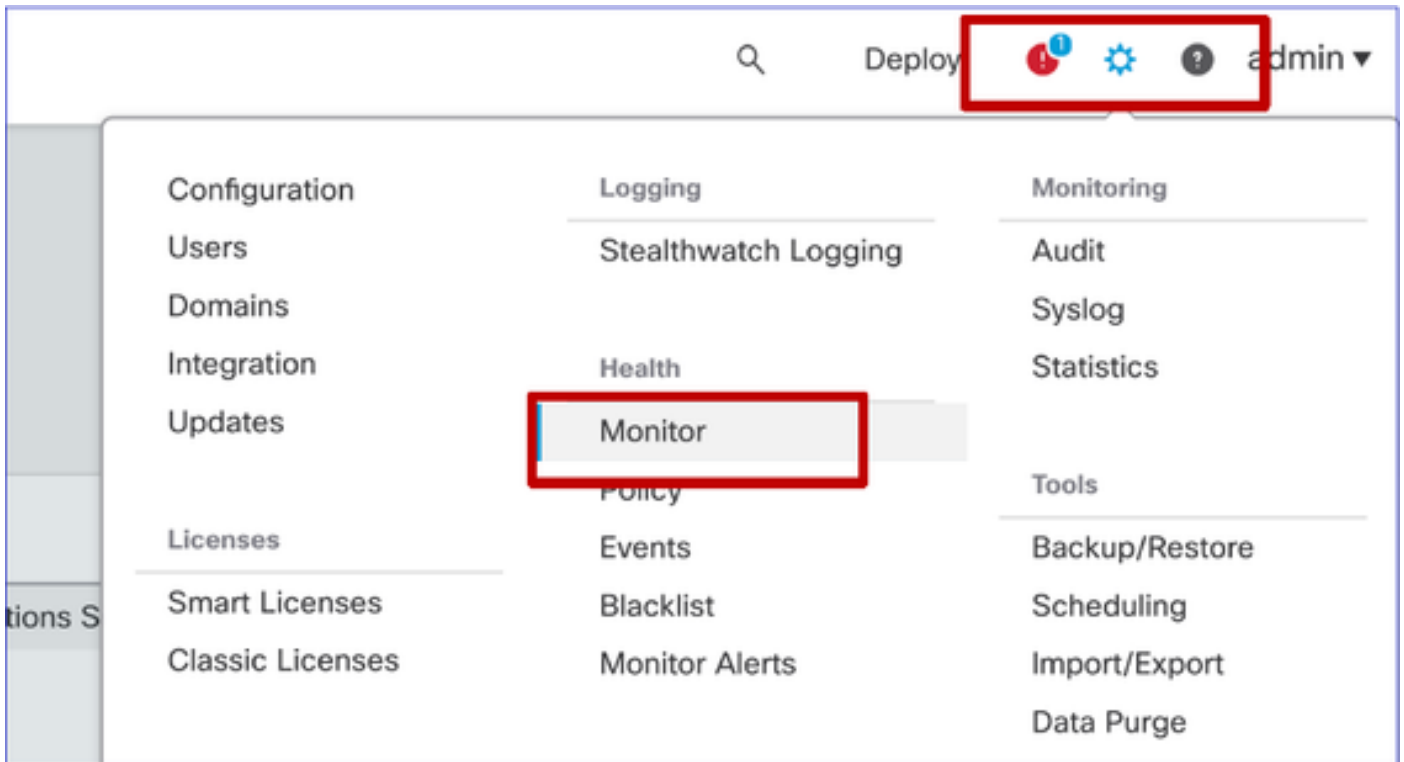
Caratteristiche

- 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.

