FP-Upgrade - Gerätezustandsüberwachung

Inhalt

Einleitung

In diesem Dokument wird die neue Funktion zur Überwachung der Geräteintegrität beschrieben, die in Version 6.7 und 7.0 hinzugefügt wurde.

Hintergrundinformationen

Migration von:

https://confluence-eng-rtp2.cisco.com/conf/display/IFT/Change+Management+FP+7.0

https://confluence-eng-rtp2.cisco.com/conf/pages/viewpage.action?spaceKey=IFT&title=Device+Health+Monitoring

Das Problem:

Das Systemüberwachungssystem bietet Einblick in die Geräteleistung für reaktives Debuggen und proaktive Aktionen.

Umfassende Transparenz und Analyse wird erzielt durch:

- Trenddiagramme für wichtige Kennzahlen
- Ereignis-Overlay
- Anpassbare Dashboards
- Einheitliche Architektur für die Systemüberwachung - gleiche Daten für alle Manager anzeigen
- Viele neue Kennzahlen und Erweiterbarkeit von Kennzahlen, um viele weitere hinzuzufügen

Neuerungen in Version 7.0

Neuerungen oder Unterschiede gegenüber FP 7.0

- FMC-Dashboard mit HA-Unterstützung
- Mehr als 110 neue Kennzahlen für FTD
- Gesundheitswarnung für FTD Split Brain Szenario
- Benutzerdefiniertes Laufzeitintervall für neuere Integritätsmetriken

Vorteile

- Hilft beim Debuggen von Systemen, indem Daten aus verschiedenen Subsystemen und Ressourcen auf Geräten korreliert werden können
- Transparenz für verschiedene Systemleistungsmetriken
- Kapazitätsplanung

Neu bei 6.7

Neu oder anders als die unmittelbar vorangehende Version (allgemein):

- Neue Benutzeroberfläche für die Überwachung des Gerätestatus auf dem FMC
- FTD Device REST API: Device-Metrik API: Viele neue Metriken hinzugefügt
- FMC-APIs: Neue APIs: Integritätswarnungen, Integritätsmetriken und Bereitstellungsdetails
- Allgemeiner Überblick über den Marktplatz, reale Anwendungen
- Hilft beim Debuggen von Systemen, indem Daten aus verschiedenen Subsystemen und Ressourcen auf Geräten korreliert werden können
- Transparenz
- Kapazitätsplanung

Funktionsüberblick

So funktioniert es

- Überwachung der Geräteintegrität in FP 7.0
- Neues Health Dashboard für FMC mit Trenddiagrammen, Overlays und benutzerdefinierten Dashboards
- Neue FTD-Kennzahlen in FTD-Dashboards verfügbar
- Über 110 Kennzahlen für 12 Kategorien
- FTD-APIs: ermöglicht die Abfrage von Metriken durch externe Einheiten

Unter der Haube

- Erfasst den Zustand eines Geräts mit Telegraf (ein Open-Source-Framework zur Metriksammlung)
- Exportiert die Daten an FMC (mit Prometheus, das auf FMC läuft und angeschlossene Geräte abfragt)

Zusätzliche Hinweise

Systemüberwachungsdaten sind verfügbar

- Im FMC Health Dashboard, über das Systemmenü zugänglich (System > Health > Monitor)
- Von der FMC REST API
- Wenn das Gerät von FDM verwaltet wird, über die REST-API des FTD-Geräts

Einige Kennzahlen (FMC und FTD) sind standardmäßig deaktiviert.

- Integritätsmodule in der Integritätsrichtlinie müssen aktiviert und bereitgestellt werden, damit Metriken angezeigt werden.

Implementierung der von den IFTs des RP 6.7 angeforderten Verbesserungen

- Standardmäßig automatisch aktualisieren
- Filter mit benutzerdefiniertem Zeitbereich auf Dashboard
- Auswahl von Schnittstellen anhand des benutzerdefinierten Namens (sowie des physischen Schnittstellennamen) in der Schnittstellenauswahl
- Starten Sie das Geräte-Dashboard über die Startseite des Systemmonitors.

Überwachung des Gerätestatus in FP 6.7

- Neue Benutzeroberfläche auf FMC mit Trend-Diagrammen, Overlays und benutzerdefinierten Dashboards.
- FTD-APIs: Bereitstellung derselben Metriken für Abfragen durch externe Einheiten

Unter den Deckblättern:

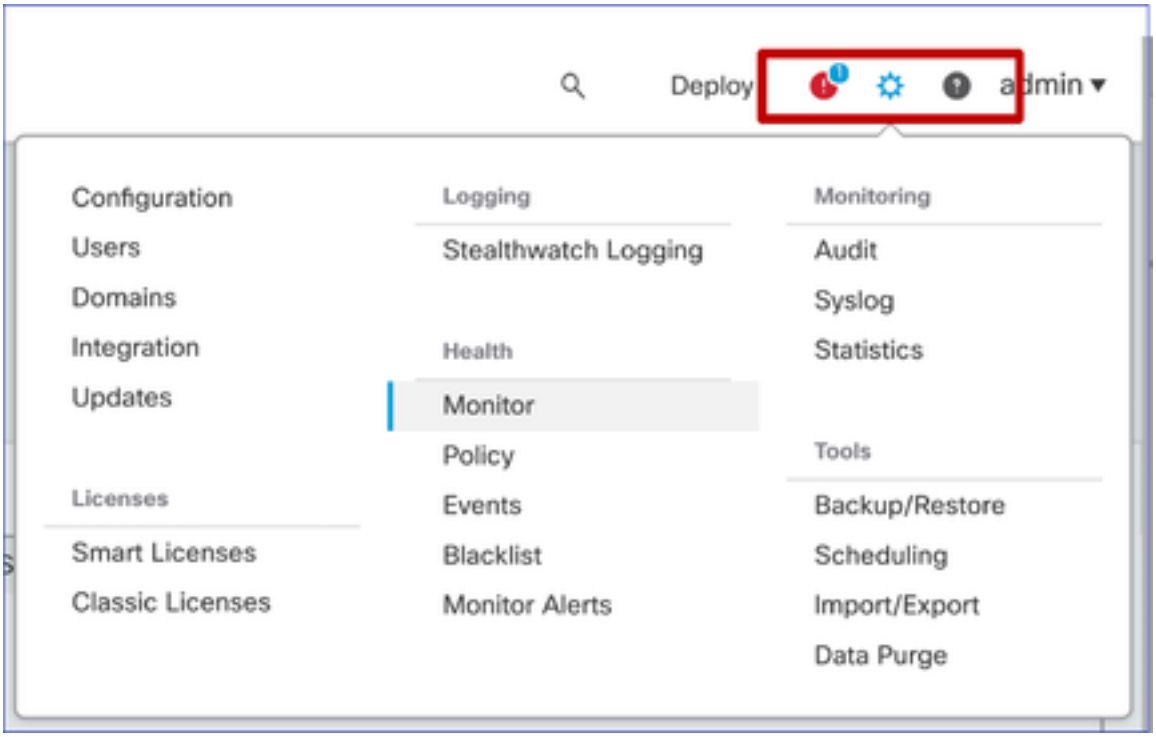
- Erfasst den Zustand eines Geräts mithilfe des Open-Source-Tools Telegraf.
- Exportiert die Daten in FMC (mithilfe der Open Source-Datenbank der Zeitreihe Prometheus, die auf FMC ausgeführt wird, indem alle Geräte eine Minute abgefragt werden).
- Manager: FMC, FMC REST API, FTD Device REST API

Zusammenfassung der Einschränkungen:

- Die Funktion wird auf der FDM-GUI oder CDO nicht unterstützt.
- Die Überwachung von FMC selbst innerhalb der neuen Benutzeroberfläche für die Systemüberwachung wird nicht unterstützt.
- Abfrageintervalle sind nicht konfigurierbar. Sie können keine unterschiedlichen Abfrageintervalle für verschiedene Geräte konfigurieren. Alle werden in einem festen Intervall von einer Minute abgefragt.

Bereitstellungsbeispiele

- Es ist keine spezielle Bereitstellung zum Testen der Funktion erforderlich. Aktualisieren Sie einfach FMC und Gerät auf FP 6.7.
- Die Statusüberwachungsdaten sind im FMC-Statusdashboard verfügbar, auf das Sie über die Systemregisterkarte zugreifen können.



Voraussetzungen und unterstützte Plattformen

Mindestanzahl unterstützter Software- und Hardwareplattformen

Min. unterstützte Manager-Version	Verwaltete Geräte	Min. unterstützte Version des verwalteten Geräts erforderlich	Hinweise
FMC 6.7	FTD 6.7	FXOS 2.9.1 FTD 6.7	Nur auf FTDs unterstützt
REST-API für FTD-Geräte	FTD 6.7	FXOS 2.9.1 FTD 6.7	Nur REST-API für FTD-Geräte (keine FDM- oder CDO-GUIs)

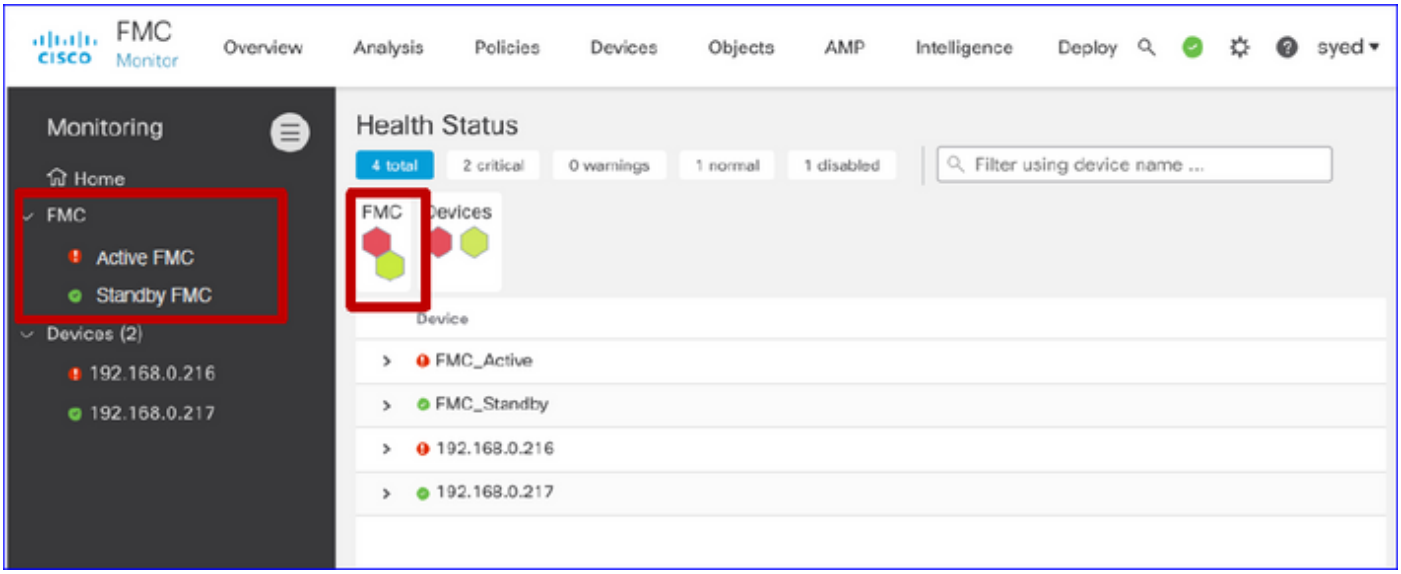
Interoperabilität

Keine spezifischen Anforderungen an die Interoperabilität.

Funktionsdetails 7.0

FMC-Benutzeroberfläche: Standalone und HA-Unterstützung

Navigation zur Seite "Systemüberwachung"



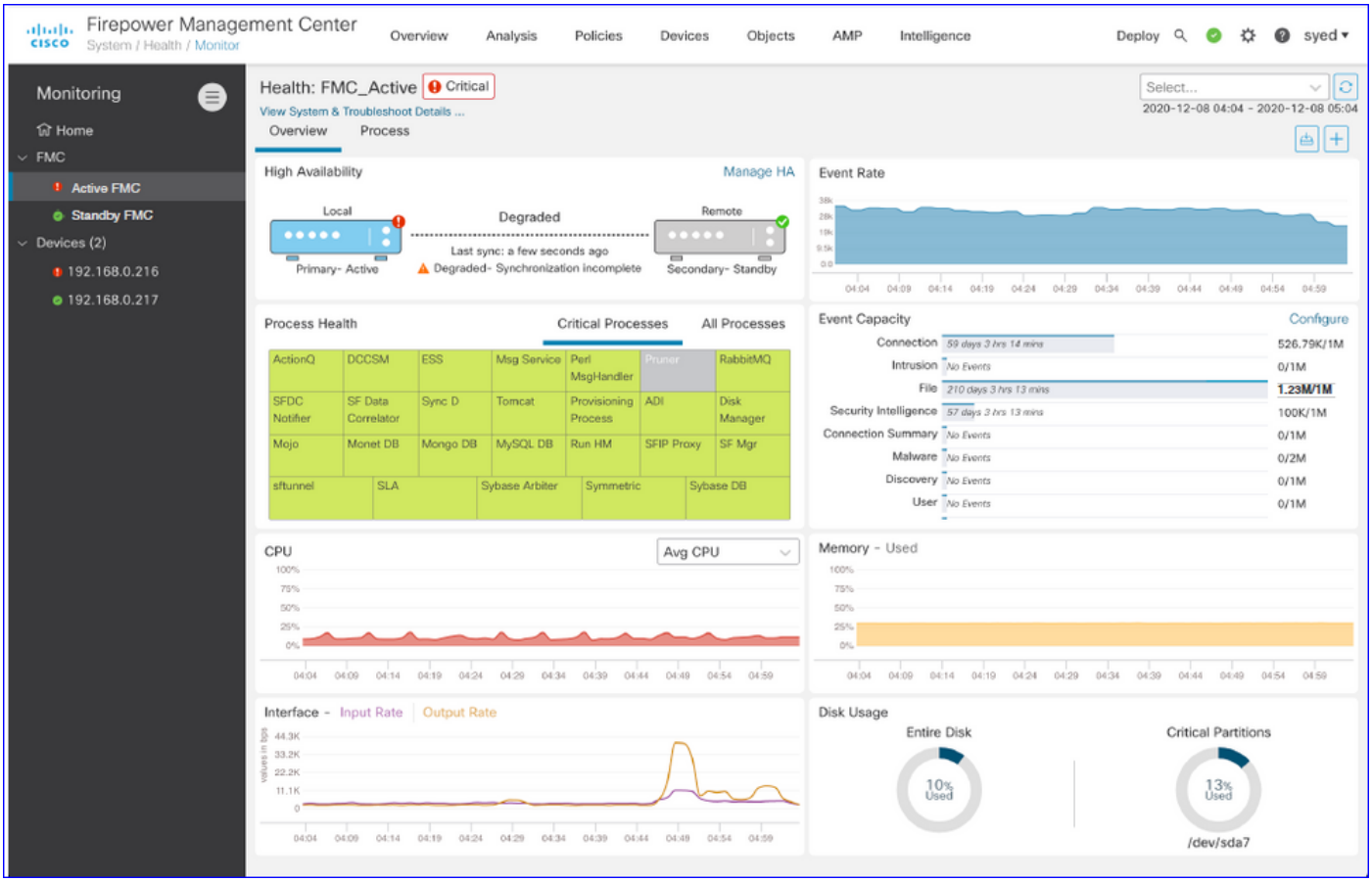
- Standalone-FMC wird als einzelner Knoten angezeigt
- FMC HA als Paar von Knoten dargestellt
- Für jedes FMC wird der Status "Health" angezeigt.

