Mise à niveau FP - Surveillance de l'état des périphériques

Table des matières

Introduction

Ce document décrit la nouvelle fonctionnalité de surveillance de l'état de santé des périphériques ajoutée dans les versions 6.7 et 7.0.

Informations de fond

Le problème :

Le système de surveillance de l'état du périphérique offre une visibilité sur les performances du périphérique pour un débogage réactif et des actions proactives.

Une visibilité et une analyse complètes sont obtenues par :

- Graphiques de tendance pour les indicateurs clés
- Recouvrement d'événements
- Tableaux de bord personnalisables
- Architecture de surveillance unifiée de l'état : voir les mêmes données pour tous les responsables
- De nombreuses nouvelles mesures et l'extensibilité des mesures pour en ajouter de nombreuses autres

Nouveautés de la version 7.0

Nouveautés ou différences par rapport à FP 7.0

- Tableau de bord FMC avec prise en charge haute disponibilité
- Plus de 110 nouvelles mesures pour le FTD
- Alerte de santé pour le scénario FTD split brain
- Intervalle d'exécution personnalisé pour les nouvelles mesures d'intégrité

Avantages

- Aide au débogage des systèmes en permettant de corréler les données de différents sous-systèmes et ressources sur le périphérique
- Visibilité sur diverses mesures de performances système
- Planification de capacité

Nouveauté sur 6.7

Nouveau ou différent par rapport à la version qui précède immédiatement (niveau élevé) :

- Nouvelle interface utilisateur pour la surveillance de l'état des périphériques sur FMC
- FTD Device REST API : device-metric API : de nombreuses nouvelles métriques ajoutées
- API FMC : nouvelles API : alertes d'intégrité, mesures d'intégrité et détails de déploiement
- Présentation du marché de haut niveau, applications réelles
- Aide au débogage des systèmes en permettant de corréler les données de différents sous-systèmes et ressources sur le périphérique
- Visibilité
- Planification de capacité

Présentation des fonctionnalités

Comment ça fonctionne

- Surveillance de l'état des périphériques dans FP 7.0
- Nouveau tableau de bord d'intégrité pour FMC qui fournit des graphiques de tendances, des superpositions et des tableaux de bord personnalisés
- Nouvelles mesures FTD disponibles dans les tableaux de bord FTD
- Plus de 110 indicateurs couvrant 12 catégories
- API FTD : rend les mesures disponibles pour la requête par des entités externes

Sous le capot,

- Collecte l'état de santé d'un périphérique avec Telegraf (un cadre de collecte de métriques open source)

Notes supplémentaires

Des données de surveillance sanitaire sont disponibles

- Dans le tableau de bord de l'état de santé FMC, accessible à partir du menu système (Système > État de santé > Surveillance)
- À partir de l'API REST FMC
- Lorsque le périphérique est géré par FDM, via l'API REST du périphérique FTD

Certaines métriques (FMC et FTD) sont désactivées par défaut

- Les modules d'intégrité de la politique d'intégrité doivent être activés et déployés pour que certaines mesures apparaissent.

Mise en oeuvre des améliorations demandées par les utilisateurs de FP 6.7 IFT

- Actualisation automatique par défaut
- Filtre avec plage horaire personnalisée sur le tableau de bord
- Sélectionnez les interfaces par nom défini par l'utilisateur (ainsi que par nom d'interface physique) dans le sélecteur d'interface
- Tableau de bord du périphérique de lancement croisé de la page d'accueil de Health Monitor

Surveillance de l'état des périphériques dans FP 6.7

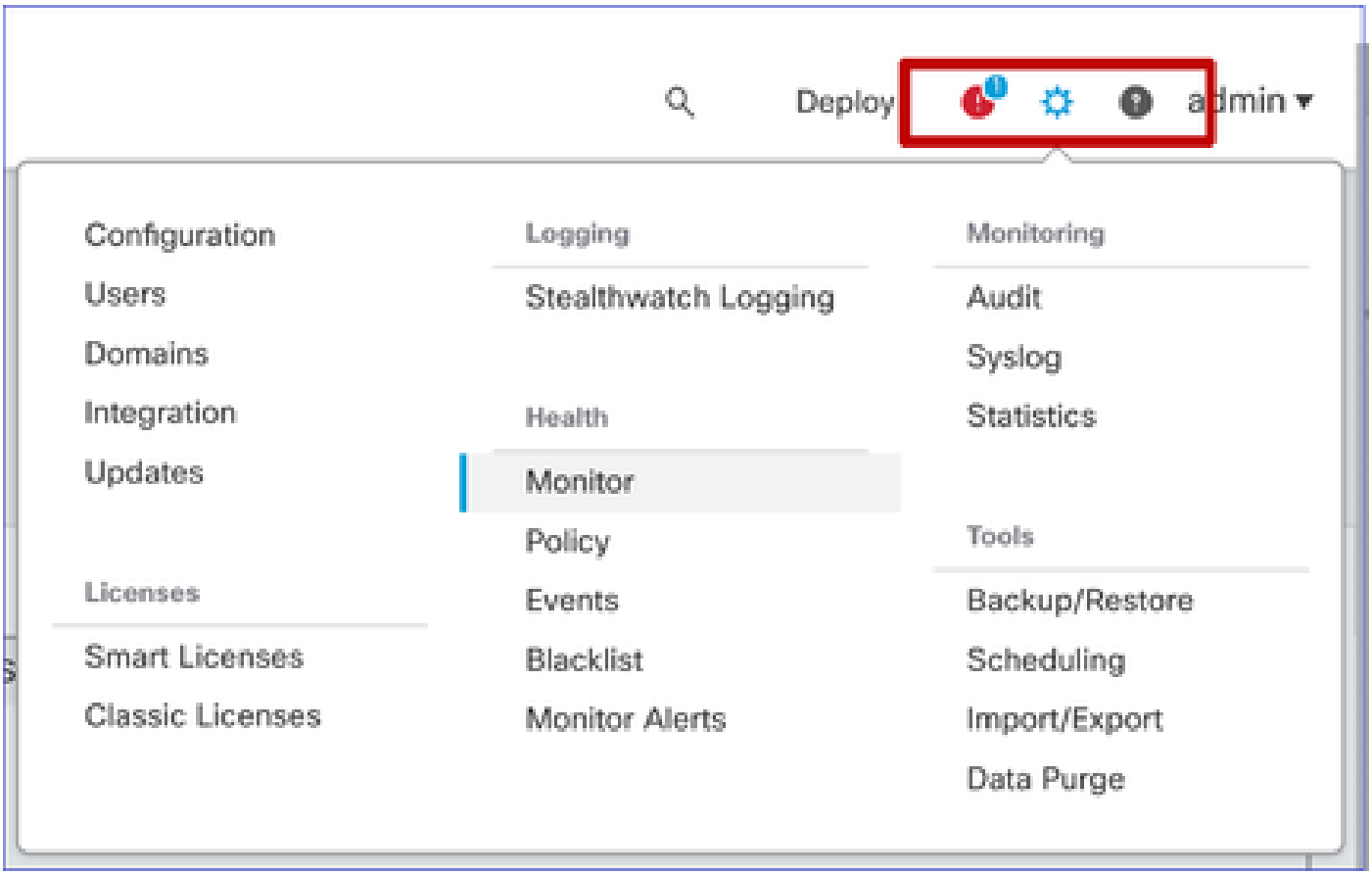
- Nouvelle interface utilisateur sur FMC qui fournit des graphiques de tendances, des superpositions et des tableaux de bord personnalisés.
- API FTD : rend les mêmes métriques disponibles pour la requête par des entités externes

Résumé des limites :

- La fonctionnalité n'est pas prise en charge sur FDM GUI ou CDO
- La surveillance de FMC dans la nouvelle interface utilisateur de surveillance de l'état n'est pas prise en charge.
- Les intervalles d'interrogation ne sont pas configurables. Vous ne pouvez pas configurer différents intervalles d'interrogation pour différents périphériques. Tous sont interrogés à intervalles fixes d'une minute.

Exemples de déploiement

- Aucun déploiement spécifique n'est nécessaire pour tester la fonctionnalité. Mettez simplement à niveau FMC et le périphérique vers FP 6.7.
- Les données de contrôle d'état sont disponibles dans le tableau de bord d'état FMC, accessible depuis l'onglet Système.