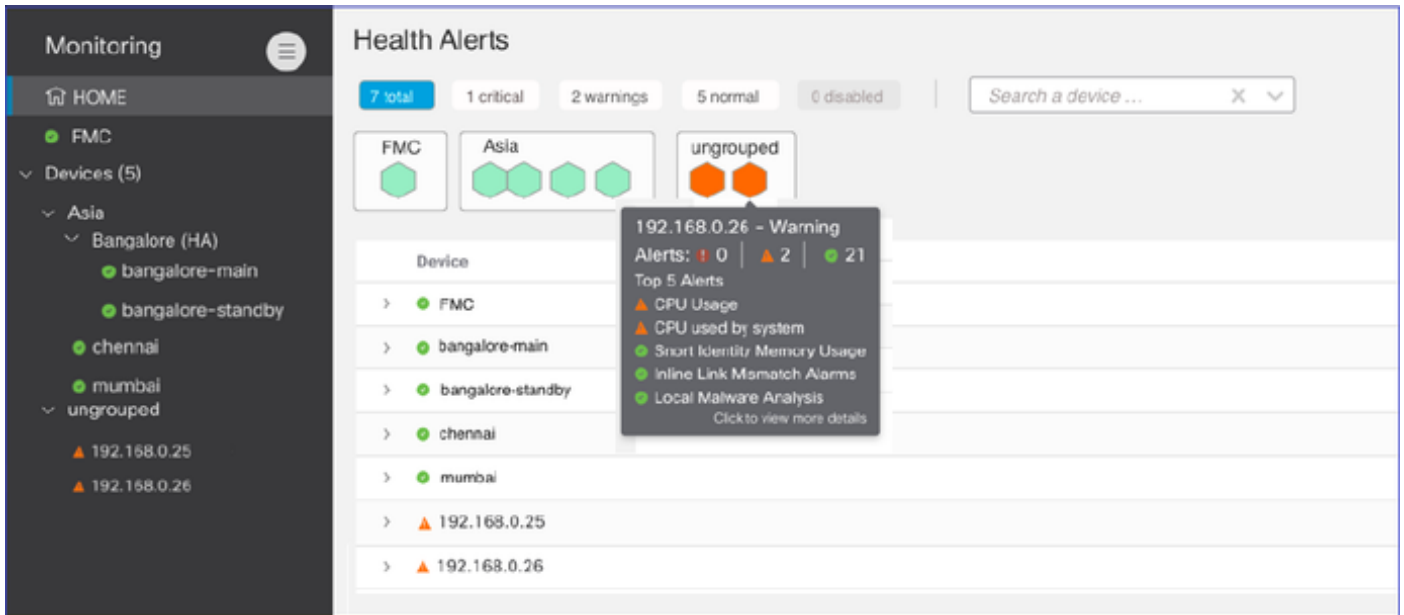


Interfaccia utente FMC: pagina Nuovo stato integrità

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.