Integritätsstatus

- FMC HA ist in Doppelhexagonal dargestellt.
- Aktive und Standby-Geräte des FMC werden ebenfalls in der Warnmeldungstabelle aufgeführt.

FMC-Dashboard

FMC Health Monitoring Dashboard in 7.0



Zusammenfassende Ansicht von:

- Hohe Verfügbarkeit
- Ereignisrate und -kapazität
- Prozesssicherheit
- CPU
- Arbeitsspeicher
- Schnittstelle
- Festplatte

Dieses Dashboard ist für aktive und Standby-FMCs verfügbar. Benutzer können benutzerdefinierte Dashboards erstellen, um Metriken ihrer Wahl zu überwachen.

FMC-Dashboard: FMC HA-Panel

HA-Panel zeigt

- Aktueller HA-Status
- Aktiv und Standby
- Letzte Synchronisierungszeit
- Geräteintegrität

FMC-Dashboard: Ereignisrate und Kapazität

Ereignisrate

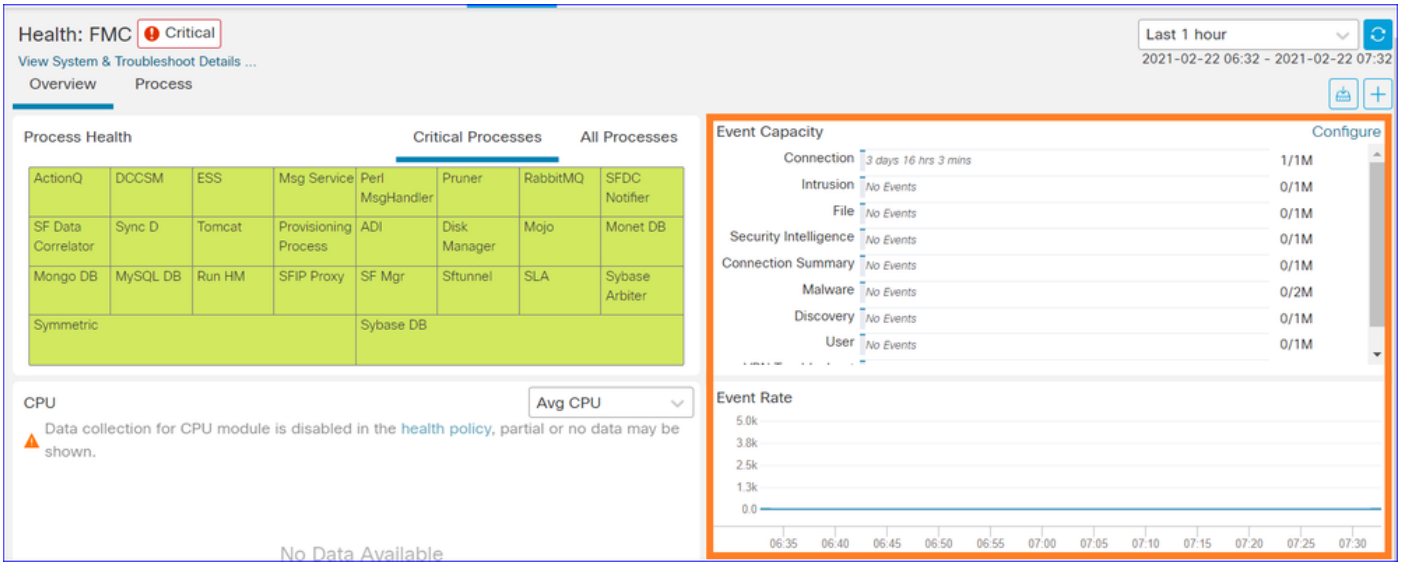
- Maximale Ereignisrate als Grundlinie
- Gesamtereignisrate, die FMC erhält

Event-Kapazität

- Stromverbrauch nach Ereigniskategorien
- Aufbewahrungszeit von Ereignissen
- Aktuell vs. Maximum

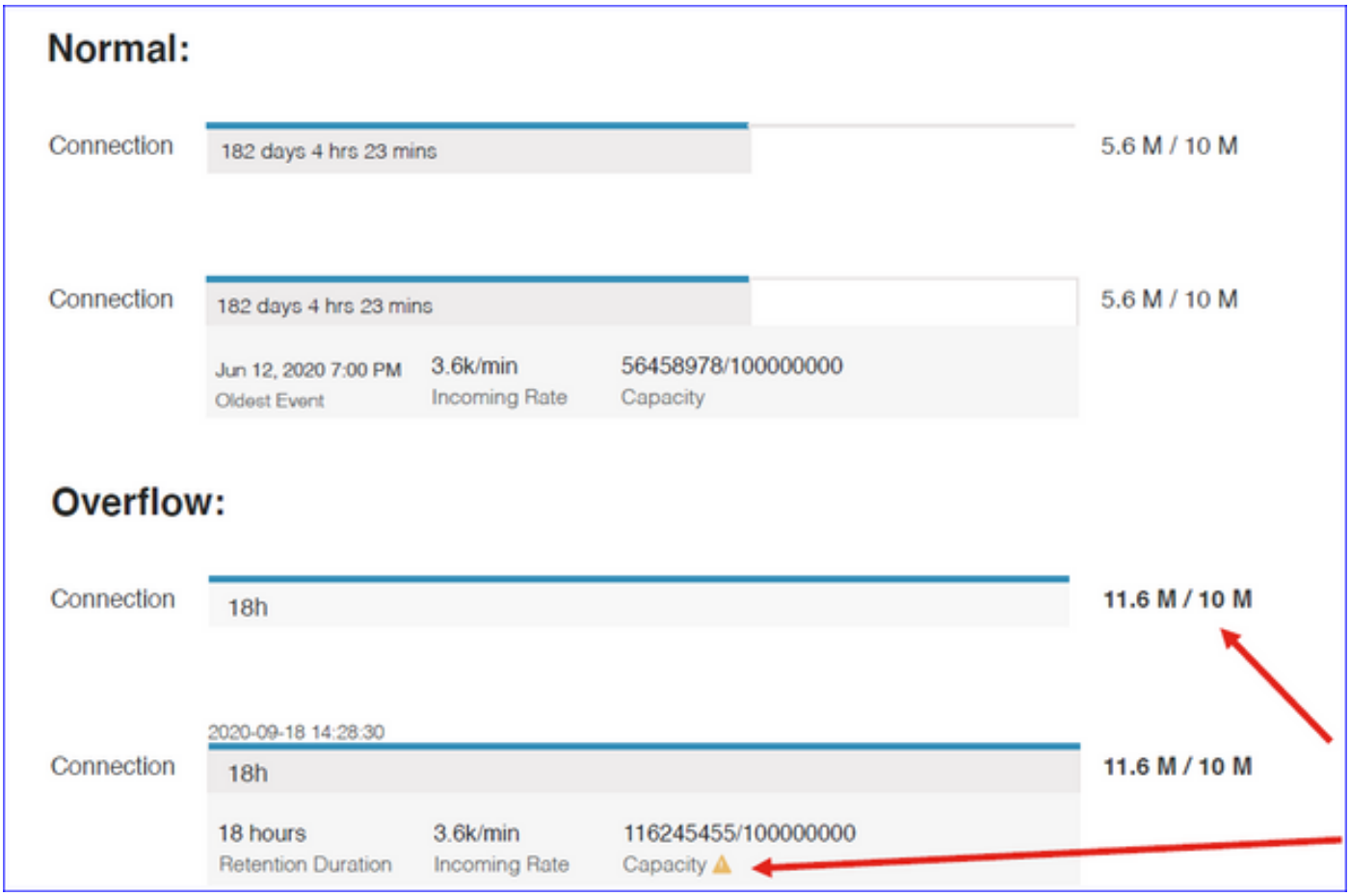
Ereigniskapazität

- Kapazitätsüberlaufmarkierung



FMC-Dashboard: Event-Kapazität

Normaler Kapazitätsverbrauchszustand bei Ereignissen



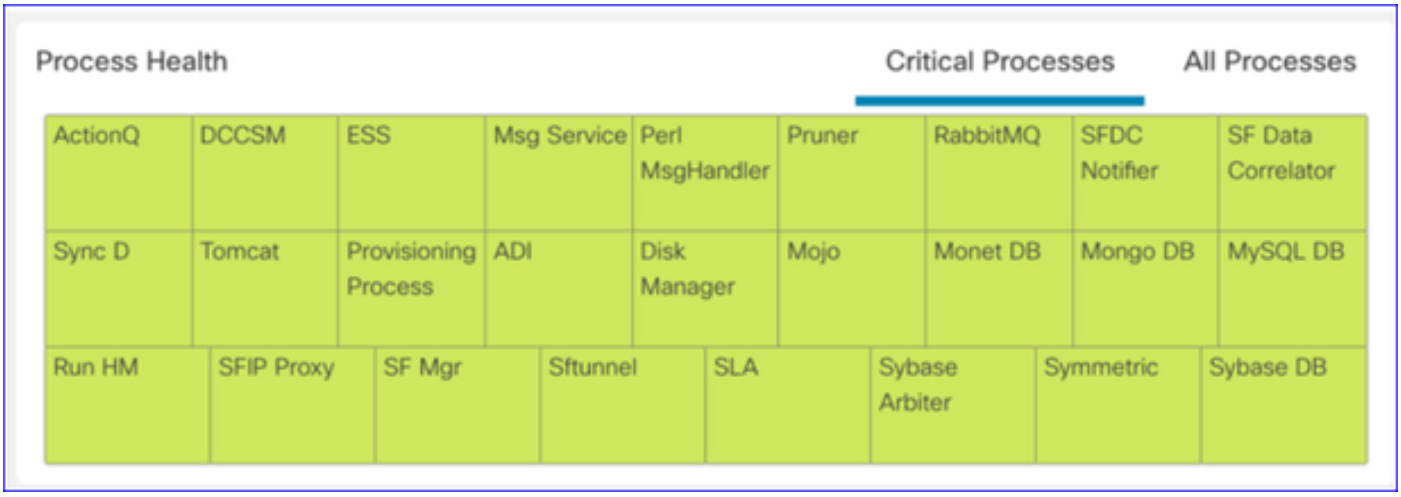
Überlaufszenario, wenn Ereignisse über die konfigurierte maximale Kapazität hinaus gespeichert werden.

- Fettformatierter Text weist auf Überlauf hin
- Ein Warnsymbol zeigt den Kapazitätsüberlauf an.

FMC-Dashboard: FMC-Prozess-Panel

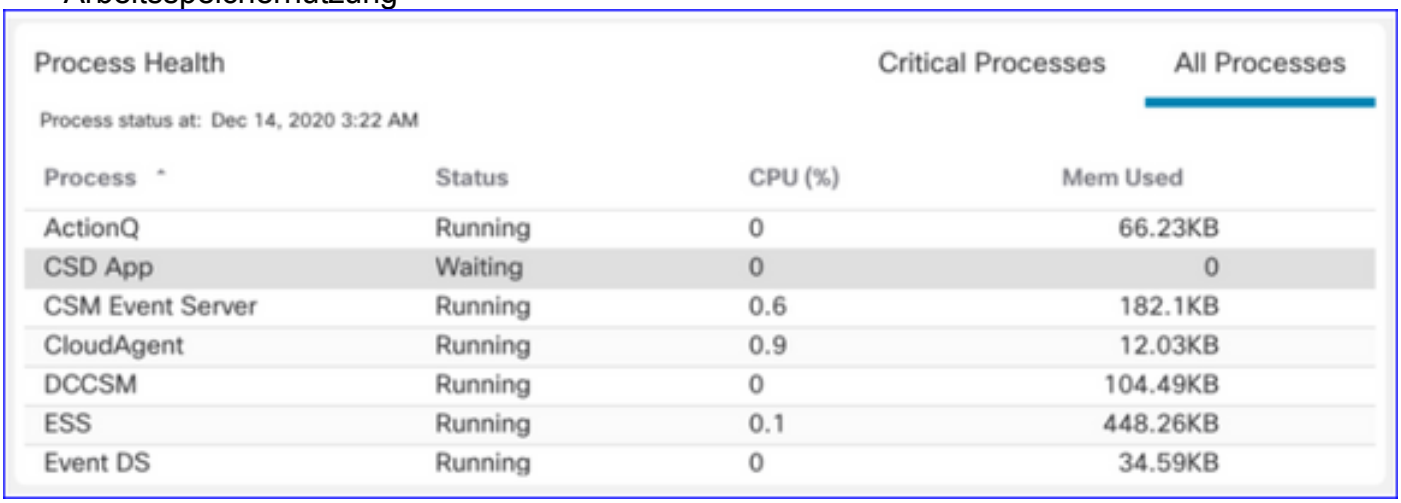
Anzeige "Kritische Prozesse"

- Aktuellen Status verarbeiten
- Anzahl der Prozessneustarts



Das Prozess-Panel zeigt die folgenden Metriken für alle "pmconfig"-Prozesse an:

- Aktueller Status
- CPU-Nutzung
- Arbeitsspeichernutzung



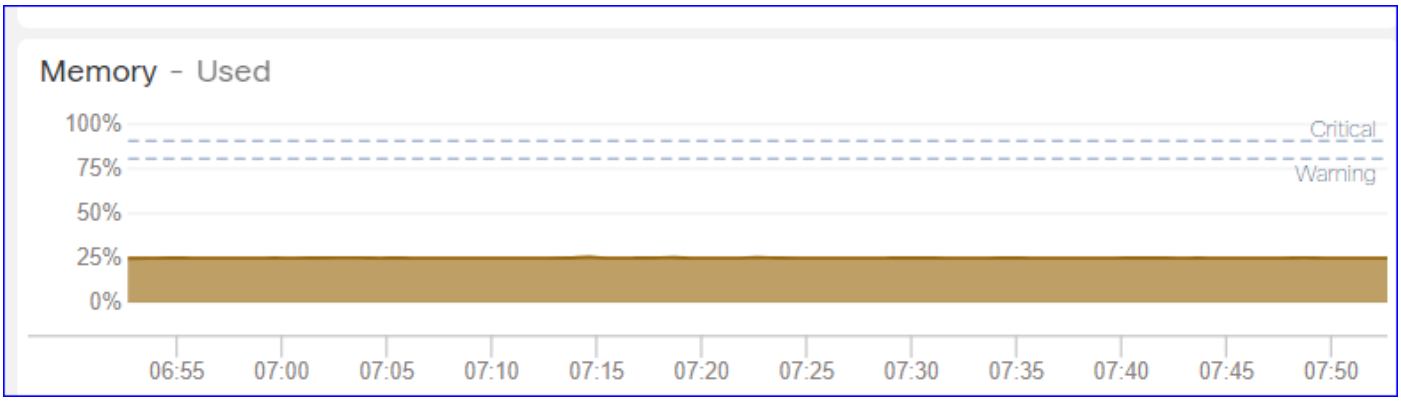
FMC-Dashboard: FMC-CPU

CPU-Anzeige

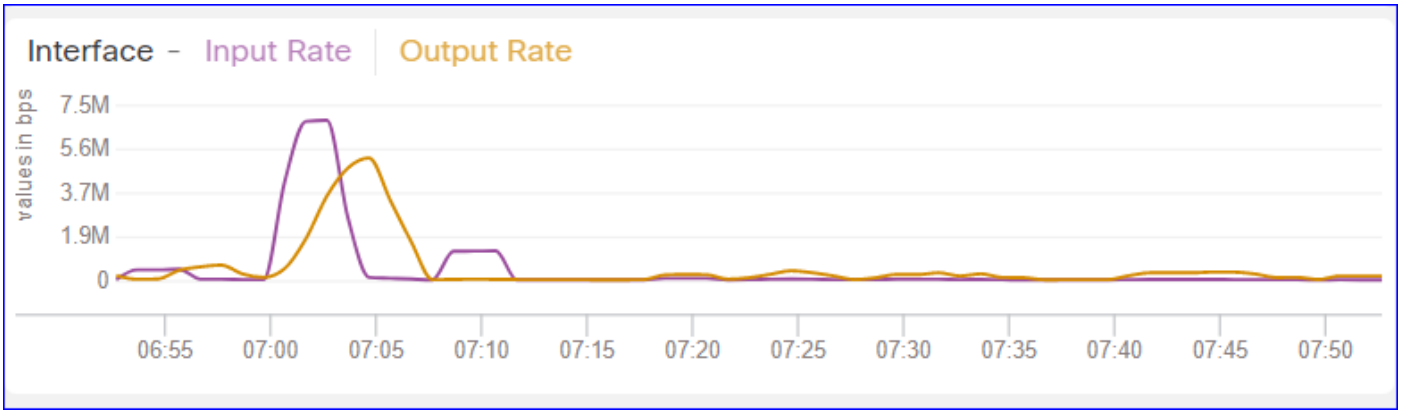
- Durchschnittliche CPU (Standard)
- Alle Kerne