Conditions préalables et plates-formes prises en charge

Plates-formes logicielles et matérielles minimales prises en charge

Version min. du gestionnaire supportée	Périphériques gérés	Version minimale du périphérique géré prise en charge requise	Remarques
FMC 6,7	DFT 6,7	FXOS 2.9.1 DFT 6,7	Pris en charge uniquement sur les FTD
API REST du périphérique FTD	DFT 6,7	FXOS 2.9.1 DFT 6,7	API REST du périphérique FTD uniquement (pas les interfaces utilisateur graphiques FDM ou CDO)

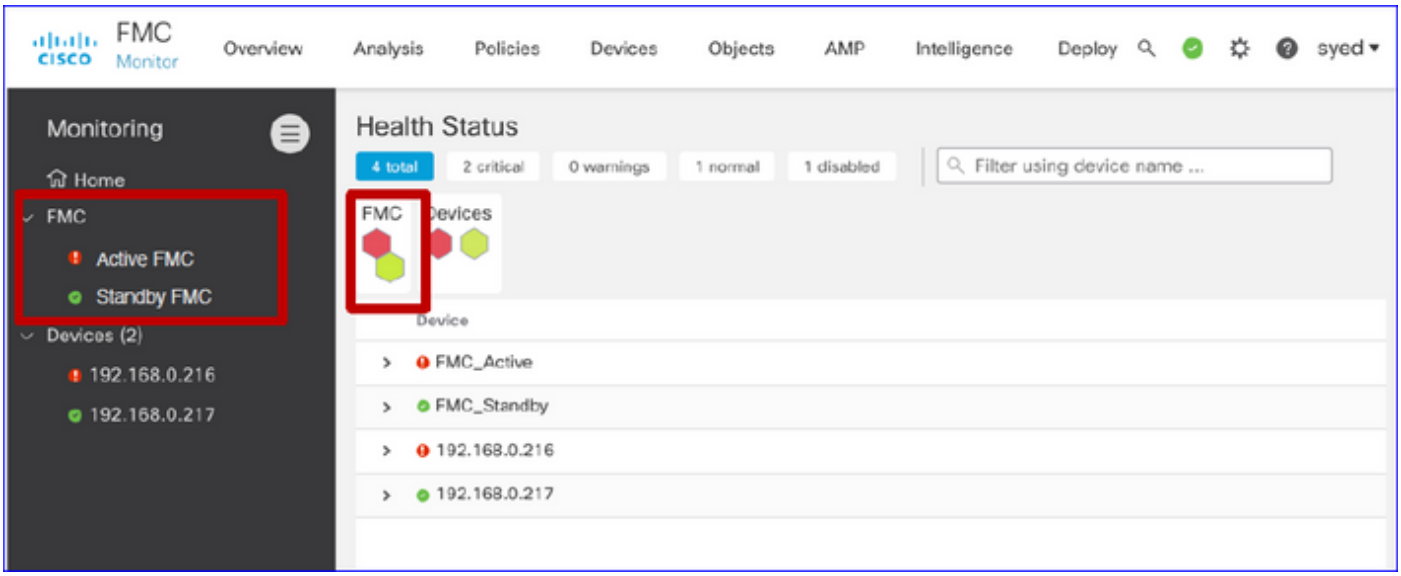
Interfonctionnement

Aucune exigence spécifique d'interopérabilité.

Détails des fonctionnalités 7.0

Interface utilisateur FMC : autonome et assistance haute disponibilité

Navigation dans la page Health Monitoring



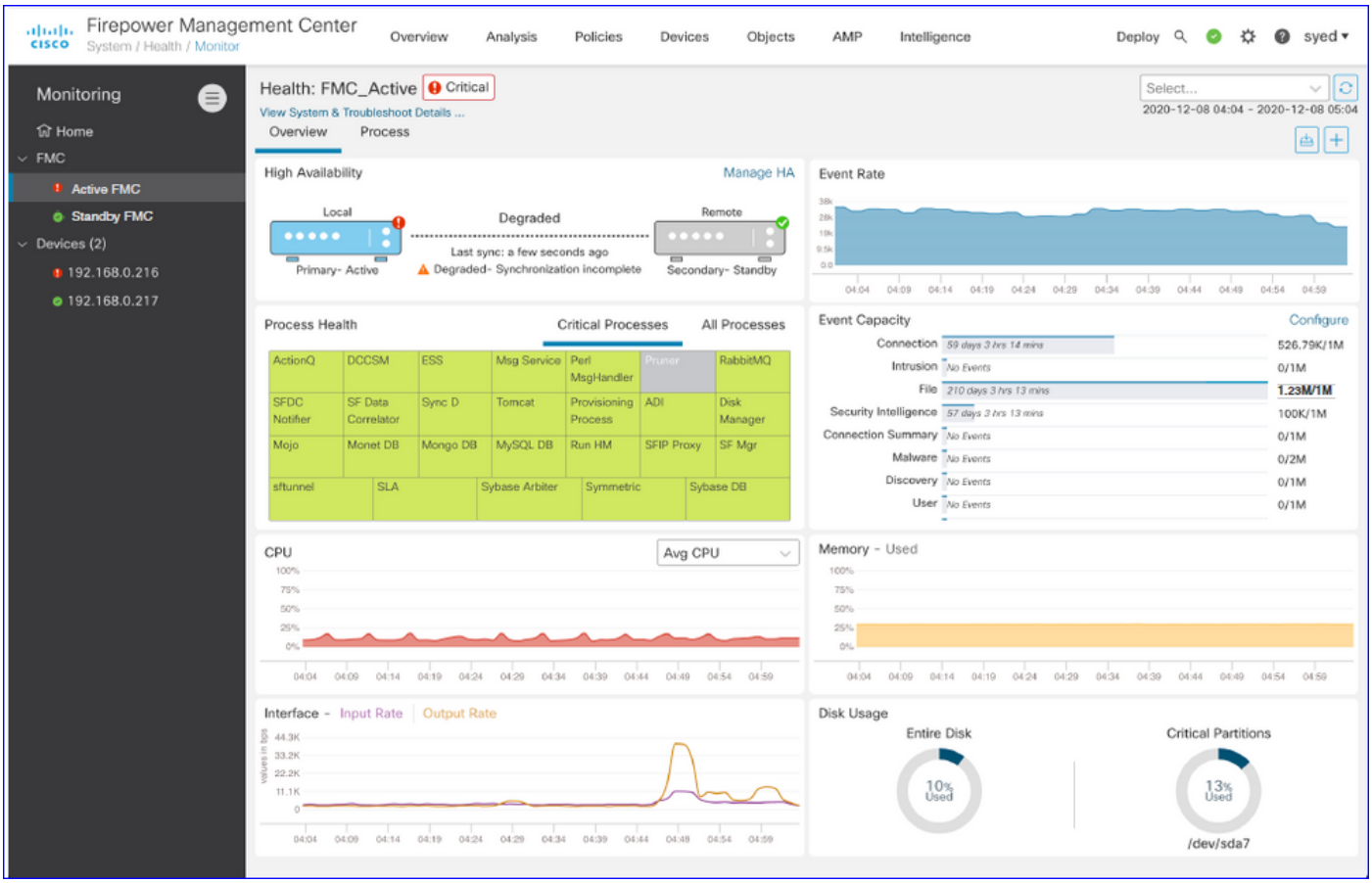
- Le FMC autonome est représenté sous la forme d'un noeud unique
- FMC HA représenté sous la forme d'une paire de noeuds
- Chaque FMC est affiché avec l'état de santé

État de santé

- FMC HA est représenté en double hexagone.
- Les périphériques FMC actifs et en veille sont également répertoriés dans le tableau des alertes.

Tableau de bord FMC

Tableau de bord de surveillance de l'état FMC dans 7.0



Vue récapitulative de :

- Haute disponibilité
- Débit et capacité des événements
- Intégrité du processus
- CPU
- Mémoire
- Interface
- Disque

Ce tableau de bord est disponible pour les FMC actifs et en veille. L'utilisateur peut créer des tableaux de bord personnalisés pour surveiller les mesures de son choix.

Tableau de bord FMC : panneau haute disponibilité FMC

Le panneau HA affiche

- État actuel de haute disponibilité
- Actif ou En veille
- Heure de la dernière synchronisation
- Intégrité des périphériques

Tableau de bord FMC : taux d'événements et capacité

Taux D'Événements

- Taux d'événements maximum comme ligne de base
- Taux d'événements global reçu par FMC

Capacité des événements

- Consommation actuelle par catégorie d'événement
- Temps de rétention des événements
- Comparatif Actuel/Maximum