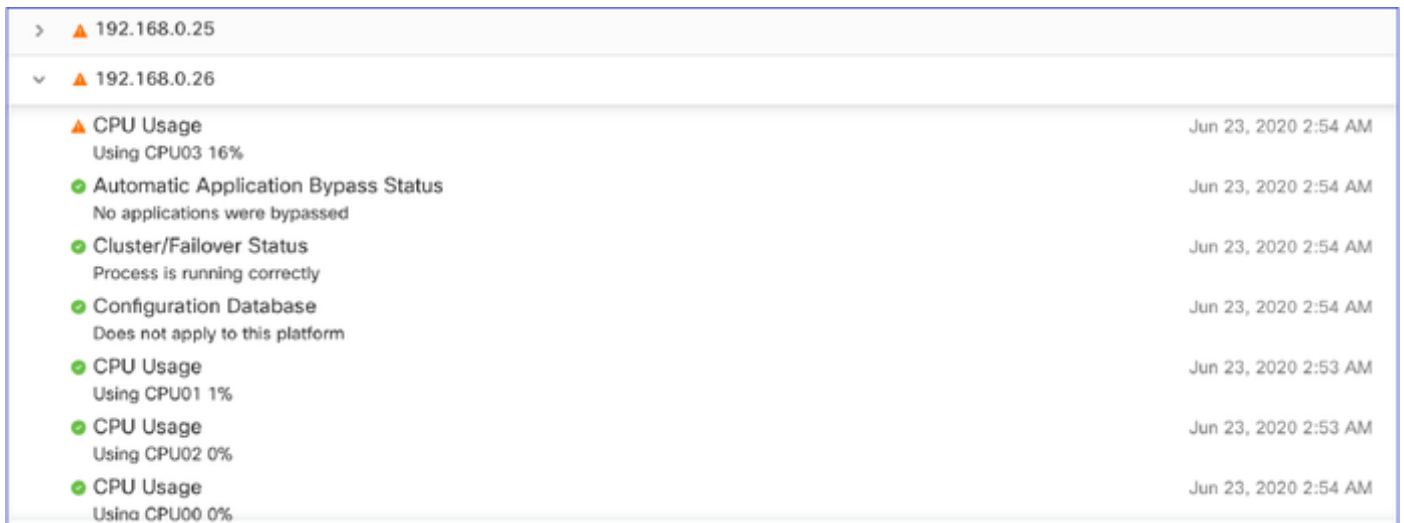




### Interfaccia utente di FMC: eventi di integrità del dispositivo

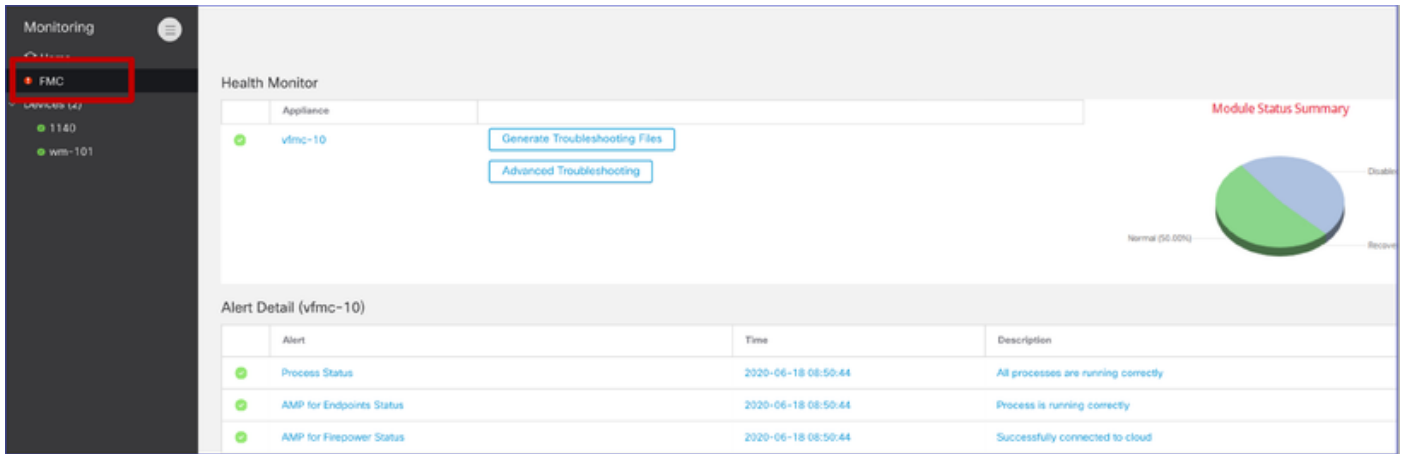
Fare clic sul dispositivo nel pannello inferiore per visualizzare gli eventi di stato associati al dispositivo. Gli avvisi vengono ordinati in base allo stato di salute (gravità).