FMC-Dashboard: Andere Bereiche

Speicherbereich zeigt die gesamte Speichernutzung auf FMC an



Schnittstellenanzeige zeigt die Ein-/Ausgaberate des Durchschnitts aller Schnittstellen an

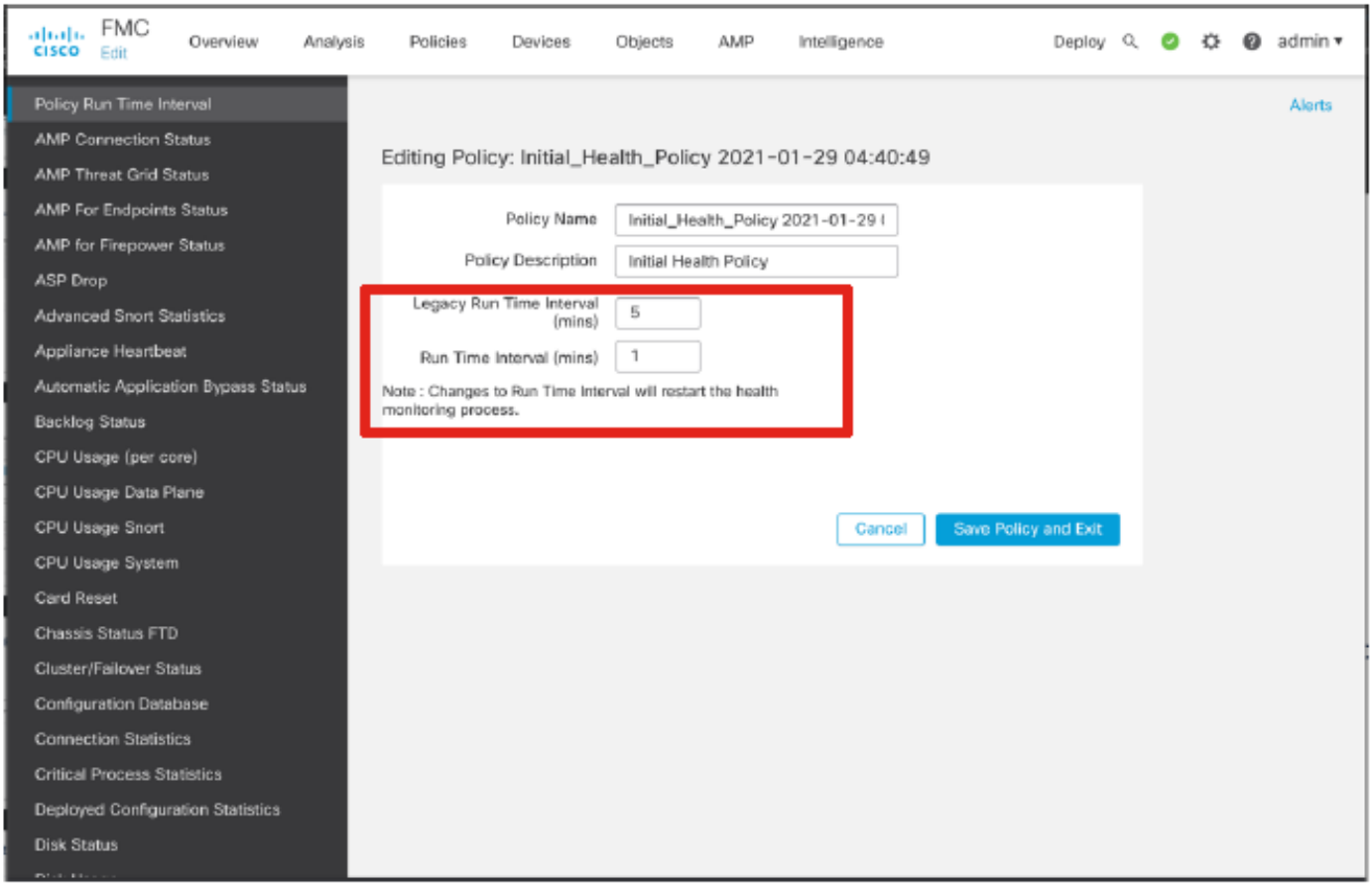


Das Datenträgerfeld wird angezeigt.

- Gesamte Festplattenkapazität
- Kritische Partitionskapazität, in der FMC-Daten gespeichert werden

Laufzeitintervall

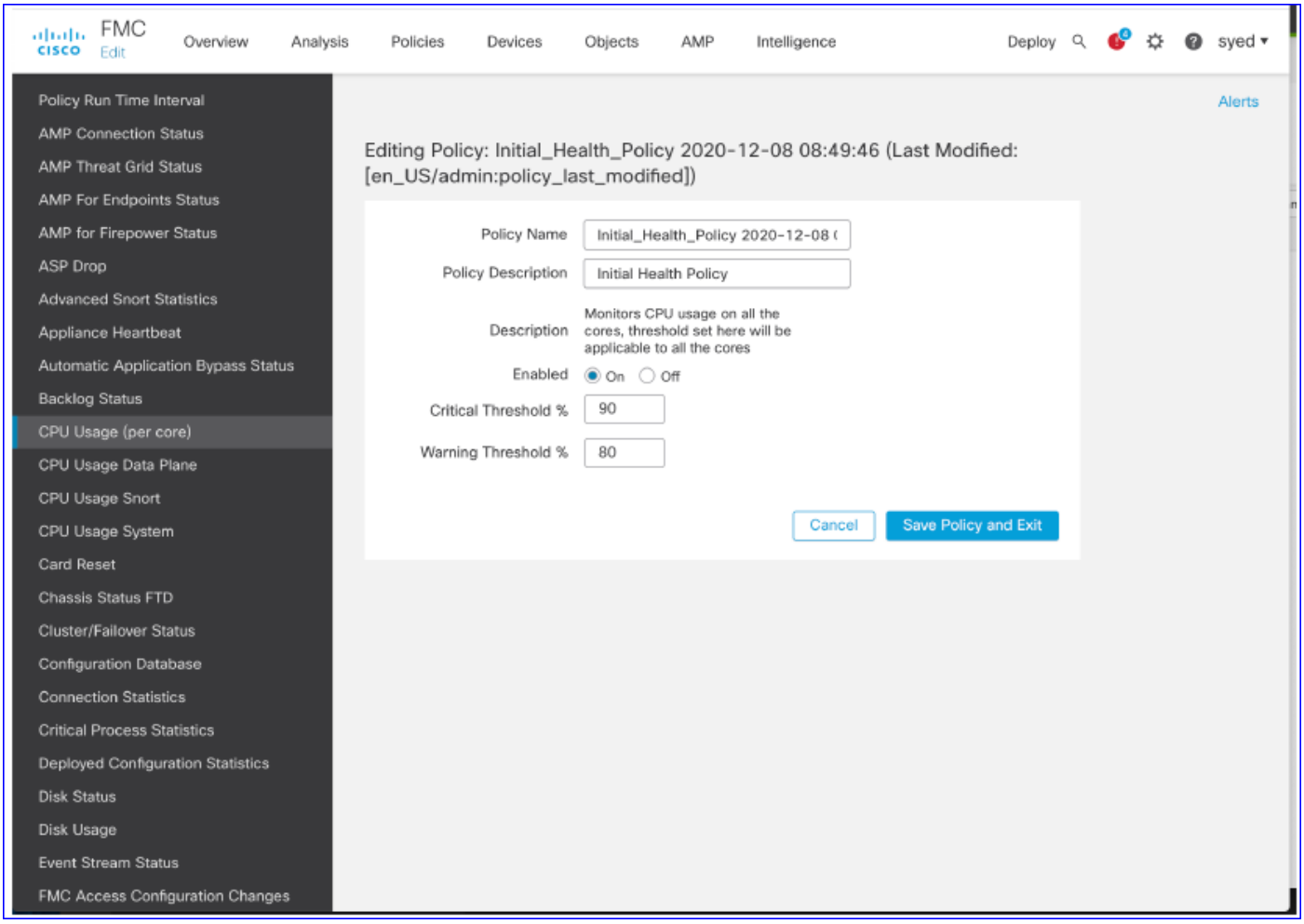
- Das Laufzeitintervall für das alte Integritätsmodul wird in "Legacy-Laufzeitintervall" umbenannt.
- "Run Time Interval" bezieht sich auf die neuen Telegraf-basierten Statusmodule
- Globale Einstellung, wirkt sich auf alle Geräte aus
- Prometheus Scrape-Zeit zurücksetzen und startet den Health Monitoring-Prozess neu.



Verfügbare Kennzahlen

Verfügbare Kennzahlen für benutzerdefinierte Dashboards

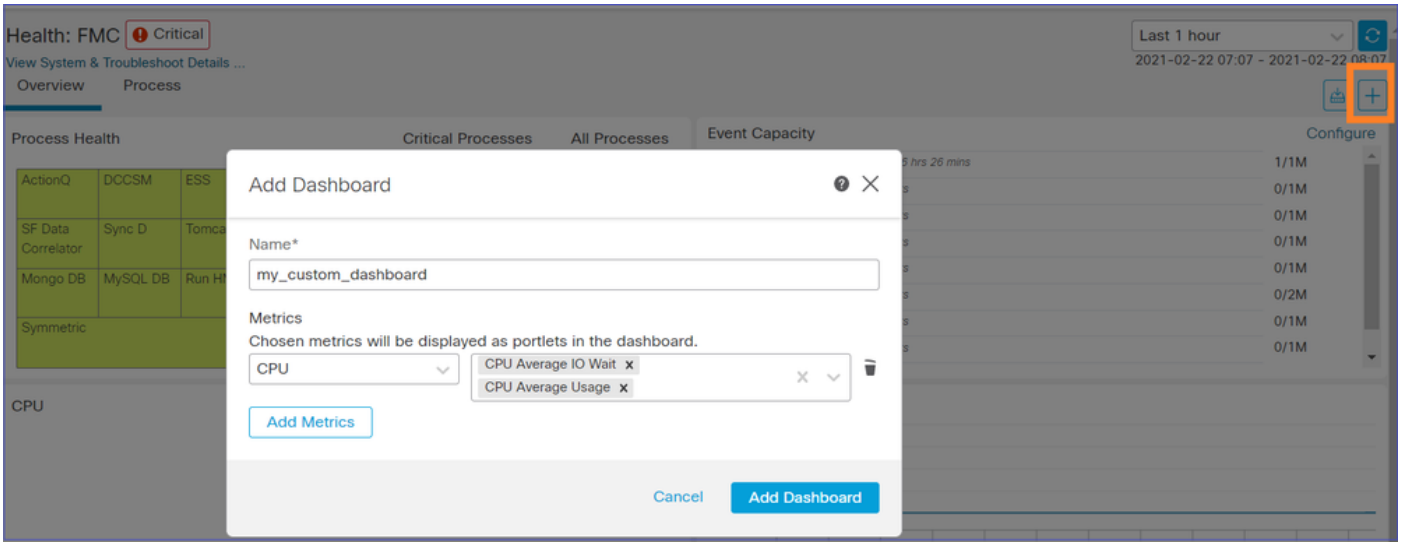
- Wenn ein Benutzer ein benutzerdefiniertes Dashboard erstellen möchte, dienen diese Folien als Leitfaden für die verfügbaren Metriken.
- Einige Kennzahlen müssen in der Integritätsrichtlinie aktiviert sein, bevor sie in einem benutzerdefinierten Integritäts-Dashboard verwendet werden können.



FMC-Benutzeroberfläche: FMC Custom Dashboard

Neue FMC Monitoring Metrics-Kategorien in 7.0

- CPU
- Arbeitsspeicher
- Schnittstelle
- Festplatte
- Veranstaltung
- Prozess
- KaninchenMQ
- Sybase
- MySQL



FMC-Benutzeroberfläche: FMC-Kennzahlen

40 Metriken, die über verschiedene Kategorien hinweg hinzugefügt wurden (im benutzerdefinierten Dashboard verfügbar). Um die deaktivierten Metriken zu aktivieren, aktivieren Sie das entsprechende Integritätsmodul in der zugeordneten Integritätsrichtlinie (**System > Health > Policy**).

Metrik-Gruppenname	Standardmäßig aktiviert	Beschreibung
CPU	Nein	Überwacht FMC-CPU
Arbeitsspeicher	Ja	Überwacht FMC-Speicher
Festplatte	Ja	Überwachung der FMC-Festplattennutzung
Schnittstelle	Ja	Überwacht FMC-Schnittstelle
Prozess	Ja	Überwacht FMC-Prozesse
Veranstaltung	Ja	Überwacht die Ereignisrate
MySQL	Nein	Überwacht MySQL
KaninchenMQ	Nein	Monitore RabbitMQ
Sybase	Nein	Überwacht Sybase

FTD: Kennzahlen aus FP 7.0

Standardmäßig aktiviert: Metriken werden standardmäßig gesammelt. Um die deaktivierten Metriken zu aktivieren, aktivieren Sie das entsprechende Integritätsmodul in der zugeordneten Integritätsrichtlinie (System > Health > Policy).