capacité événementielle

- Marqueur de dépassement de capacité

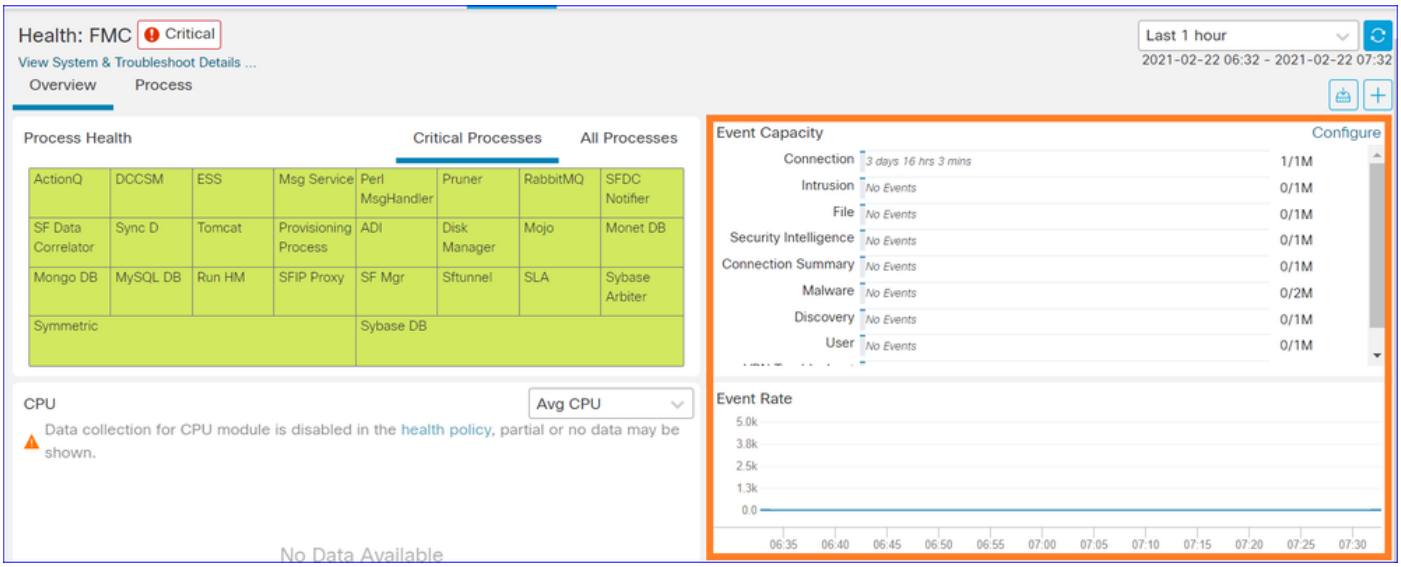
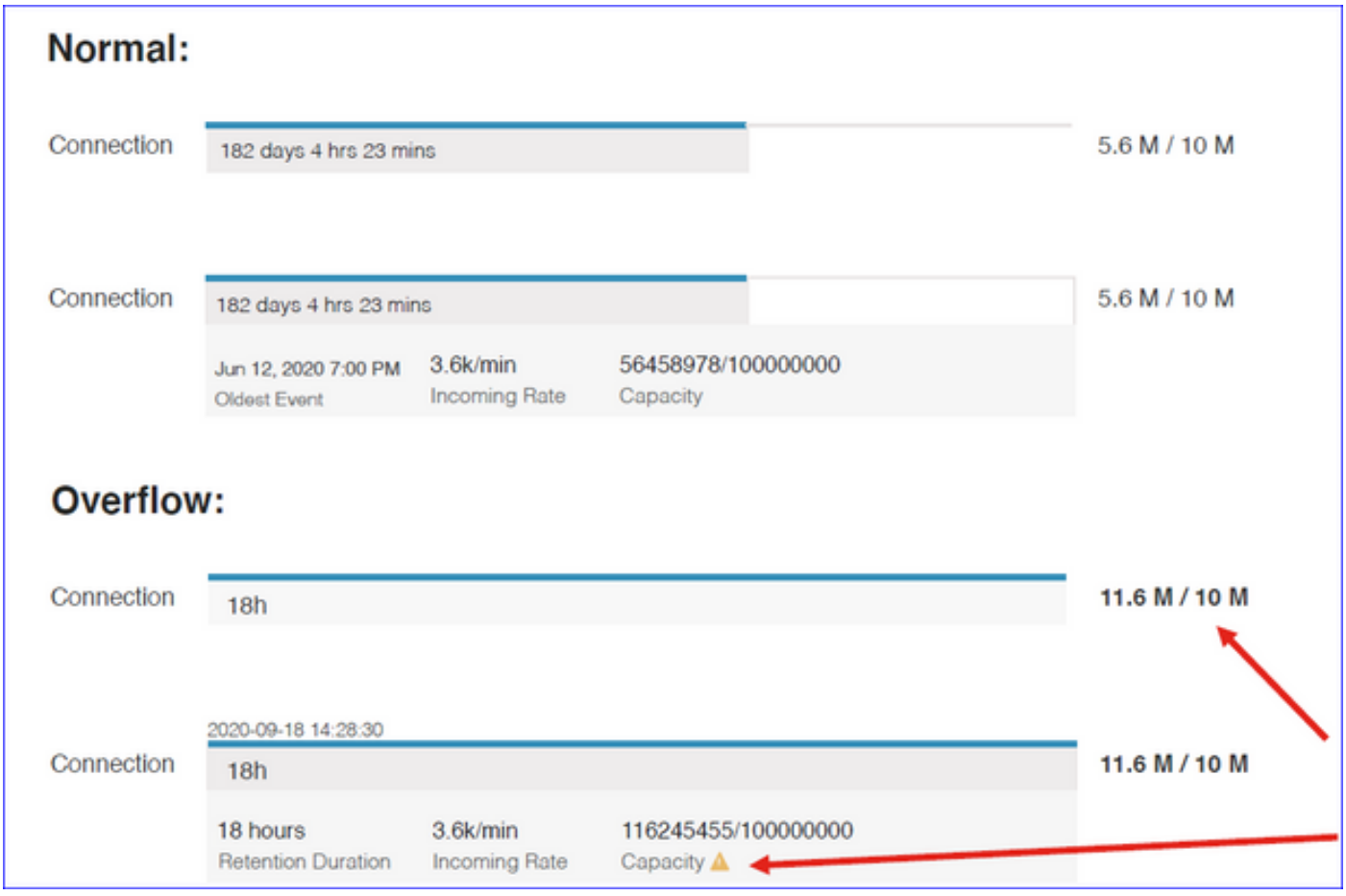


Tableau de bord FMC : capacité des événements

État De Consommation De Capacité En Événement Normal



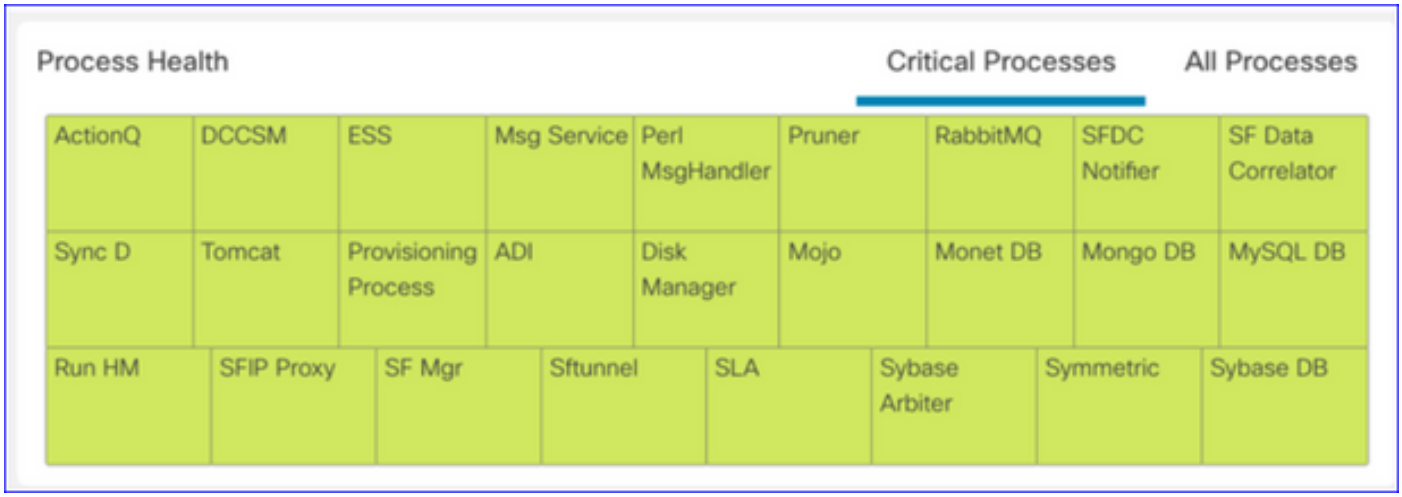
Scénario de dépassement, lorsque les événements sont stockés au-delà de la capacité maximale configurée.

- Le texte en gras indique un débordement
- Une icône d'avertissement met en évidence le dépassement de capacité

Tableau de bord FMC : panneau de processus FMC

Le panneau Processus critiques affiche

- État actuel du processus
- Nombre de redémarrages de processus



Le panneau des processus affiche les mesures suivantes pour tous les processus « pmconfig » :