### Pagina Monitoraggio stato



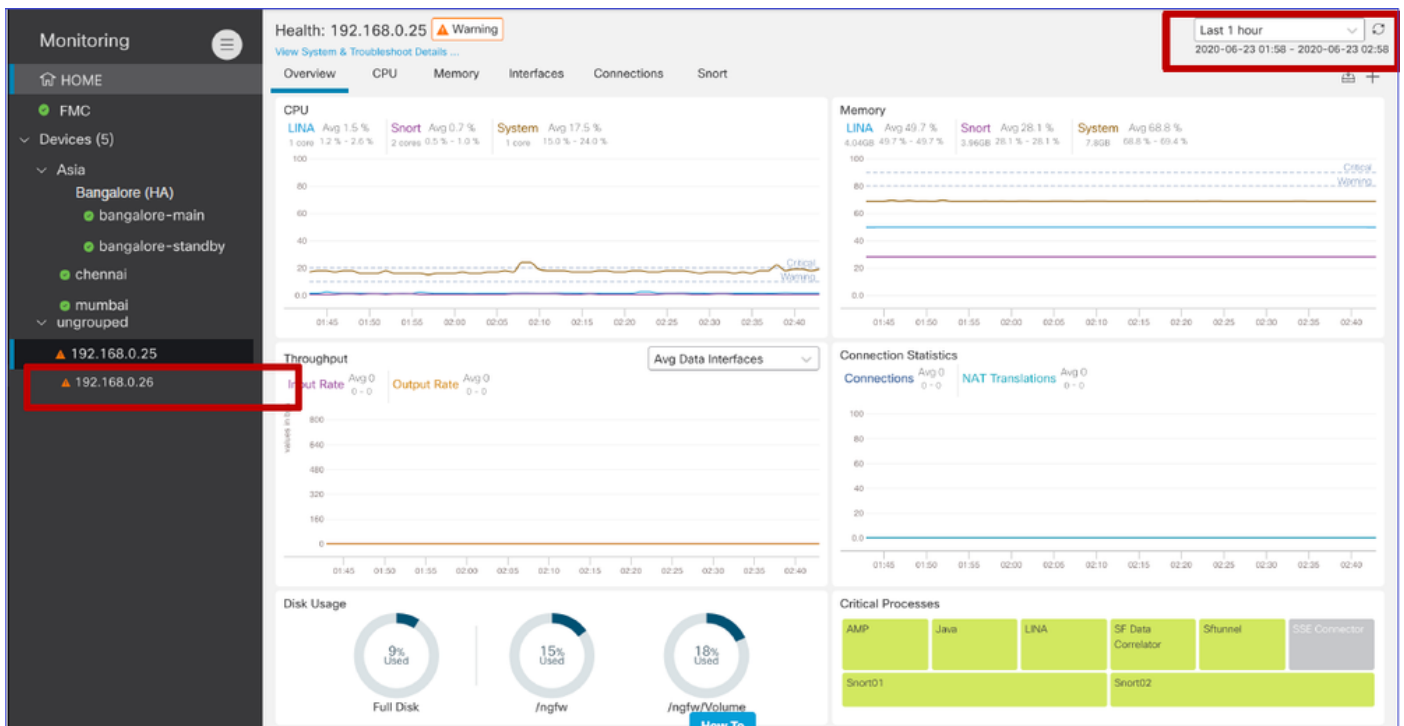
### Interfaccia utente FMC: monitoraggio stato FMC non modificato