Metrik-Gruppenname	Standardmäßig aktiviert	Beschreibung	Plattform
Chassis-Status	Ja	Unterschiedliche Chassis-Parameter wie Lüftergeschwindigkeit und Temperatur werden überwacht.	Nur für Plattformen FPR2100 und FPR1000 geeignet
Flow-Offload	Ja	Überwacht Statistiken zum Hardware-Fluss-Offload	Gilt für FPR9300 und FPR4100-Plattformen
ASP-Drops	Ja	Überwachung von Paketverlusten auf der Lina-	Alle

Trefferanzahl	Nein	Seite Überwachung der Trefferanzahl für Zugriffskontrollrichtlinien-Regeln	Alle
AMP Threat Grid-Status	Ja	Überwacht die Verbindung zu AMP ThreatGrid	Alle
AMP-Verbindungsstatus	Nein	Überwachung der AMP-Cloud-Konnektivität über FTD	Alle
Status des SSE-Connectors	Nein	Überwachung der SSE-Cloud-Konnektivität über die FTD	Alle
NTP-Status	Nein	Überwacht NTP-Uhrensynchronisierungsparameter auf die FTD	Alle
VPN-Statistiken	Ja	Überwacht S2S- und RA VPN-Tunnelstatistiken	Alle
Routenstatistik	Ja	Überwachung von Paketverlusten auf der Lina-Seite	Alle
Snort 3 Perf Statistiken	Ja	Überwacht bestimmte Snort3-Leistungsstatistiken (perfstats)	Alle
xTLS-Zähler	Nein	Überwachung von xTLS/SSL-Datenflüssen, Arbeitsspeicher- und Cache-Effektivität	Alle

REST-APIs, Syslog, SNMP

In Version 7.0 wurden keine neuen REST-APIs für FMC- oder FTD-Geräte eingeführt. Die vorhandenen REST-APIs unterstützen neue Metriken, die in Version 7.0 hinzugefügt wurden.

Syslog und SNMP

Syslog

- Keine Änderung im Syslog für die Integritätsüberwachung

SNMP

- Separate TOI für "SNMP Device Health Monitoring"

SAL/CTR/Integration von Drittanbieterprodukten

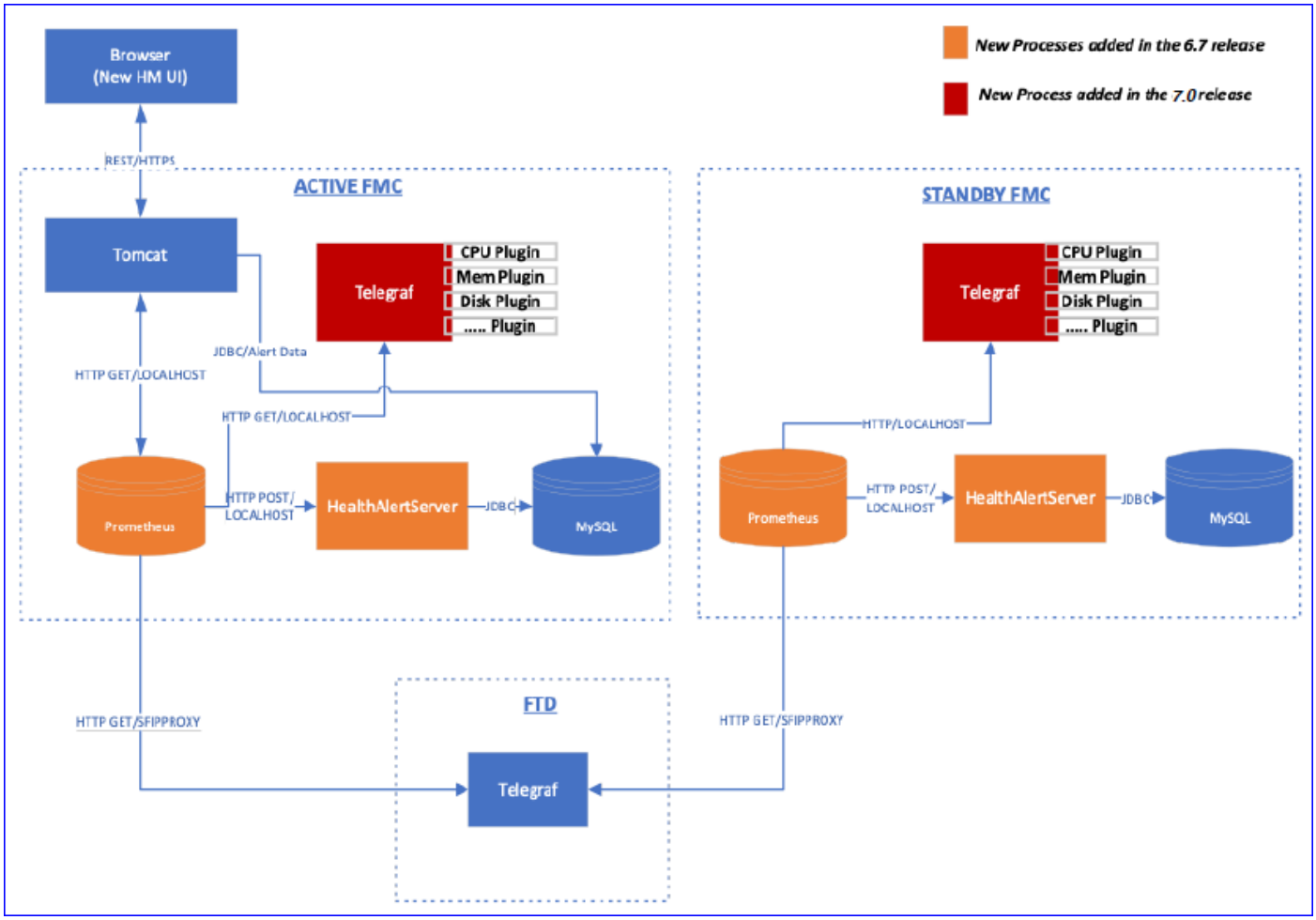
- Separater TOI für "Azure Application Insights"-Support
- Keine spezifische Änderung zur Unterstützung der Integration von "Health Monitoring" mit SAL/CTR/SecureX
- REST-API kann für Drittanbieterintegration genutzt werden

Software-Technologie

Überblick über die Architektur

- Telegraf-Health-Agent wird in FMC hinzugefügt, um FMC-spezifische Metriken zu sammeln
- Prometheus sammelt die Metriken von Telegraf und speichert sie in Zeitreihenmode.

- Warnungen werden generiert, wenn die Werte den benutzerdefinierten Schwellenwert in der Integritätsrichtlinie überschreiten.
- Telegraf Health Agent ist ein Open-Source-Plugin-gesteuerter Agent zum Erfassen von Metriken. Es sammelt alle 1 Minute Daten.
- Prometheus, eine Open-Source-Zeitreihendatenbank auf FMC, ruft alle 1 Minute die Kennzahlen vom Gerät ab.



Funktionsdetails 6.7

Beschreibung der Funktionsmerkmale

Neue NGFW-Zustandsüberwachung für FTD-Zustand und -Leistung

Erleichtert Benutzern

- Reaktives Debuggen, wie Ursachenanalyse, das Problem nach dem Auftreten
- Proaktive Maßnahmen wie die Überwachung von Nutzung und Sättigung, um potenzielle Kapazitätsprobleme zu identifizieren und die Benutzer bei Kapazitätserweiterungen oder Umgestaltungen zu unterstützen.

Vorteile für unsere TAC- und Technikerteams:

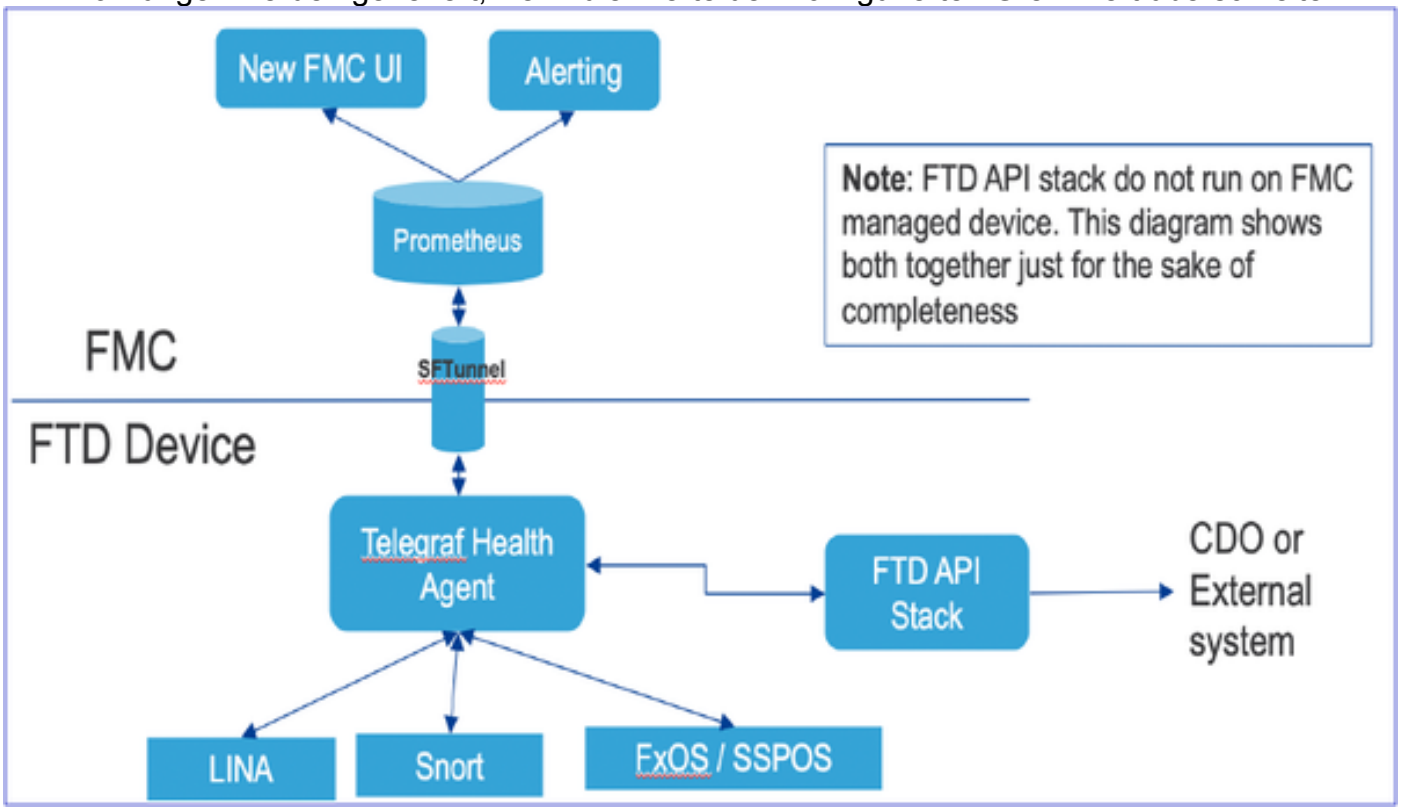
- Isolierung und Behebung von Systemproblemen
- Identifizieren von Engpässen im System sowohl bei der Entwicklung als auch in der Produktion.

Highlights

- **Trenddiagramme**: Trenddiagramme erleichtern das Erkennen von Anomalien und das Ermitteln der Ursache von Problemen. Mithilfe visueller Inspektionen können Trends erkannt und Korrelationen zwischen verschiedenen Metriken aufgezeichnet werden, um einen kausalen Zusammenhang zwischen ihnen zu finden.
- **Ereignis-Overlays**: Ereignis-Overlays zeigen wichtige Informationen an, z. B. die Konfigurationsbereitstellung und SRU-Updates in Trenddiagrammen, die ursächliche Zusammenhänge anzeigen.
- **Anpassbare Dashboards**: Benutzer können ihre eigenen Dashboards erstellen, um die gewünschten Metriken auf einer Seite zusammenzufassen.
- **Einheitliche Architektur** für die **Integritätsüberwachung: Zentrale** Stelle für die Erfassung und den Export von Kennzahlen, unabhängig davon, welcher Manager an den Kennzahlen "interessiert" ist. FTD-APIs und das FMC verwenden Daten vom gleichen Kennzahlensammler.
- **Erweiterbarkeit von Metriken**: Eines der Ziele der Architektur für die Plattform war es, einfach neue Metriken hinzufügen zu können. Dies wird durch die Verwendung von Open Source-Tools zur Sammlung und Speicherung von Metriken und durch anpassbare Dashboards erreicht.

So funktioniert es

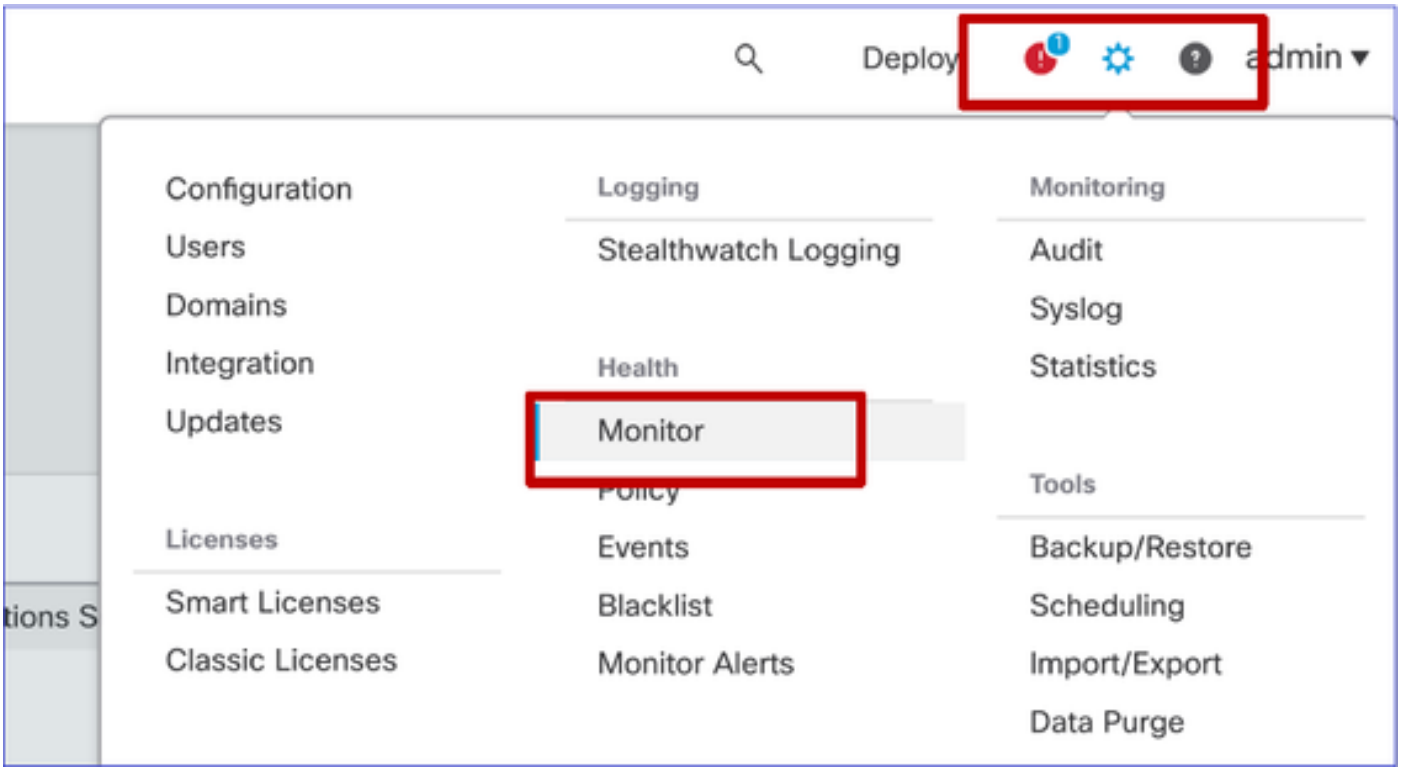
- Telegraf Health Agent ist ein Open Source Plugin-gesteuerter Agent zum Sammeln von Metriken. Es sammelt regelmäßig - alle 1 Minute.
- Prometheus, eine Open-Source-Zeitreihendatenbank auf FMC, bezieht die Kennzahlen regelmäßig - alle 1 Minute.
- Die Metrikwerte stellen aktuelle Daten dar.
- Prometheus speichert die Daten im Zeitreihenformat, das von der Benutzeroberfläche wiedergegeben wird.
- Warnungen werden generiert, wenn die Werte den konfigurierten Grenzwert überschreiten.