- État actuel
- Utilisation du processeur
- Utilisation de la mémoire

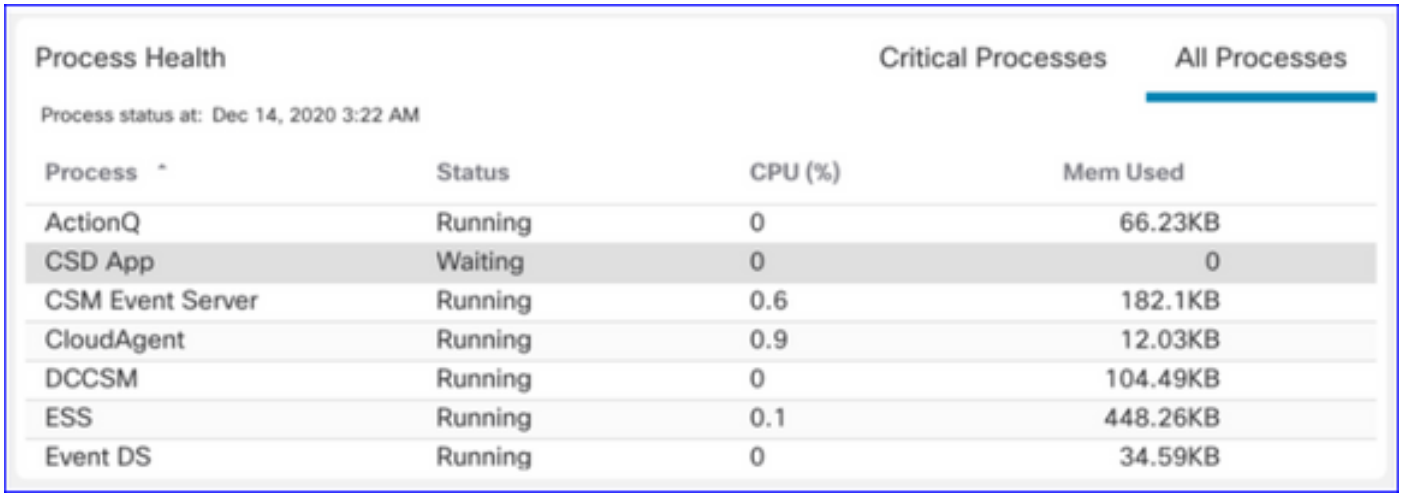


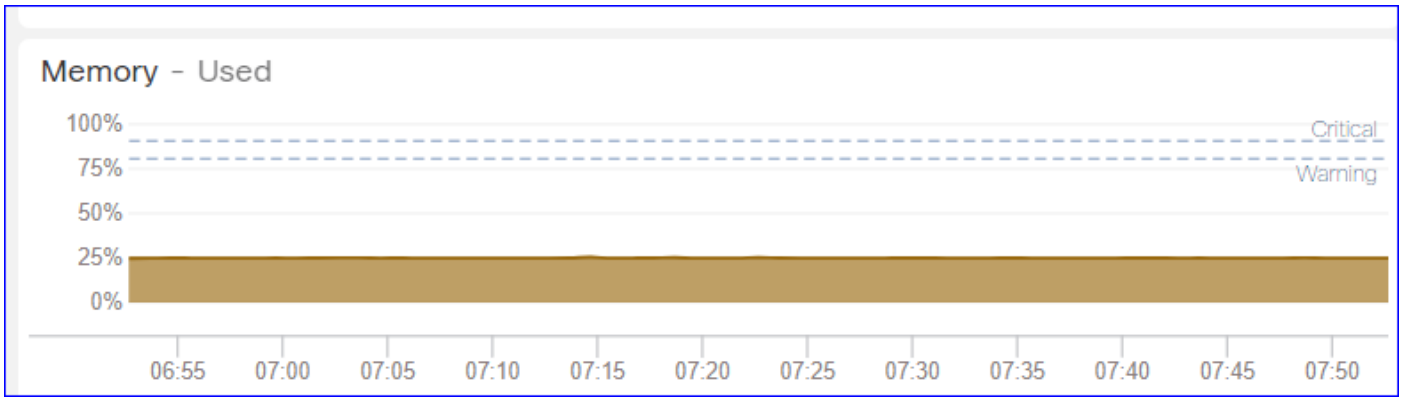
Tableau de bord FMC : processeur FMC

Le panneau UC affiche

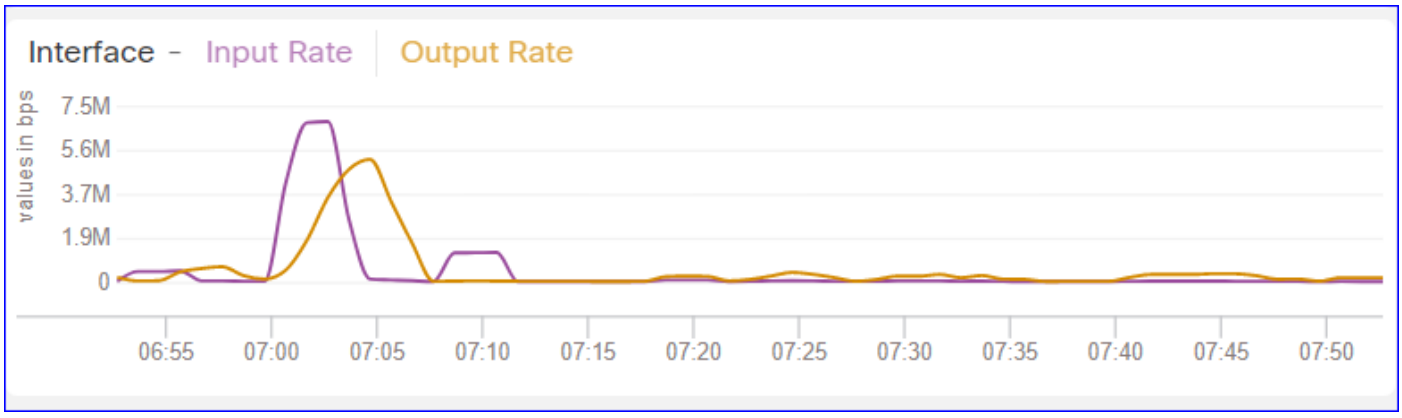
- Processeur moyen (par défaut)
- Tous les coeurs

Tableau de bord FMC : autres panneaux

Le panneau Mémoire affiche l'utilisation globale de la mémoire sur FMC



Le panneau d'interface affiche le débit d'entrée/sortie moyen de toutes les interfaces

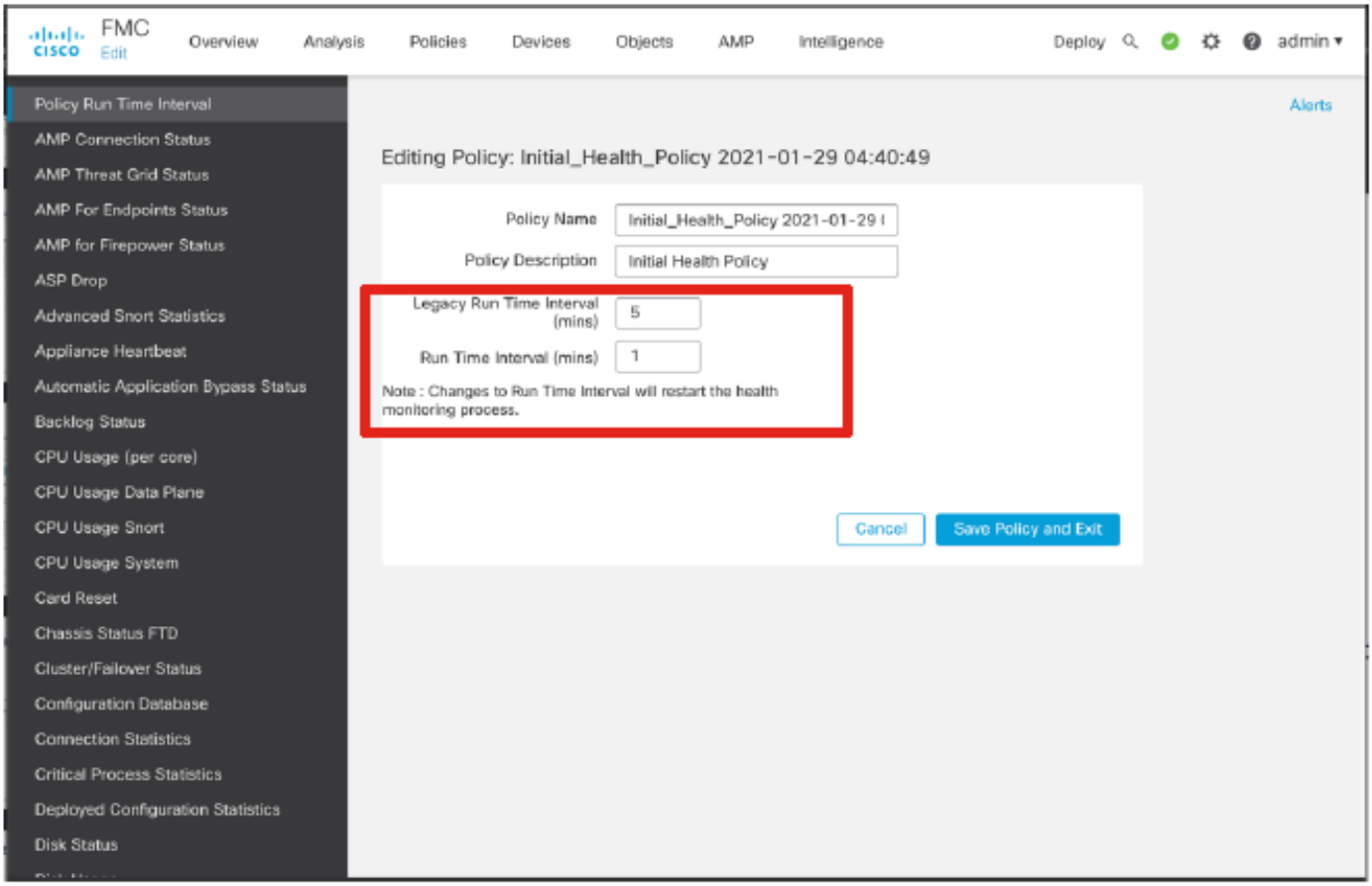


Le panneau Disque affiche

- Capacité totale du disque
- Capacité de partition critique où les données FMC sont stockées

Intervalle d'exécution

- L'intervalle d'exécution de l'ancien module d'intégrité est renommé « Intervalle d'exécution hérité »
- « Run Time Interval » cible les nouveaux modules de santé basés sur Telegraf
- Paramètre global, affecte tous les périphériques