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+



## 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



## Interfaccia utente di FMC: overlay dei dati di distribuzione

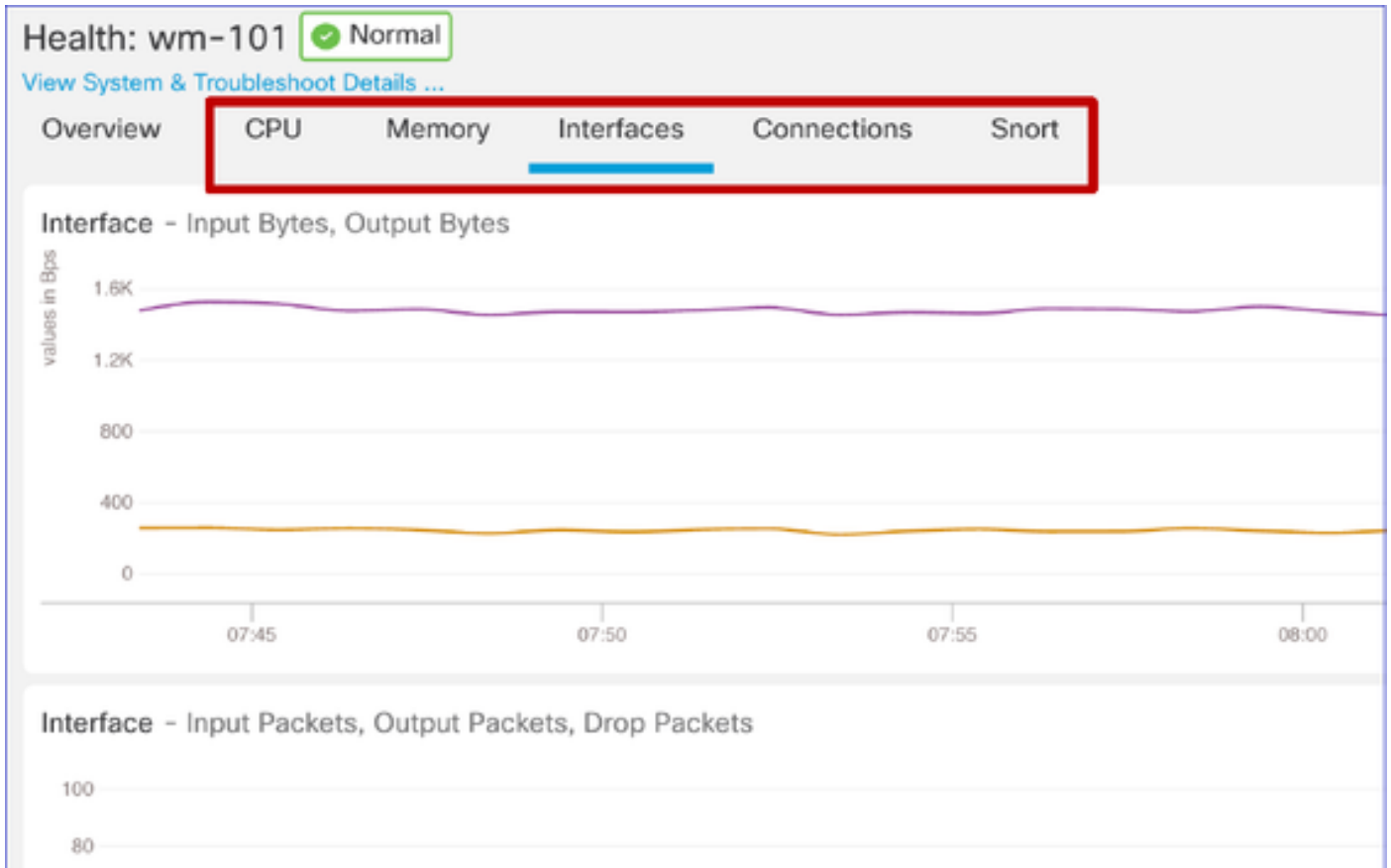
Fare clic sull'icona di distribuzione per visualizzare i dettagli della sovrapposizione di distribuzione nel grafico relativo all'intervallo di tempo selezionato