FMC-GUI

FMC-Benutzeroberfläche: Navigieren zum Integritätsstatus

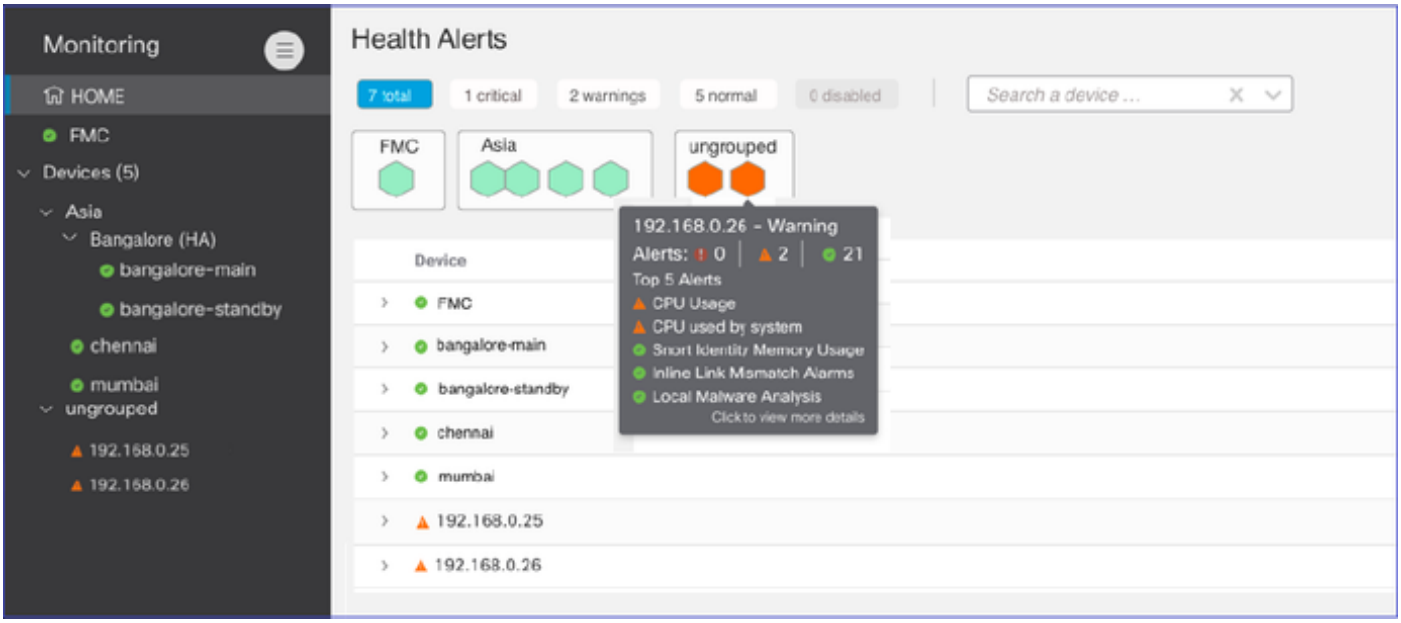
Klicken Sie auf FMC auf das Symbol **System > Health > Monitor**, um zur Seite **Health Status (Systemstatus) zu** gelangen.



FMC-Benutzeroberfläche: Neue Statusseite

Die Seite "Health Status" (Status - Status - Status) soll eine Statusübersicht aller vom FMC verwalteten Geräte anzeigen, einschließlich des Status des FMC.

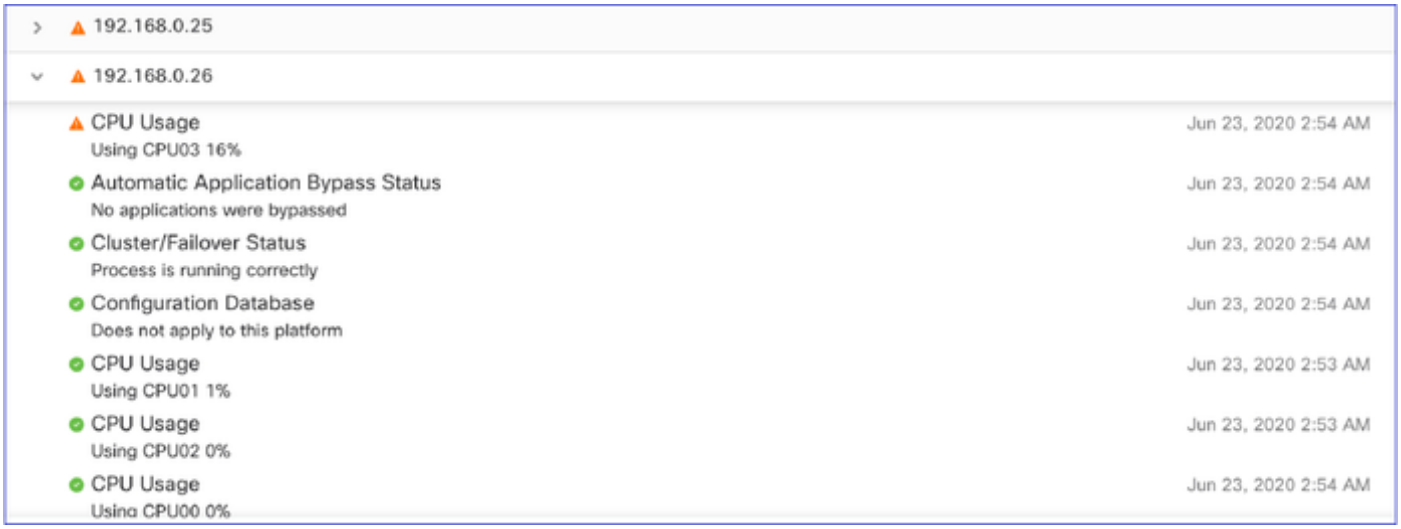
- Die Geräte werden nach ihrer Gruppe/ha/Cluster gruppiert.
- Ein Punkt links neben dem Gerät zeigt seinen Zustand an.
- Grün - keine Alarme
- Orange - mindestens eine Gesundheitswarnung
- Rot - mindestens ein kritischer Statusalarm
- Die Statuszusammenfassung wird angezeigt, wenn der Mauszeiger auf das Sechseck zeigt, das den Gerätestatus darstellt.
- Grenzwerte für Warnungen und kritische Meldungen können in der Integritätsrichtlinie genauso konfiguriert werden wie vor FP 6.7.



FMC-Benutzeroberfläche: Gerätestatusereignisse

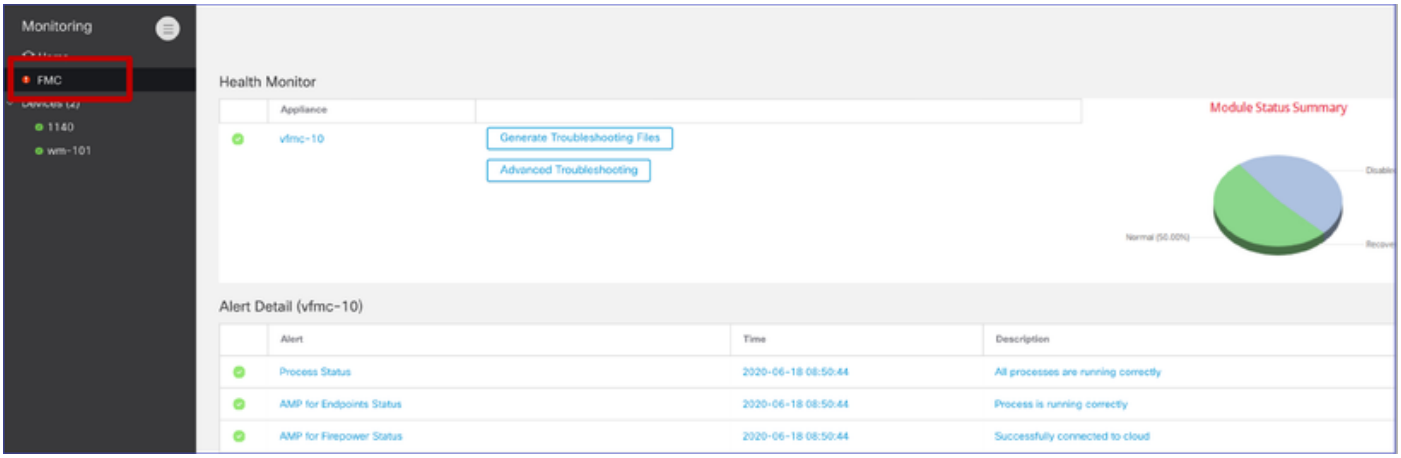
Klicken Sie auf das Gerät im unteren Bereich, um die Systemzustandsereignisse anzuzeigen, die mit den Gerätewarnungen verknüpft sind. Diese werden nach ihrem Systemzustand (Schweregrad) sortiert.

Seite "Systemüberwachung"



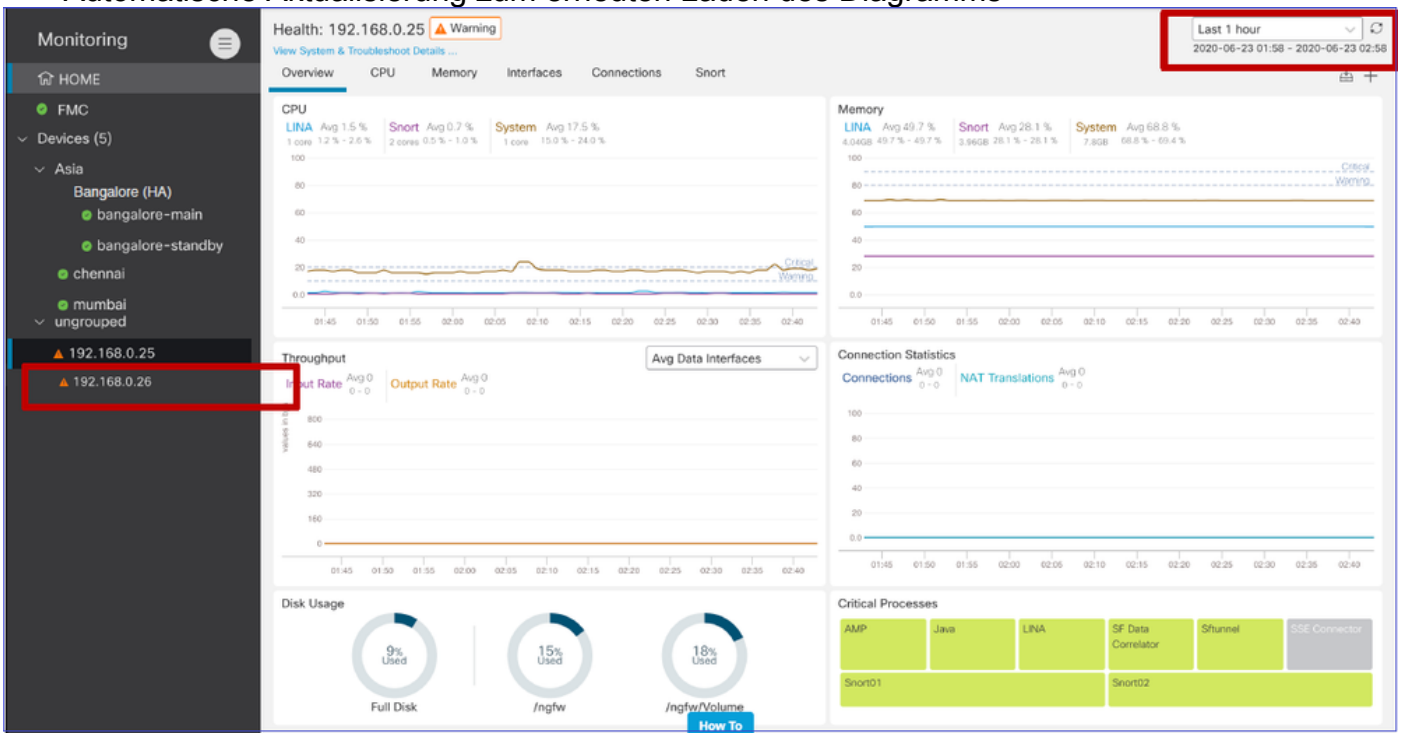
FMC-Benutzeroberfläche: FMC-Zustandsüberwachung unverändert

Die FMC-Diagnoseseite ist nach wie vor die Legacy-Seite. Die neue Benutzeroberfläche wird nur für FTD mit 6.7+ unterstützt.