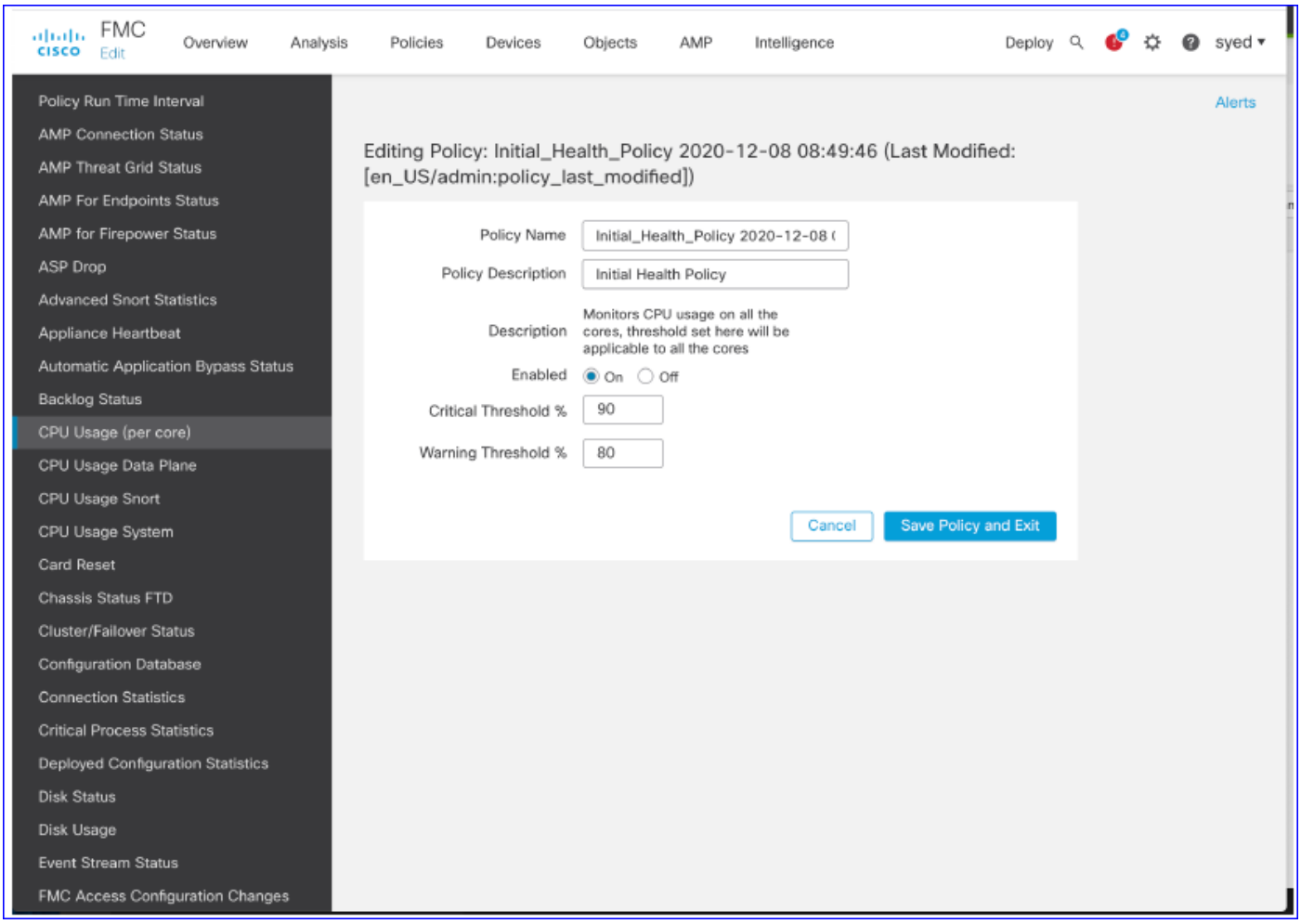


Mesures disponibles

Mesures disponibles pour les tableaux de bord personnalisés

- Si un utilisateur souhaite créer un tableau de bord personnalisé, ces diapositives constituent un guide des mesures disponibles.

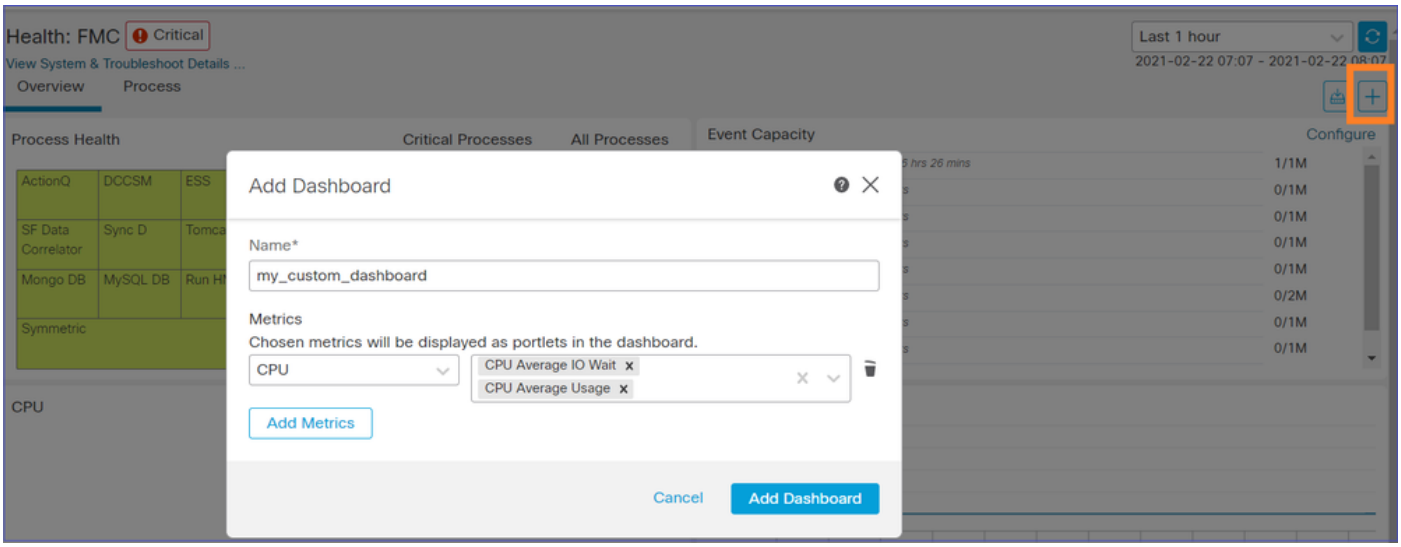
- Certaines mesures doivent être activées dans la stratégie d'intégrité avant de pouvoir être utilisées dans un tableau de bord d'intégrité personnalisé



Interface utilisateur FMC : tableau de bord personnalisé FMC

Nouvelles catégories de mesures de surveillance FMC dans 7.0

- CPU
- Mémoire
- Interface
- Disque
- Événement
- Process
- RabbitMQ
- Sybase
- MySQL



Interface utilisateur FMC : mesures FMC

40 mesures ajoutées dans différentes catégories (disponibles dans le tableau de bord personnalisé). Pour activer les mesures désactivées, activez le module d'intégrité correspondant dans la stratégie d'intégrité associée (Système > Intégrité > Stratégie).

Nom du groupe de mesures	Activé par défaut	Description
CPU	Non	Surveille le processeur FMC
Mémoire	Oui	Surveille la mémoire FMC
Disque	Oui	Surveille l'utilisation des disques FMC
Interface	Oui	Surveille l'interface FMC
Process	Oui	Surveille les processus FMC
Événement	Oui	Surveille le taux d'événements
MySQL	Non	Surveille MySQL
RabbitMQ	Non	Moniteurs RabbitMQ

Sybase	Non	Surveille Sybase

FTD : mesures introduites dans FP 7.0

Activé par défaut : les mesures sont collectées par défaut. Afin d'activer les métriques désactivées, activez le module d'intégrité correspondant dans la politique d'intégrité associée (Système > Intégrité > Politique).

Nom du groupe de mesures	Activé par défaut	Description	Plateforme
État du châssis	Oui	Surveille différents paramètres du châssis, tels que la vitesse et la température du ventilateur.	Applicable uniquement aux plates-formes FPR2100 et FPR1000
Décharge de flux	Oui	Surveille les statistiques de déchargement du flux matériel	Applicable au FPR9300 et FPR4100
Gouttes ASP	Oui	Surveille les pertes de paquets côté Lina	tout
Nombre de visites	Non	Surveille le nombre de résultats pour les règles de stratégie de contrôle d'accès	tout
État d'AMP Threat Grid	Oui	Surveille la connectivité à AMP ThreatGrid	tout
État de la connectivité AMP	Non	Surveille la connectivité du cloud AMP à partir du FTD	tout
État du connecteur SSE	Non	Surveille la connectivité du cloud SSE à partir du FTD	tout
État NTP	Non	Surveille les paramètres de synchronisation d'horloge	tout

		NTP sur le FTD	
Statistiques VPN	Oui	Surveille les statistiques du tunnel VPN S2S et RA	tout
Statistiques de route	Oui	Surveille les pertes de paquets côté Lina	tout
Statistiques des performances de Snort 3	Oui	Surveille certaines statistiques de performances Snort3 (perfstats)	tout
Compteurs xTLS	Non	Surveille les flux xTLS/SSL, la mémoire et l'efficacité du cache	tout

API REST, Syslog, SNMP

Aucune nouvelle API REST FMC ou FTD Device n'a été introduite dans la version 7.0. Les API REST existantes prennent en charge les nouvelles métriques ajoutées à la version 7.0.