- 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

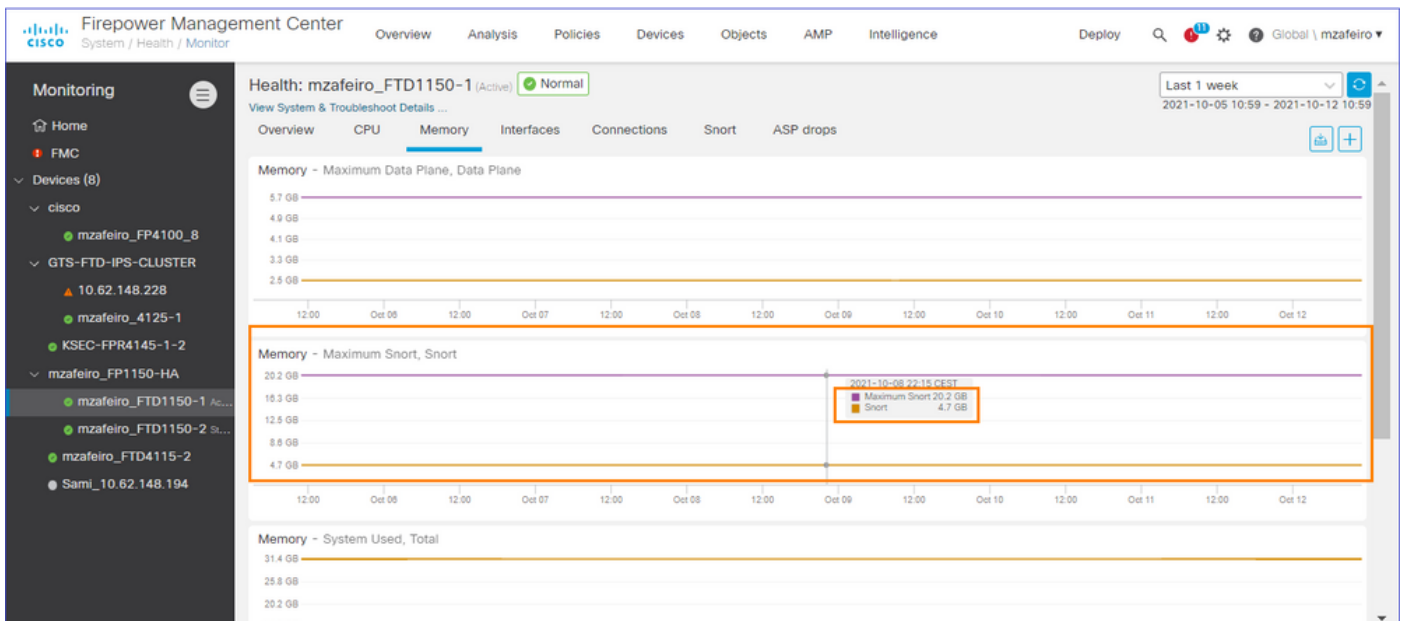


## Interfaccia utente di FMC: dashboard predefiniti del dispositivo

- 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.



FTD Snort Memory - Da dove ha origine?

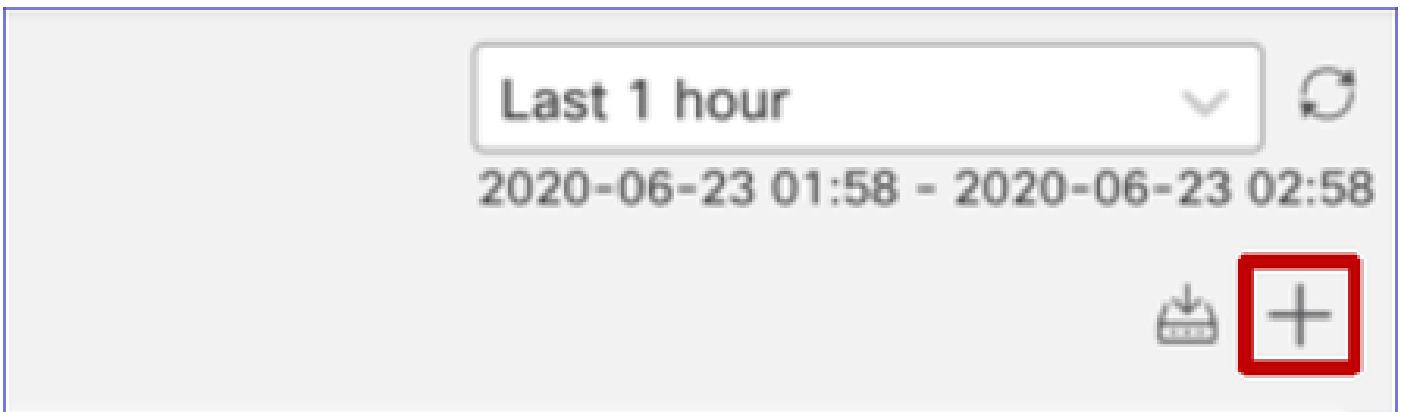


Interfaccia utente di FMC: è possibile creare dashboard personalizzati

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 ▼

[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>	<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>	<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>	<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>	<span style="float: right;">🗑</span>