FMC-Benutzeroberfläche: Neu! Geräte-Dashboards

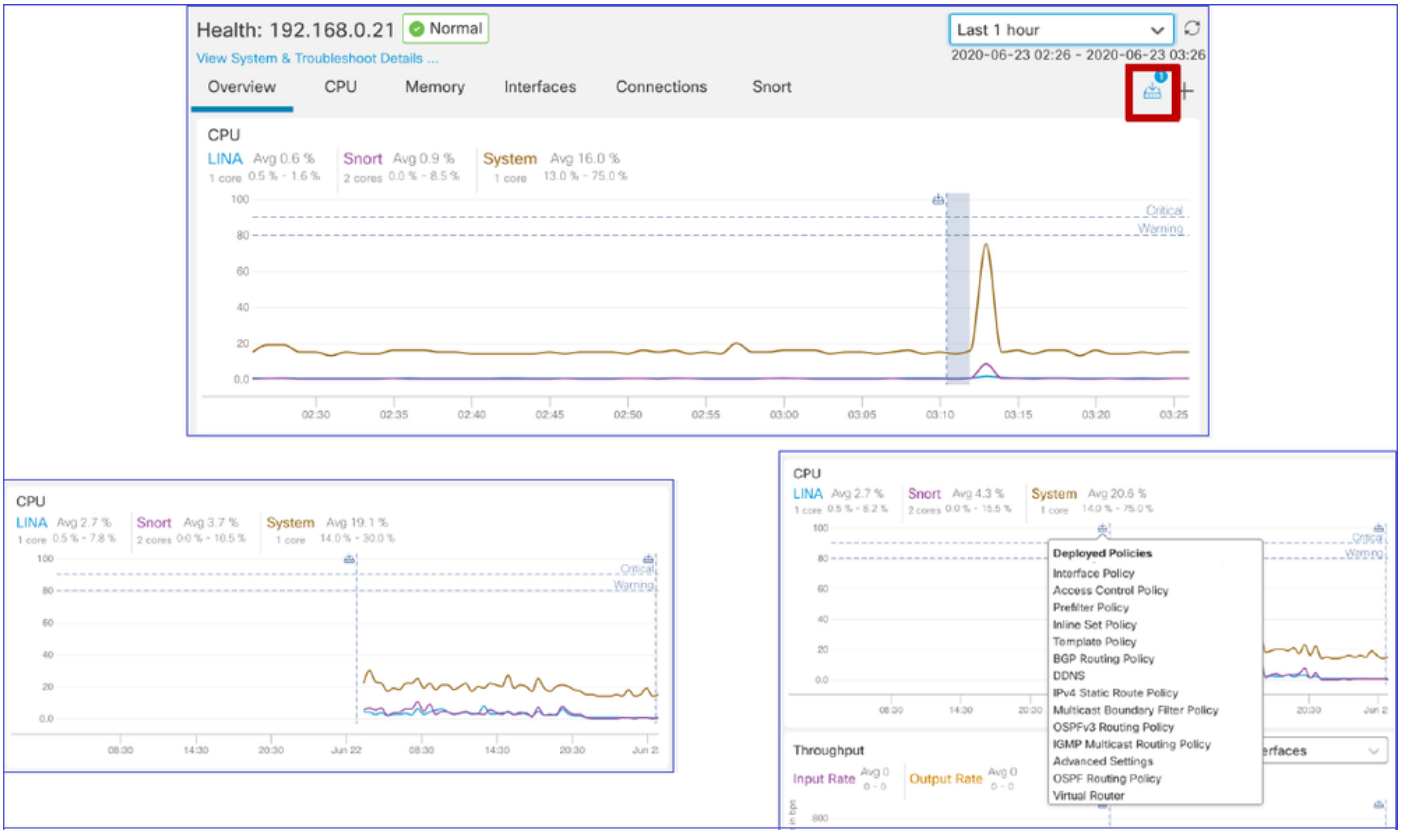
- Klicken Sie im linken Bereich auf den Gerätenamen, um zur Übersichtsseite des Geräts zu gelangen.
- Die Statusübersicht enthält alle wichtigen Trenddiagramme für die Integritätsmetriken.
- Verschiedene Zeitbereiche sind verfügbar (Standard ist die letzte Stunde)
- Automatische Aktualisierung zum erneuten Laden des Diagramms



FMC-Benutzeroberfläche: Overlay der Bereitstellungsdaten

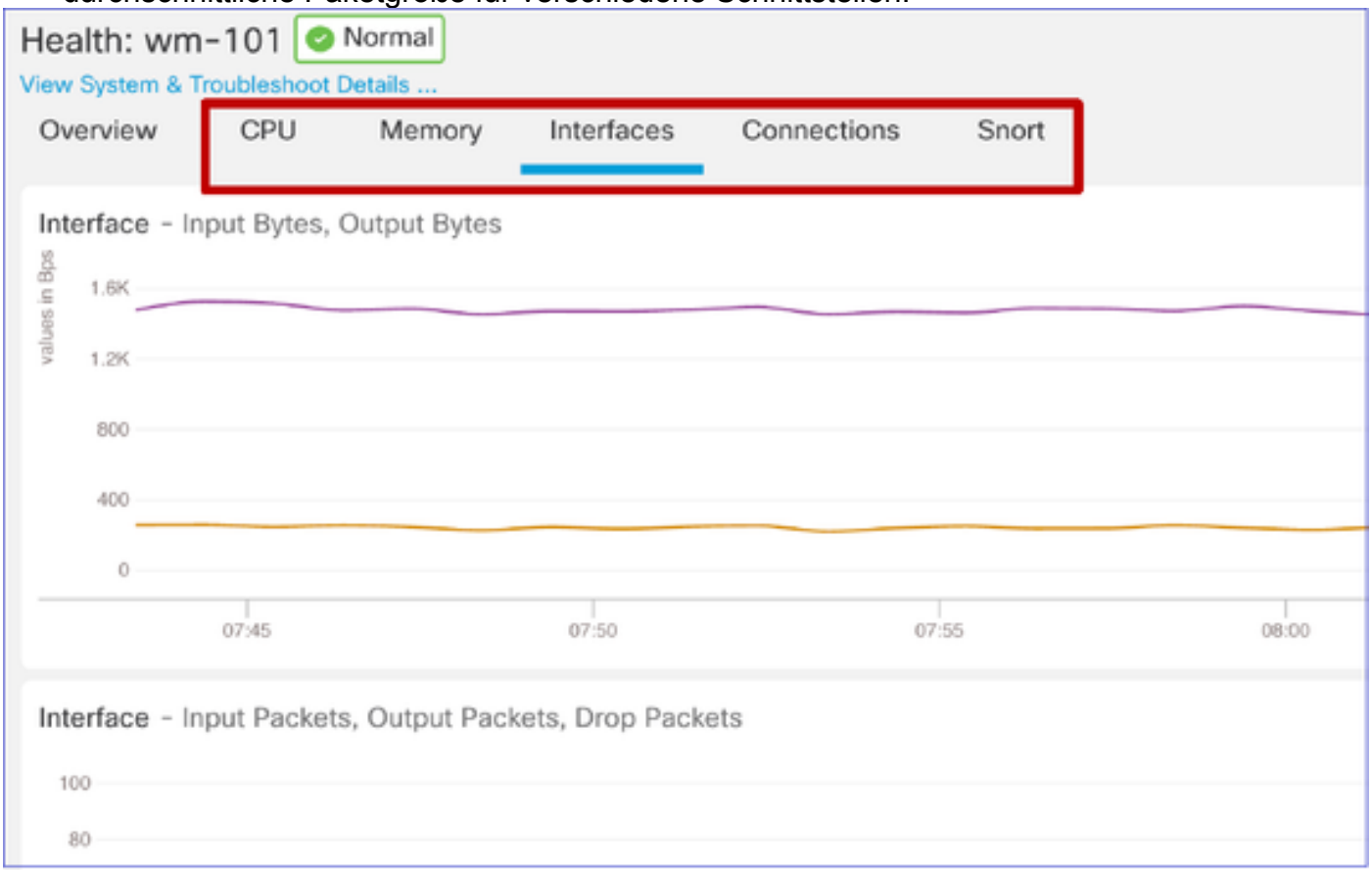
Klicken Sie auf das Bereitstellungssymbol, um Details zum Bereitstellungs-Overlay in dem Diagramm für den ausgewählten Zeitraum anzuzeigen.

- Symbol gibt die Anzahl der Bereitstellungen während des ausgewählten Zeitbereichs an
- Band zeigt den Beginn und das Ende der Bereitstellung an.
- Bei mehreren Bereitstellungen werden mehrere Bänder/Leitungen angezeigt.
- Klicken Sie auf das Symbol oben in der gepunkteten Linie, um die Details anzuzeigen.

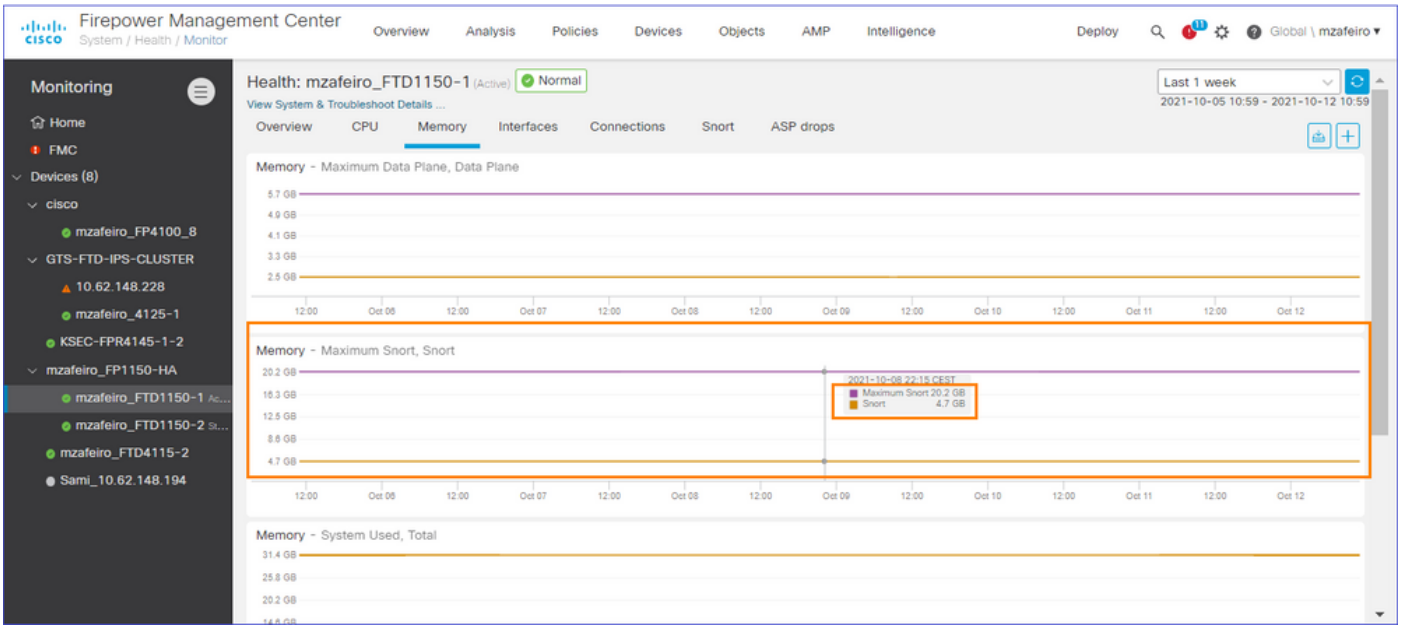


FMC-Benutzeroberfläche: Vorgefertigte Dashboards für Geräte

- In der FMC-Benutzeroberfläche sind vordefinierte Status-Dashboards vorhanden.
- Diese vordefinierten Dashboards enthalten zusammengehörige Kennzahlen.
- Das Schnittstellen-Dashboard verfügt über ein Trenddiagramm für alle schnittstellenbezogenen Metriken wie Eingabe-/Ausgabe-Bytes, Pakete und die durchschnittliche Paketgröße für verschiedene Schnittstellen.



FTD Snort Memory - Von wo stammt es?



Die Ausgabe der Benutzeroberfläche bezieht sich auf:

```
admin@FP1150-1:~$ sudo pmtool show CGroupsStatus | grep "Detectio" -A 20
[/dev/cgroups/memory/Detection]
Resources:
memory.memsw.failcnt: 0
memory.max_usage_in_bytes: 7,840,403,456
memory.limit_in_bytes: 21,719,199,744
memory.memsw.max_usage_in_bytes: 7,840,403,456
memory.usage_in_bytes: 5,035,372,544
memory.memsw.limit_in_bytes: 22,403,170,304
memory.failcnt: 0
memory.memsw.usage_in_bytes: 5,035,372,544
Procs:
<p9738> sfhassd
<p26746> snort
<p26747> snort
<p26748> snort
<p26749> snort
<p26750> snort
<p26751> snort
<p26752> snort
<p26753> snort
```

Diese Informationen wurden von Technikern unter https://jira-eng-rtp3.cisco.com/jira/browse/FPSVZ-1033 bereitgestellt.

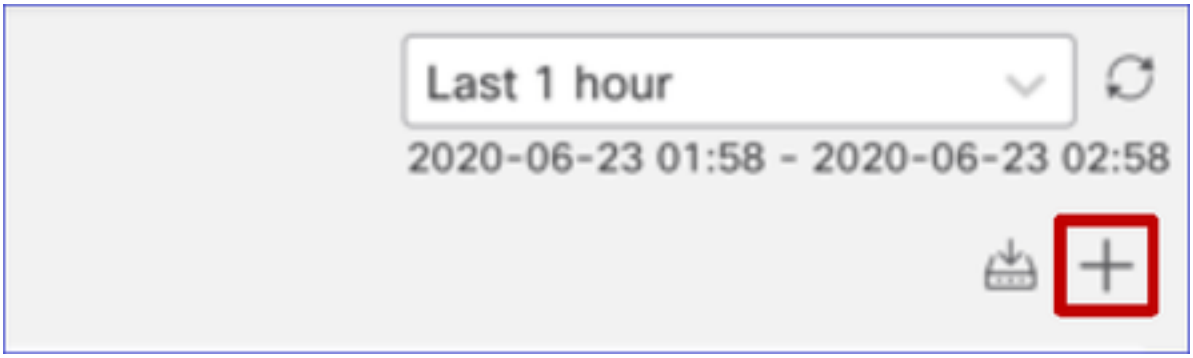
FMC-Benutzeroberfläche: Erstellung benutzerdefinierter Dashboards möglich

Benutzer können ein eigenes benutzerdefiniertes Dashboard erstellen

- Zusätzlich zu den vordefinierten Dashboards können Benutzer auch benutzerdefinierte Dashboards erstellen.
- Im benutzerdefinierten Dashboard kann eine beliebige Anzahl von Metriken hinzugefügt werden.
- In der Regel wird ein benutzerdefiniertes Dashboard erstellt, wenn Metriken aus verschiedenen Metrikgruppen korreliert werden können, um die Ursache eines Problems zu

ermitteln.

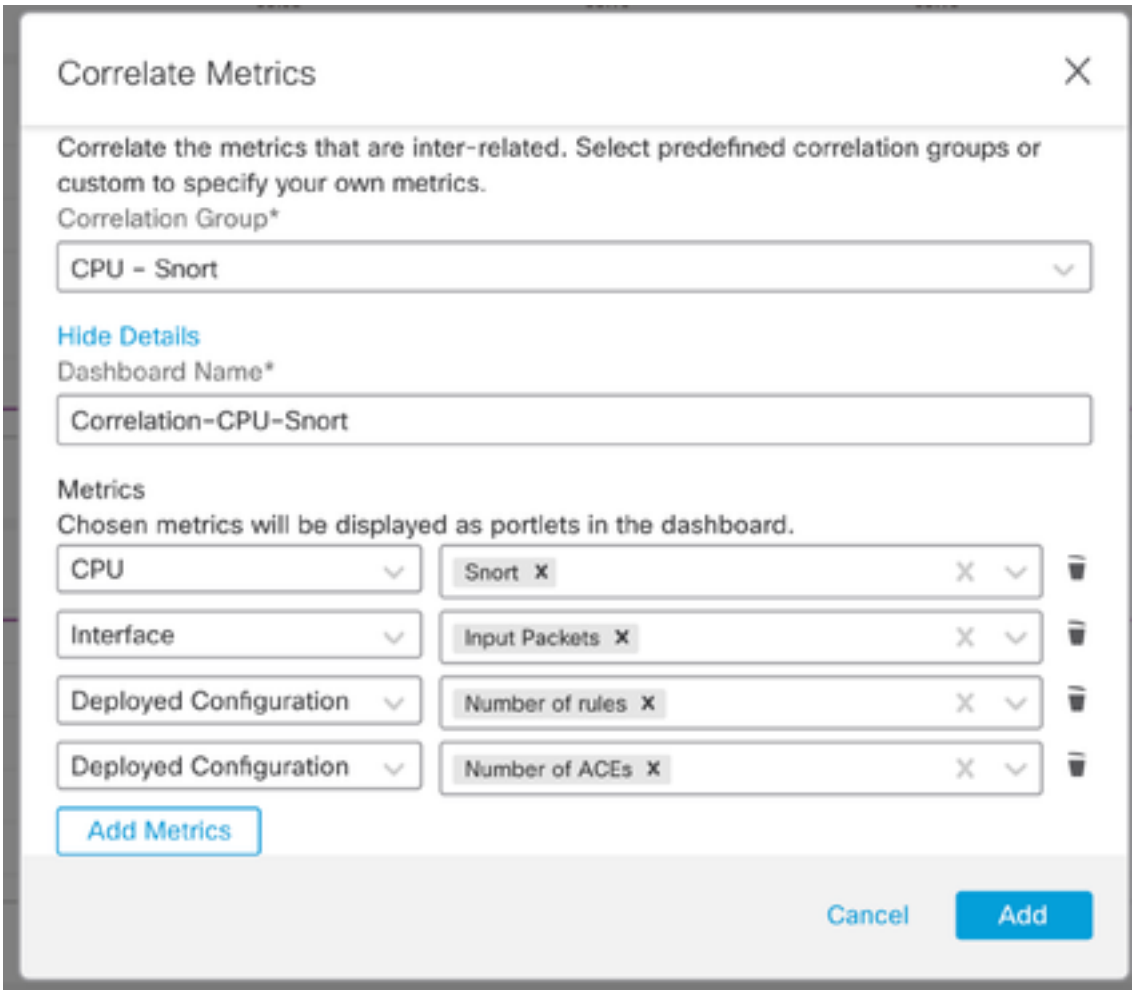
- Im Falle einer hohen Lina CPU kann man die eingehende Verbindung pro Sekunde (Connection Per Second, CPS), Schnittstellenstatistiken (und so weiter) sehen, die eine hohe CPU verursachen können.