Syslog et SNMP

Syslog

- Aucun changement dans syslog pour le moniteur d'intégrité

SNMP

- RUBRIQUE D'INFORMATIONS DISTINCTE pour « Surveillance de l'état des périphériques SNMP »

Intégration de produits SAL/CTR/tiers

- Informations à fournir distinctes pour la prise en charge d'Azure Application Insights
- Aucune modification spécifique n'a été apportée pour prendre en charge l'intégration du « Health Monitoring » avec SAL/CTR/SecureX
- L'API REST peut être exploitée pour l'intégration tierce

Technologie logicielle

Caractéristiques détaillées 6.7

Nouvelle surveillance de l'état du pare-feu de nouvelle génération

Aide les utilisateurs à

- Débogage réactif, comme l'analyse de la cause première du problème après qu'il se soit produit
- Des actions proactives telles que la surveillance des niveaux d'utilisation et de saturation pour identifier les problèmes potentiels de capacité et aider ainsi les utilisateurs à améliorer ou refactoriser la capacité.

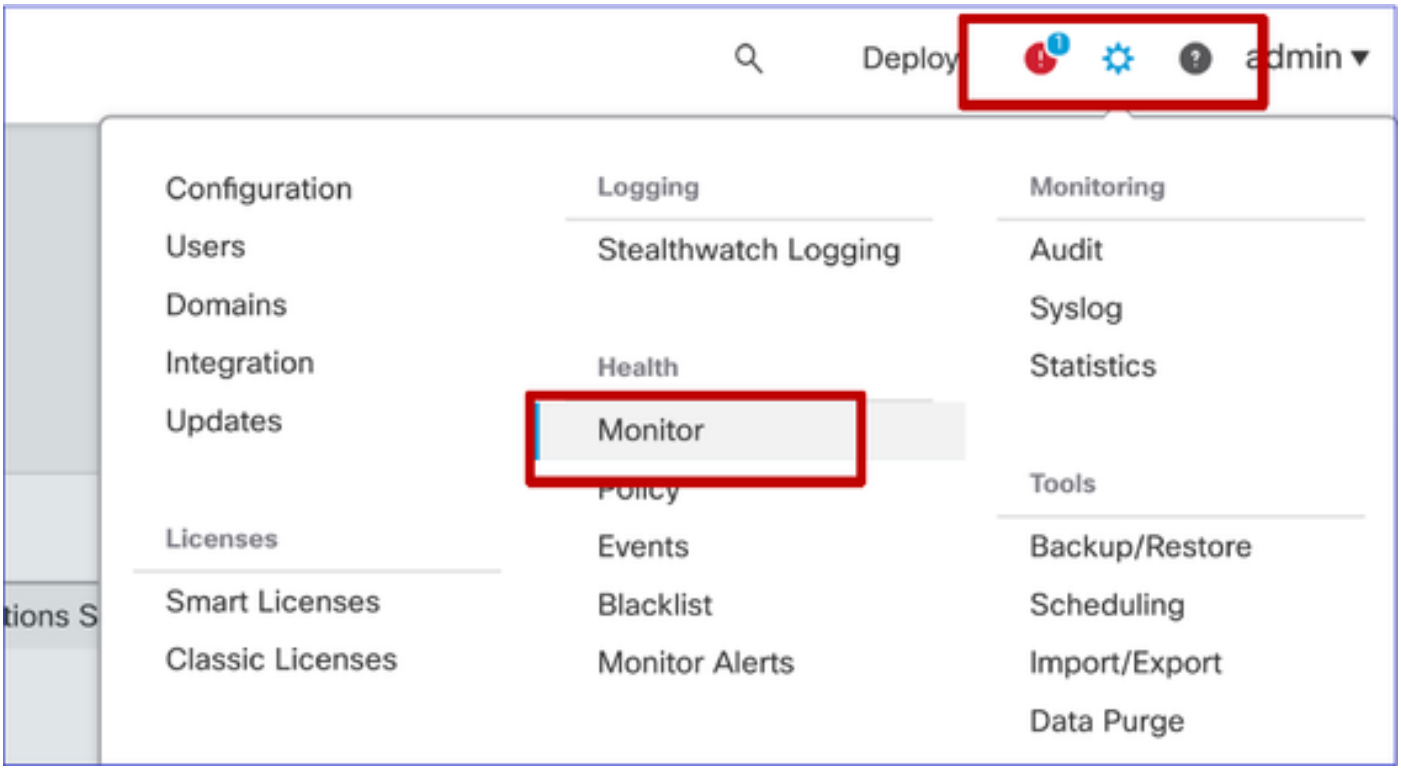
Points saillants

- Graphiques de tendance : les graphiques de tendance permettent de détecter très facilement les anomalies et de déterminer la cause première des problèmes. Avec l'inspection visuelle, les tendances peuvent être repérées et des corrélations peuvent être tracées entre différentes métriques pour trouver une relation causale entre elles.
- Recouvrement d'événements : les recouvrements d'événements affichent des informations importantes, telles que le déploiement de la configuration et les mises à jour SRU sur les graphiques de tendances pour indiquer les relations causales.
- Tableaux de bord personnalisables : les utilisateurs peuvent créer leurs propres tableaux de bord pour regrouper les mesures qu'ils souhaitent voir ensemble sur une page.
- Architecture de surveillance unifiée de la santé : point unique de collecte et d'exportation des indicateurs, quel que soit le responsable « intéressé » par ces indicateurs. Les API FTD et le FMC utilisent les données du même collecteur de mesures.
- Extensibilité des métriques : l'un des objectifs de l'architecture de la plate-forme était de pouvoir ajouter facilement de nouvelles métriques. Pour ce faire, des outils de collecte et de stockage de mesures Open Source et des tableaux de bord personnalisables sont utilisés.

Interface graphique FMC

Interface utilisateur FMC : accéder à l'état de santé

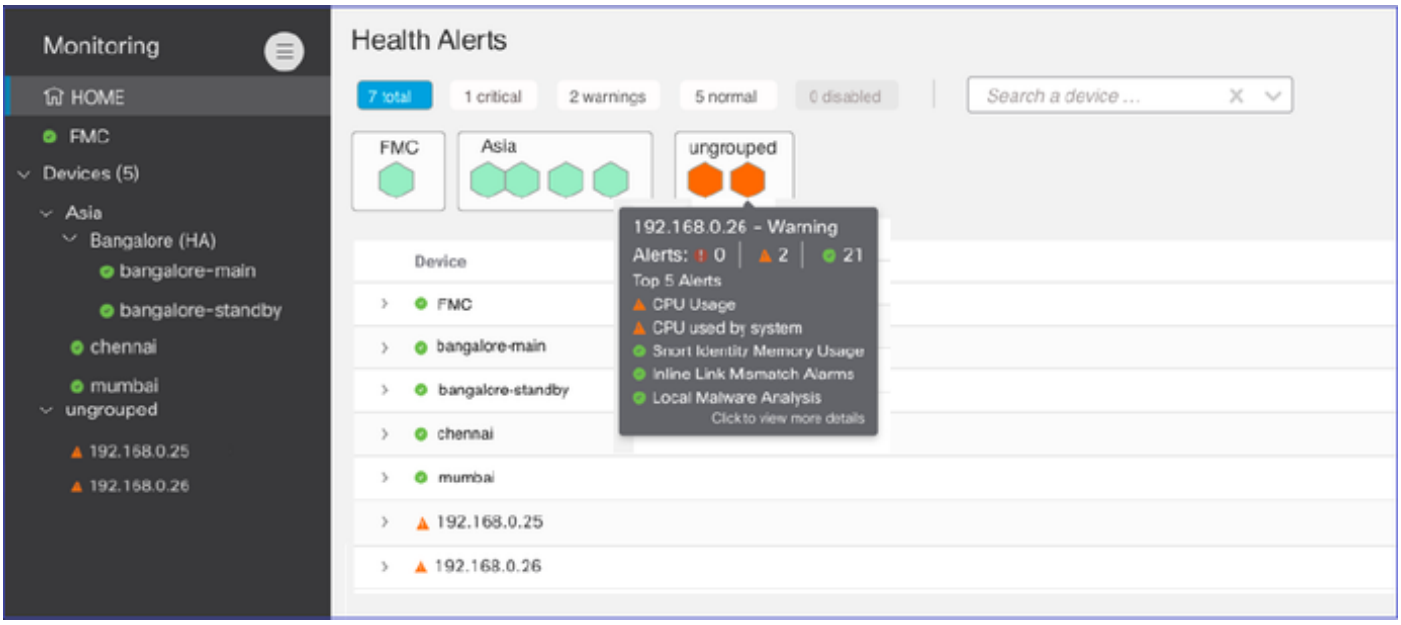
Sur FMC, cliquez sur l'icône System **>** Health **>** Monitor pour accéder à la page Health Status.



Interface utilisateur FMC : page New Health Status

La page Health Status (Etat de santé) est conçue pour présenter un aperçu de l'état de santé de tous les périphériques gérés par le FMC, y compris l'état de santé du FMC.