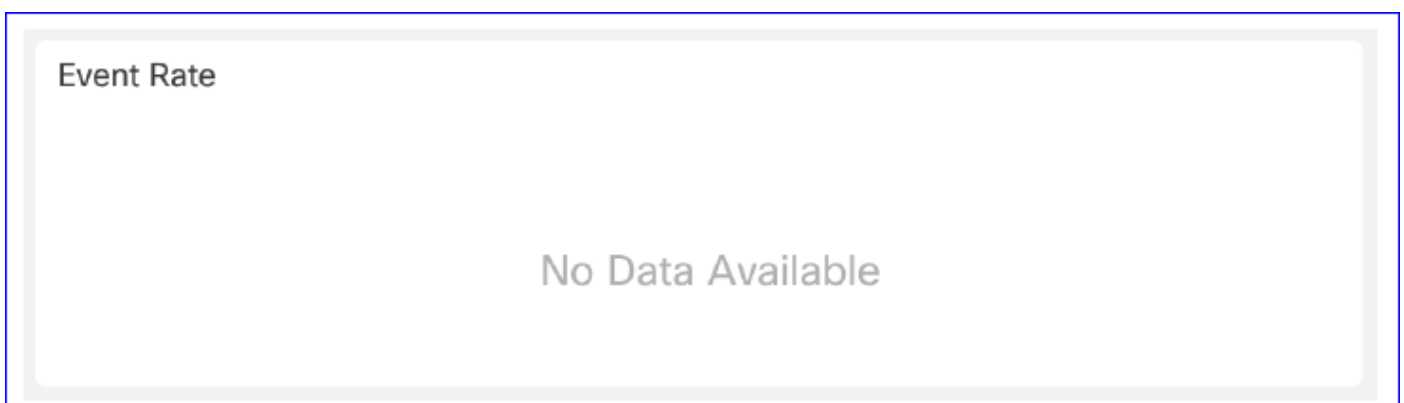
[Add Metrics](#)

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

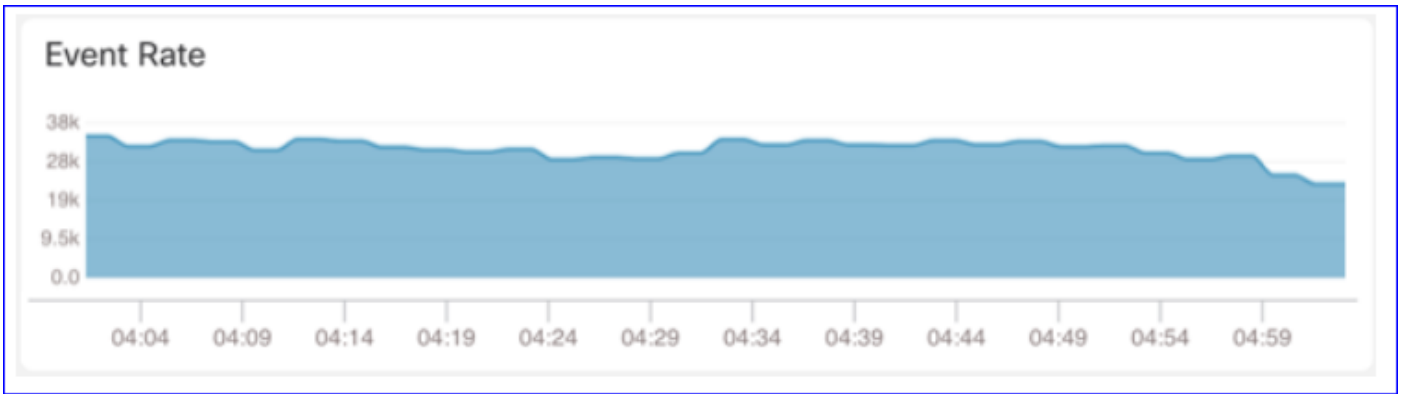
Raccolta dati da (dispositivo) - GUI

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:



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

The screenshot shows 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 panels: 'CPU' (Data Plane, Snort, System), 'Memory' (Data Plane, Snort, System), 'Throughput' (Input Rate, Output Rate), and 'Connection Statistics' (Connections, NAT Translations). Below these panels is a browser console window showing a stack trace for an error in 'index.js:11'. The stack trace includes frames for 'FadeIn', 'Suspense', 'Root', 'application', 'MessageProvider', 'ToastProvider', 'FeatureFlagProvider', 'Router', 'InputModeProvider', 'IntegrationProvider', 'ThemeProvider', 'ConnectFunction', 'IntlProvider', 'LocaleProvider', 'Provider', 'ReactQueryCacheProvider', 'QueryCacheProvider', and 'StrictMode'.

Esempio di registro della console del browser

Console Tab

Exception details



## 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).