FMC-Benutzeroberfläche: Erstellen eines benutzerdefinierten Dashboards

Dialogfeld "Metriken korrelieren"

- Wenn ein Benutzer auf "+" klickt, um ein benutzerdefiniertes Dashboard zu erstellen, wird das Fenster "Metriken korrelieren" geöffnet.
- Ein Benutzer kann verschiedene Metriken hinzufügen, die er gemeinsam überwachen möchte.



REST-APIs

FMC REST APIs - Zusammenfassung

FMC GET-API	Beschreibung
/api/fmc_config/v1/domain/{domainUID}/health/al Warnungen	Dadurch wird der Status aller Statusmodule für die angegebene UUID.
/api/fmc_config/v1/domain/{domainUID}/health/ metriken	Die API ruft die Kennzahlen intern vom Time Series DB - Prometheus und senden Sie sie zurück an Anrufer.

FMC REST-APIs - /health/alert

Verschiedene Filterkriterien:

- startTime und endTime: in Sekunden. Beide zusammen anzugeben. Gibt alle Warnungen zurück, die zwischen den beiden Zeitpunkten generiert wurden.
- deviceUUID: Alle Warnungen für angegebene UUID zurückgeben
- Status: Gibt alle Warnungen mit dem angegebenen Status zurück (rot, gelb, grün)
- ModuleIDs: Liste der Funktionsmodul-IDs

Beispiel für das Ergebnis:

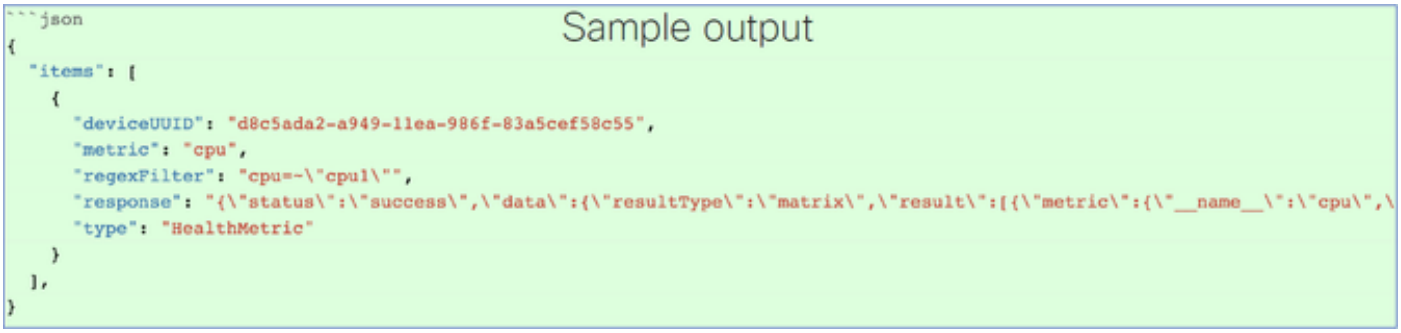

```
{
  "items": [
    {
      "deviceUUID": "a04cb2da-8915-11ea-9d2e-da80fb1fedea",
      "moduleUUID": "980ca3ae-fd69-43c1-b3cc-d71ea394b2eb",
      "moduleID": "CPU",
      "timestamp": 1589271373,
      "status": "GREEN",
      "type": "HealthAlert"
    },
```


FMC REST-APIs - /health/metrics

Verschiedene Filterkriterien:

- startTime und endTime: in Sekunden. Beide zusammen anzugeben. Alle zwischen den beiden Zeitpunkten generierten Metriken zurückgeben
- deviceUUID: Gibt alle Metriken für das angegebene Gerät zurück.
- metric: Gibt alle Metriken mit dem angegebenen Namen zurück (cpu, mem, disk)
- step: Schritt in Sekunden. Metrische Werte bei jedem Schritt in Sekunden.
- regexFilter: Regex-Filter für Metriknamen. (Beispiel: snort)

Beispiel für das Ergebnis



Beispiel für FMC REST-Eingang/Ausgang

Anforderungs-URL:

https://u32c01p12-vrouter.cisco.com:10213/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/health/metrics?filter=deviceUUIDs:c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d;**metric:cpu;regexFilter:lina_cp_avg**;
startTime:1611294885.699;endTime:1611309285.699;step:60;

Antwort:

{

"Links":{

"Elemente":[{

"Antwort":{

"Status":"Erfolg",

"Daten":{

"resultType":"matrix",

"Ergebnis":[{

"metrisch":{

"__name__":"**CPU**",

"CPU":"**lina_cp_avg**",

"Instanz":"127.0.0.1:9273",

"Job":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",

"uuid":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d"},

"Werte":[

[1611309165,699,"0,5"],

[1611309225,699,"0,5"],

[1611309285,699,"0,5"]

]

}

]}

}",

"deviceUUID":"c1f97434-d6dd-11ea-9df2-dfc9e6fdf76d",

"metrisch":"CPU",

"regexFilter":"cpu=~"lina_cp_avg"",

"Typ":"Metrisch"

}

REST-APIs für FTD-Geräte

REST-API für FTD-Geräte	Beschreibung
/devices/default/operational/metrics	Alle Metriken auslesen. Momentane Werte von Metriken werden zurückgegeben.
/devices/default/operating/metrics/{objId}	Spezifische Metrik ausgeben, die von {objId} identifiziert wurde
/devices/default/operational/metricsschema	Ausgabeschema wird bei allen Metriken zurückgegeben werden gelöscht (erste Get-Anfrage)
/devices/default/operating/metricsschema/{objId}	Ausgabeschema, das zurückgegeben wird, wenn ein bestimmtes Die Metrik von übergebenem {objId} wird abgefragt.

REST-API für FTD-Geräte: GET-Metriken

Beispiel-Antworttext für Metriken

Curl

```
curl -X GET --header 'Accept: application/json' 'https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics'
```

Request URL

```
https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics
```

Response Body


```
{
  "items": [
    {
      "name": "mem.used_swap_snort",
      "metric": {
        "value": 0,
        "unit": "BYTE",
        "type": "numericdevicemetricvalue"
      },
      "timestamp": 1592316305,
      "dateTime": "2020-06-16T14:05:05Z",
      "id": "mem.used_swap_snort",
      "type": "devicemetricdata",
      "links": {
        "self": "https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/mem.used_swap_snort"
      }
    },
    {
      "name": "mem.remaining_blocks_1550_bytes",
      "metric": {
```


Response Code

```
200
```

REST-API für FTD-Geräte: GET-spezifische Kennzahl

Um eine bestimmte Metrik abzurufen, geben Sie deren Objekt-ID in der URL an. Die Objekt-ID ist das Namensfeld der Metrik.

Curl

```
curl -X GET --header 'Accept: application/json' 'https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/snort.stats.packets_bypassed_
```

Request URL

```
https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/snort.stats.packets_bypassed_snort_busy
```

Response Body

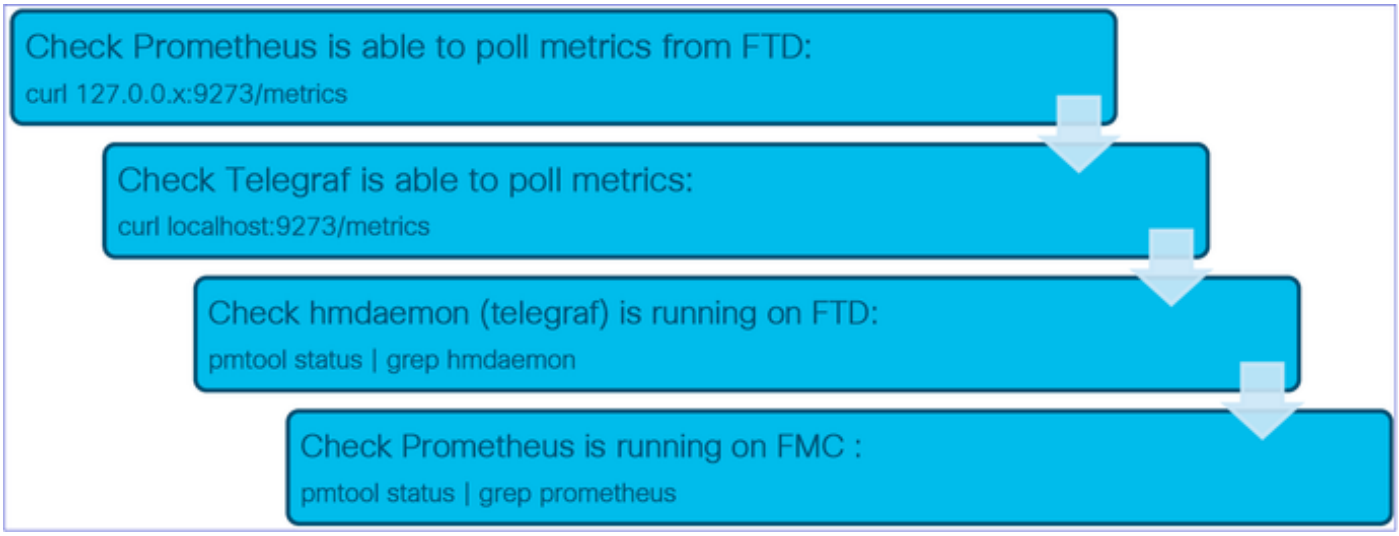

```
{
  "name": "snort.stats.packets_bypassed_snort_busy",
  "metric": {
    "value": 0,
    "unit": "COUNT",
    "type": "numericdevicemetricvalue"
  },
  "timestamp": 1592317383,
  "dateTime": "2020-06-16T14:23:03Z",
  "id": "snort.stats.packets_bypassed_snort_busy",
  "type": "devicemetricdata",
  "links": {
    "self": "https://ast0072-pod.cisco.com:670/api/fdm/v6/devices/default/operational/metrics/snort.stats.packets_bypassed_snort_busy"
  }
}
```


Response Code

```
200
```

Fehlerbehebung/Diagnose

Überblick über die Diagnose - Typischer Fehlerbehebungsablauf



Wichtige Befehle und Dateien zur Fehlerbehebung und Anmeldung am Gerät

Hinweis: In 7.0 NPI wird Port 9274 anstelle von 9273 erwähnt.

Befehl/Datei auf Gerät	**Wofür wird es verwendet?**
pmtool-Status | grep hmdaemon	Überprüfen Sie, ob Telegraf auf dem Gerät ausgeführt wird.
curl localhost:9273/metrics	Dieser Befehl ruft alle Daten ab oder gibt Metriken aus telegraf aus.
curl localhost:9273/hm/<metric Name>	Ein leerer Ein-/Aus-Zustand bedeutet, dass das Telegramm nicht richtig funktioniert.
pmtool restartbyid hmdaemon	So starten Sie hmdaemon neu
/ngfw/var/log/hmdaemon.log	Datei, in der Telegrafenprotokolle gespeichert werden.
/ngfw/etc/sf/telegraf_api.conf	Die Datei, die die Telegrafekonfiguration erfasst. Siehe Abschnitt zu Telegraf-Konfigurationsänderungen.

Markierte Datei-/Befehlsausgabe in FMC enthalten Fehlerbehebung

Wichtige Befehle und Dateien zur Fehlerbehebung und Anmeldung bei FMC

Befehl/Datei auf FMC	**Wofür wird es verwendet?**
pmtool-Status | grep Prometheus	Überprüfen Sie, ob Prometheus auf dem Gerät ausgeführt wird.
pmtool restartbyid Prometheus	So starten Sie Prometheus neu
curl localhost:9090/metrics	Der 9090-Port ist der Management-Port von Prometheus. /metrics-Endpunkt würde seine eigenen Metriken zurückgeben.
curl localhost:9090/targets	**HTML-Seite, die in Prometheus konfigurierte Ziele auflistet. Suchen Sie nach einem Textendpunkt.**
curl localhost:9090/warnt	HTML-Seite mit allen aktiven Warnmeldungen. Es ist viel einfacher zu laden. Dies im Browser überprüfen und
curl localhost:9090/rules	**HTML-Seite mit allen konfigurierten und akzeptierten Regeln. Dies kann anhand konfigurierter Regeln überprüft werden.**
/var/opt/prometheus/	Verzeichnis, in dem alles Prometheus Zeug vorhanden ist
/var/opt/prometheus/devicehm.yml	Hauptkonfigurationsdatei für Prometheus
/var/opt/prometheus/targets/	Verzeichnis, in dem alle Ziele (FTD-Telegrafinstanzen) gespeichert sind. Dateien in diesem Verzeichnis werden erstellt, wenn Ziele

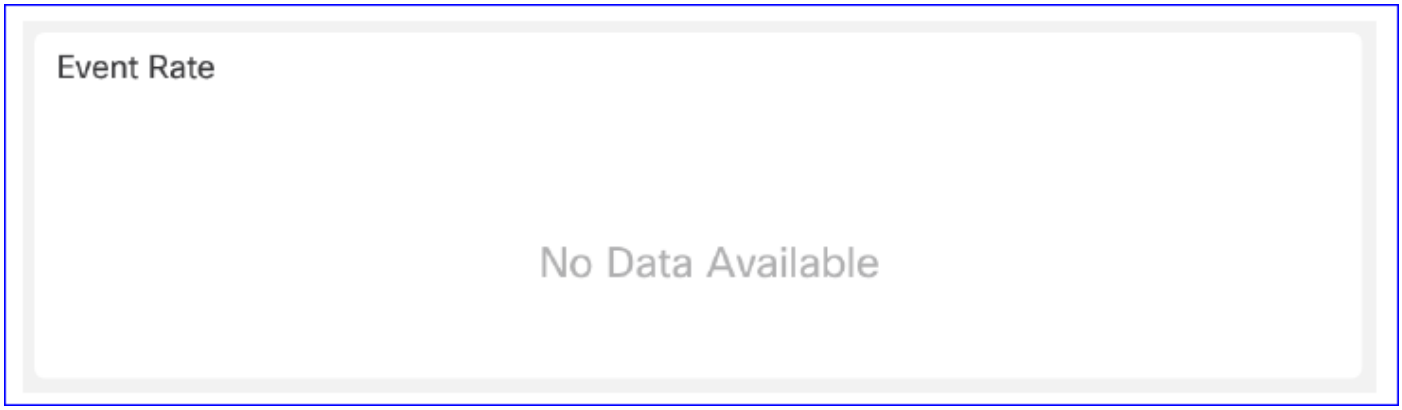
	von FMC erkannt werden.
/var/opt/prometheus/rules/	Verzeichnis, in dem alle Regeldateien gespeichert sind. Für jedes Gerät wird auf Grundlage der angewendeten Integritätsrichtlinie eine Regeldatei erstellt.
/var/opt/prometheus/data/	Die Datendatei enthält alle TSDB-Daten. "du -h ." in diesem Verzeichnis gibt den Speicher von Prometheus verwendet.
curl <target_ip>:9273/metrics	Abrufen von Metriken vom Gerät
/var/log/prometheus*	**Prometheus-Protokolle**