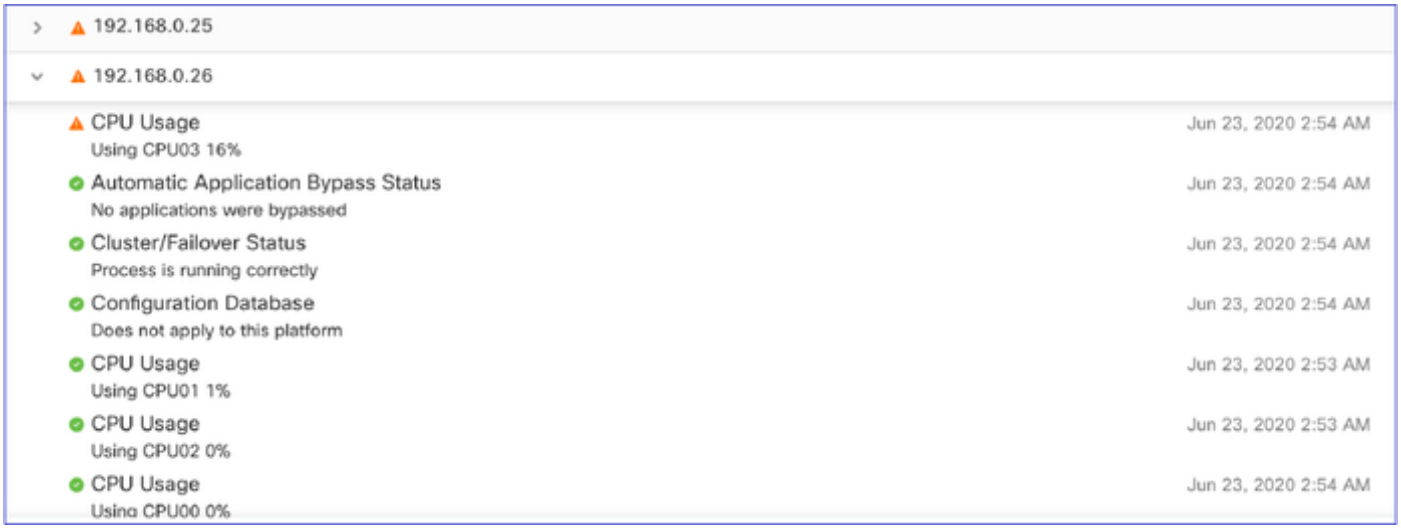
- Les périphériques sont regroupés en fonction de leur groupe/ha/cluster.
- Un point à gauche du périphérique indique son état de santé
- Vert - pas d'alarme
- Orange - au moins une mise en garde
- Rouge - au moins une alarme de santé critique
- Le résumé de l'état de santé s'affiche lorsque vous placez le curseur sur l'hexagone représentant l'état du périphérique.
- Les seuils d'avertissement et de critique peuvent être configurés dans la politique de santé, de la même manière qu'ils l'étaient avant FP 6.7.



Interface utilisateur FMC : Événements d'intégrité des périphériques

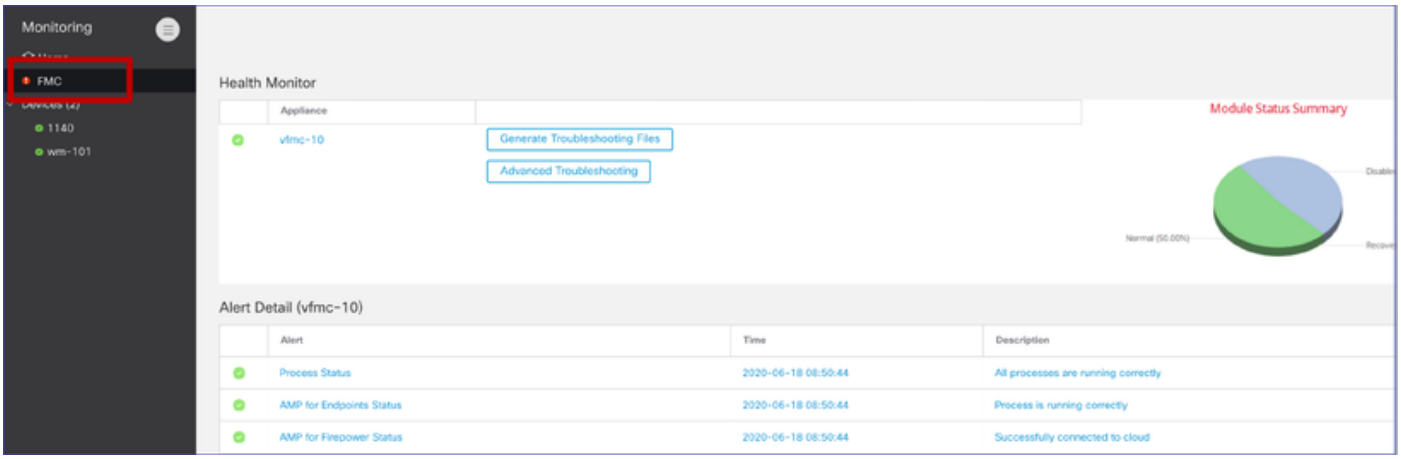
Cliquez sur le périphérique dans le panneau inférieur pour afficher les événements d'intégrité associés au périphérique. Les alertes sont triées par leur état d'intégrité (gravité).

Page Surveillance de la santé



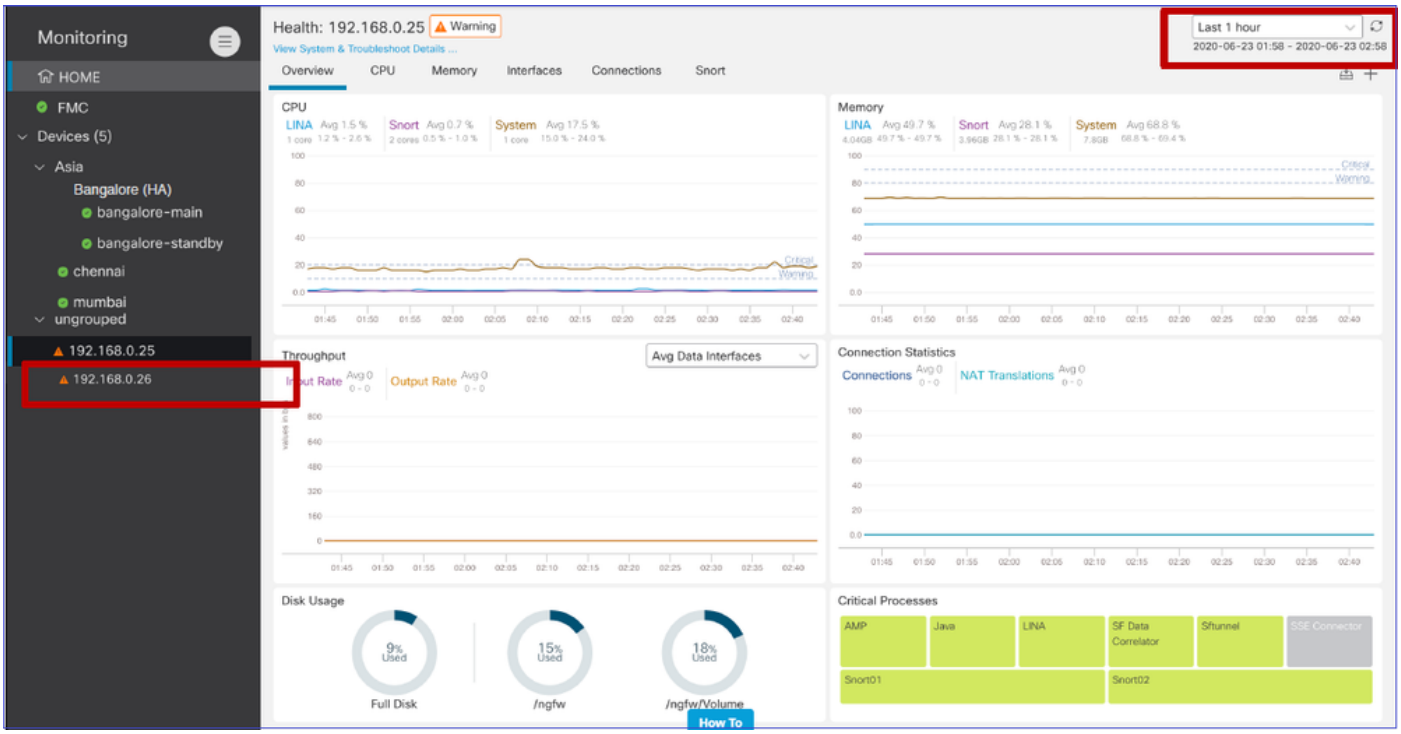
Interface utilisateur FMC : la surveillance de l'état FMC est inchangée

La page d'intégrité FMC est toujours la page héritée. La nouvelle interface utilisateur est prise en charge uniquement pour FTD avec 6.7+



Interface utilisateur FMC : nouveau ! Tableaux de bord

- Cliquez sur le nom du périphérique dans le volet de gauche pour accéder à la page de présentation de l'état du périphérique.
- La présentation de l'état de santé contient tous les principaux graphiques de tendance des indicateurs de santé.
- Différentes plages de temps sont disponibles (par défaut, la dernière heure)
- Actualisation automatique pour recharger le graphique