Hervorgehobene Datei-/Befehlsausgabe in Fehlerbehebung

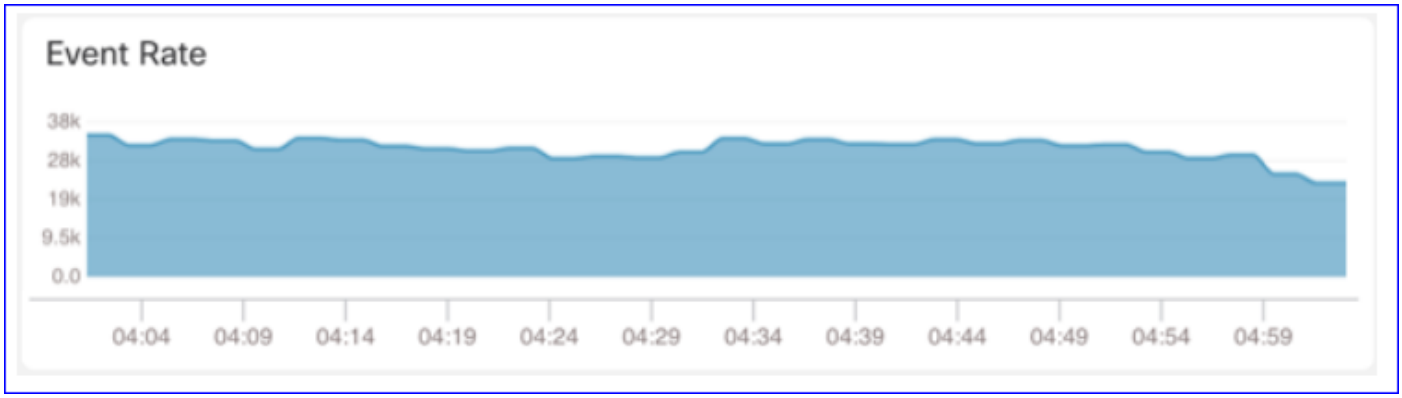
Erfassen von Daten von (Gerät) - GUI

Daten für einen Zeitraum werden in GUI angezeigt

Wenn Prometheus nicht über Daten für den ausgewählten Zeitraum verfügt, zeigt die GUI im Dashboard-Bereich "No Data Available" (Keine Daten verfügbar) an:



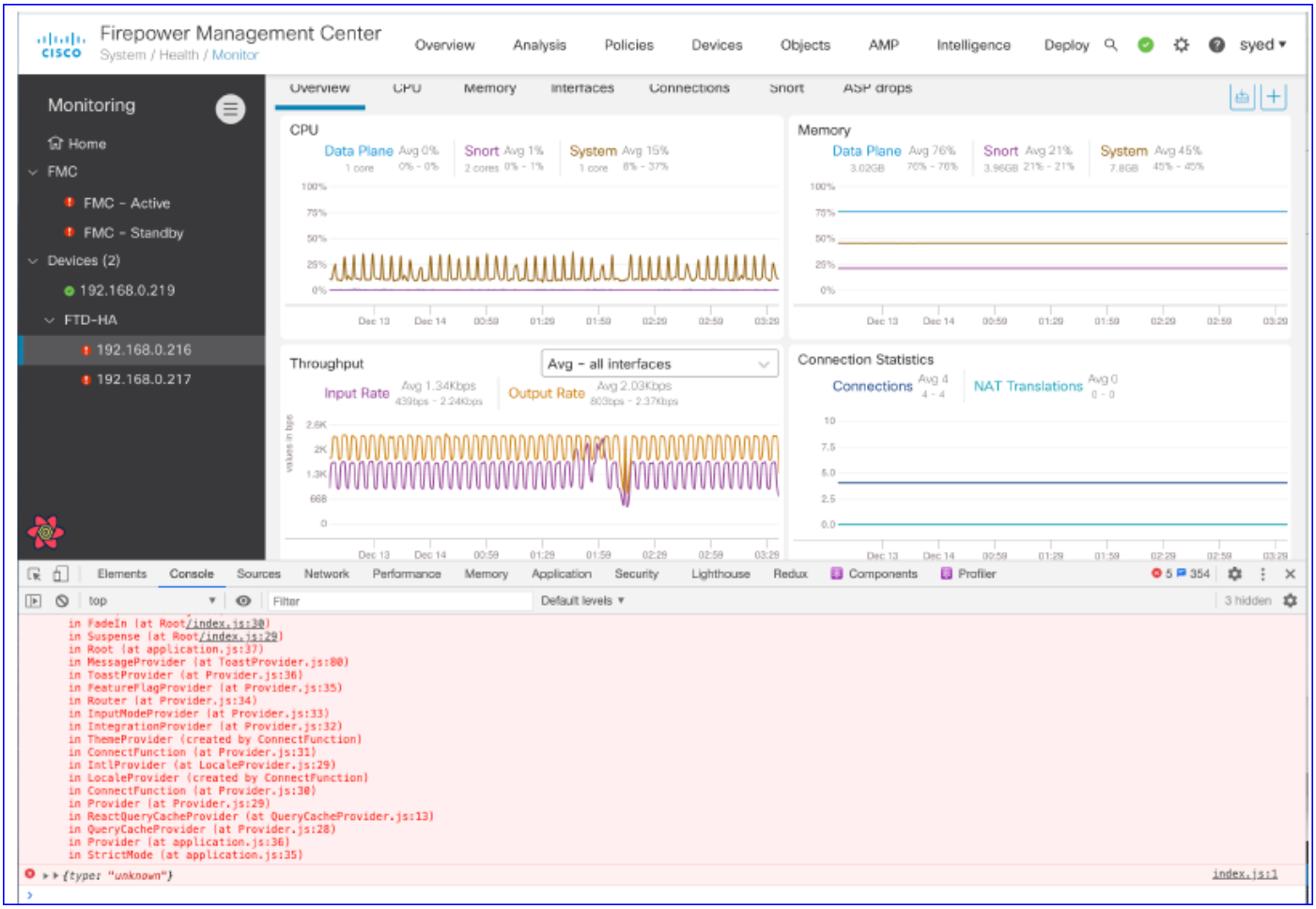
Wenn Daten verfügbar sind, sieht die Grafik wie folgt aus:



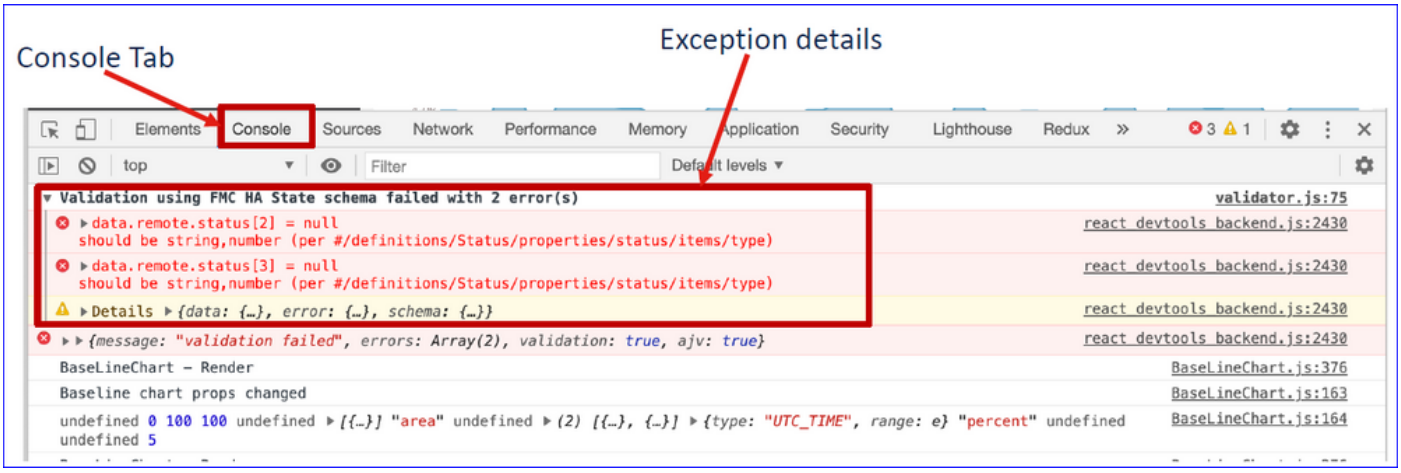
Verwenden Sie die Browser-Registerkarten "Konsole" und "Netzwerk".

Browser-Konsolenprotokoll und Netzwerk-Anrufprotokoll

- In diesem Beispiel wird die Chrome-Browser-Entwicklerkonsole angezeigt.
- Im Fehlerfall werden die Ausnahmedetails im Konsolenprotokoll angezeigt.



Beispiel für ein Browser-Konsolenprotokoll



Erfassen von Daten von (Gerät) - CLI

Aktivieren von Telegraf mit Debug-Modus in FMC

1. Wechseln Sie in den Expertenmodus für FTD, und melden Sie sich als Sudo-Root-Benutzer an.
2. Öffnen Sie die Datei /etc/sf/fmc_telegraf_api.conf im FTD.
3. Deaktivieren Sie die Option "debug".
4. Laden Sie Telegraf neu, indem Sie 'pmtool HUPByID hmdaemon' ausführen.
5. Telegraf läuft im Debug-Modus und gibt granulare Debug-Meldungen in der Datei /var/log/hmdaemon.log aus

Denken Sie daran, die "debug"-Option zu kommentieren, wenn fertig!

Einzelheiten zu Einschränkungen, häufige Probleme und Problemumgehungen

Implementierungshinweise

- Die Genauigkeit der Metrik hängt von der Häufigkeit der Abfrageinstanzen ab.
- Die maximale Datenauflösung für die Grafik beträgt 1440 (Dauer eines Tages). Wenn die Zeitspanne groß ist, sind einige Datenpunkte nicht sichtbar.
- Die Ausgabe der FTD Device REST API ist im JSON-Format.
- Die Ausgabe der FMC REST API ist im Prometheus-Format. Weitere Informationen zum Format Prometheus finden Sie unter

https://prometheus.io/docs/prometheus/latest/querying/api/

- Das Prometheus-Format ermöglicht Flexibilität bei der Integration externer Tools wie (Grafana)

Hinweis: Die CPU-Nutzungsmetrik ist in der FMC-Integritätsrichtlinie standardmäßig deaktiviert. Sie kann aktiviert werden, indem Sie die zugehörige Integritätsrichtlinie ändern.

Workarounds und Tipps

Anmerkung im Diagramm flackert am Ende des Diagramms.

- Bewegen Sie den Cursor langsam, um dieses Problem zu vermeiden.

Anmerkungen im Diagramm haben eine maximale Länge, die die angezeigten Daten begrenzt.

- Verwenden Sie in diesem Fall die im Metrikfenster verfügbare Filterfunktion.

Einschränkungen der Implementierung für Version 6.7

- Das Prometheus-Intervall für die Verschlüsselung aller Geräte und Metriken wird auf 1 Minute festgelegt.
- Das Prometheus-Abstreifintervall kann geändert werden, indem die Prometheus-Jamal-Datei auf dem FMC (/var/opt/prometheus/devicehm.yml) geändert wird.
- Die FTD API-Ausgabe ist im JSON-Format.
- Überwachung von FMC nicht unterstützt; nur FTDs
- Die Metrik für die CPU-Auslastung ist in der FMC-Integritätsrichtlinie standardmäßig deaktiviert. Sie kann aktiviert werden, indem Sie die zugehörige Integritätsrichtlinie ändern.

Was ist zu übermitteln, wenn ein Problem auftritt?

Zusammenfassung der Protokolle, die gesendet werden sollen:

- Screenshots der Benutzeroberfläche
- Protokolle von Prometheus und hmdaemon (siehe Abschnitt Fehlerbehebung/Diagnose).
- Dump der Prometheus-Datenbank (/var/opt/Prometheus/data directory)

Häufig gestellte Fragen

Frage: Ist dieses FMC nur verfügbar? Was ist mit FTD/FDM für die Benutzer, die zu CDO gegangen sind?

A: Dies ist nur FMC und die neue Benutzeroberfläche ist nur für FTD-Geräte unter 6.7.

F: Benutzerdefinierte Dashboards sind nur für Geräte in 6.7?

A: Die Dashboards sind nur für FTD-Geräte in 6.7.

Frage: Enthält diese Funktion gerätespezifische Merkmale? Ist es für IRGENDEINE Plattform, die FTD unterstützt, die all dies hat? Werden virtuelle Plattformen unterstützt?

A: Dies wird auch von virtuellen FTDv unterstützt. Es gibt mögliche gerätespezifische Variationen der Kennzahlen, die herangezogen werden. Die Funktion wird jedoch auf allen FTD-Plattformen unterstützt.

Frage: Gibt es mit der offenen API eine aktive Zusammenarbeit mit dem CDO-Team?

A: Mit "offene API" meine ich die REST-API. Die REST-API des FMC unterscheidet sich *von* der REST-API des FTD-Geräts. Die REST-API für FTD-Geräte ist bei der Verwaltung mit FMC nicht verfügbar. Nicht alle Funktionen in FMC verfügen über FMC REST APIs.

A: Die Infrastruktur für die REST-API des FTD-Geräts ist in Vorbereitung auf eine zukünftige Version vorhanden.

F: Die Download-Schaltfläche neben dem Zeitfenster (in der Nähe von "+") auf der Seite "Integritätsmonitor" würde den Integritätsbericht oder die Diagramme herunterladen, wie wir in diesem Fenster gesehen haben? Oder war es ein Widget?

A: In Bezug auf das Overlay-Symbol für die Bereitstellung, klicken Sie auf das Symbol Overlay Deployment Job, um die Zeit auf dem gewählten Diagramm auszulösen.

Interne Nachverfolgungsinformationen

CSC.content-security > sfims > ftd-plug-telemetrie, fmc_hm

- Verwendung von ftd-plug-Telemetrie zur Protokollierung von Fehlern im Zusammenhang mit FTD APIs und Telegrafen
- Verwenden Sie fmc_hm, um Probleme mit der FMC-Benutzeroberfläche und dem FMC-Backend zu protokollieren.
- FTD REST API => CSC.content-security > sfims > ftd-api-telemetrie
- EDCS-18385961

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.