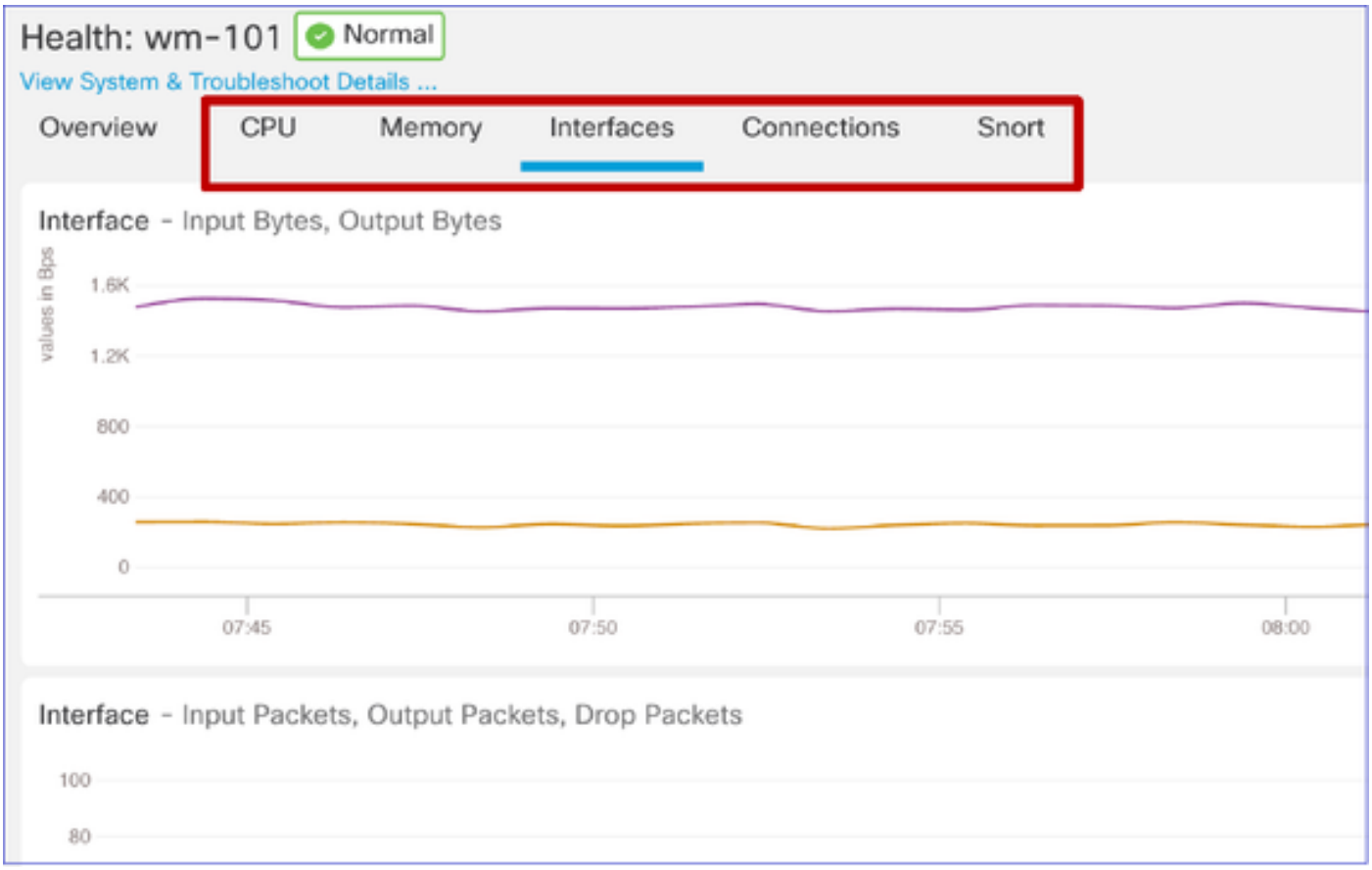
Interface utilisateur FMC : superposition des données de déploiement

Cliquez sur l'icône de déploiement pour afficher les détails de superposition de déploiement sur le graphique avec la plage de temps sélectionnée

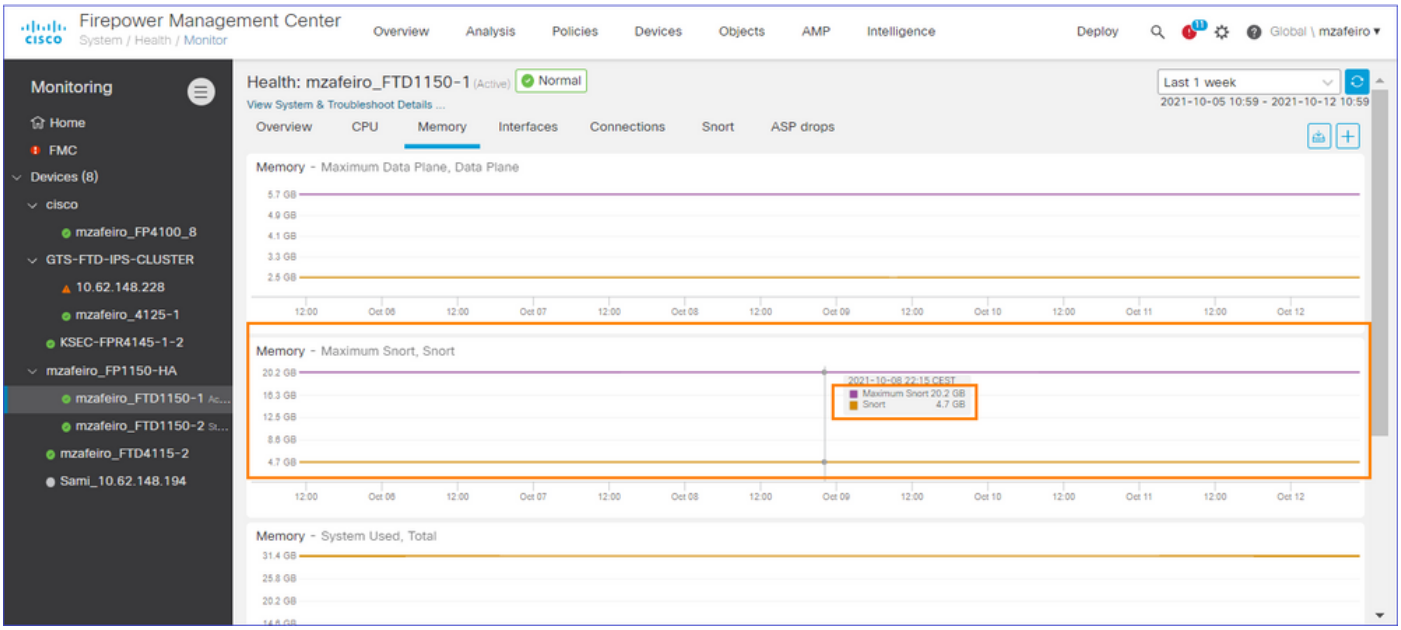
- L'icône indique le nombre de déploiements au cours de la période sélectionnée
- La bande indique les heures de début et de fin du déploiement.
- En cas de déploiements multiples, plusieurs bandes/lignes apparaissent
- Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails

Interface utilisateur FMC : tableaux de bord préconfigurés pour les périphériques

- L'interface utilisateur FMC contient des tableaux de bord d'intégrité prédéfinis.
- Ces tableaux de bord préconfigurés sont fournis avec des mesures associées regroupées.
- Le tableau de bord de l'interface présente un graphique de tendance pour toutes les mesures liées à l'interface, telles que les octets d'entrée/sortie, les paquets et la taille moyenne des paquets pour les différentes interfaces.



Mémoire FTD Snort - D'où provient-elle ?

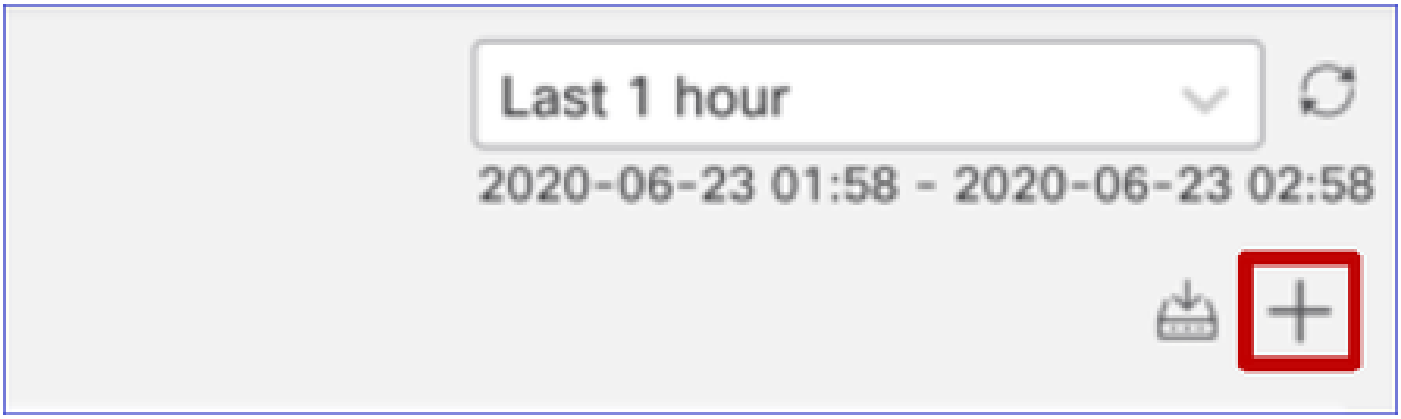


Interface utilisateur FMC : possibilité de créer des tableaux de bord personnalisés

Les utilisateurs peuvent créer leur propre tableau de bord personnalisé

- Outre les tableaux de bord prédéfinis, un utilisateur peut également créer des tableaux de bord personnalisés.

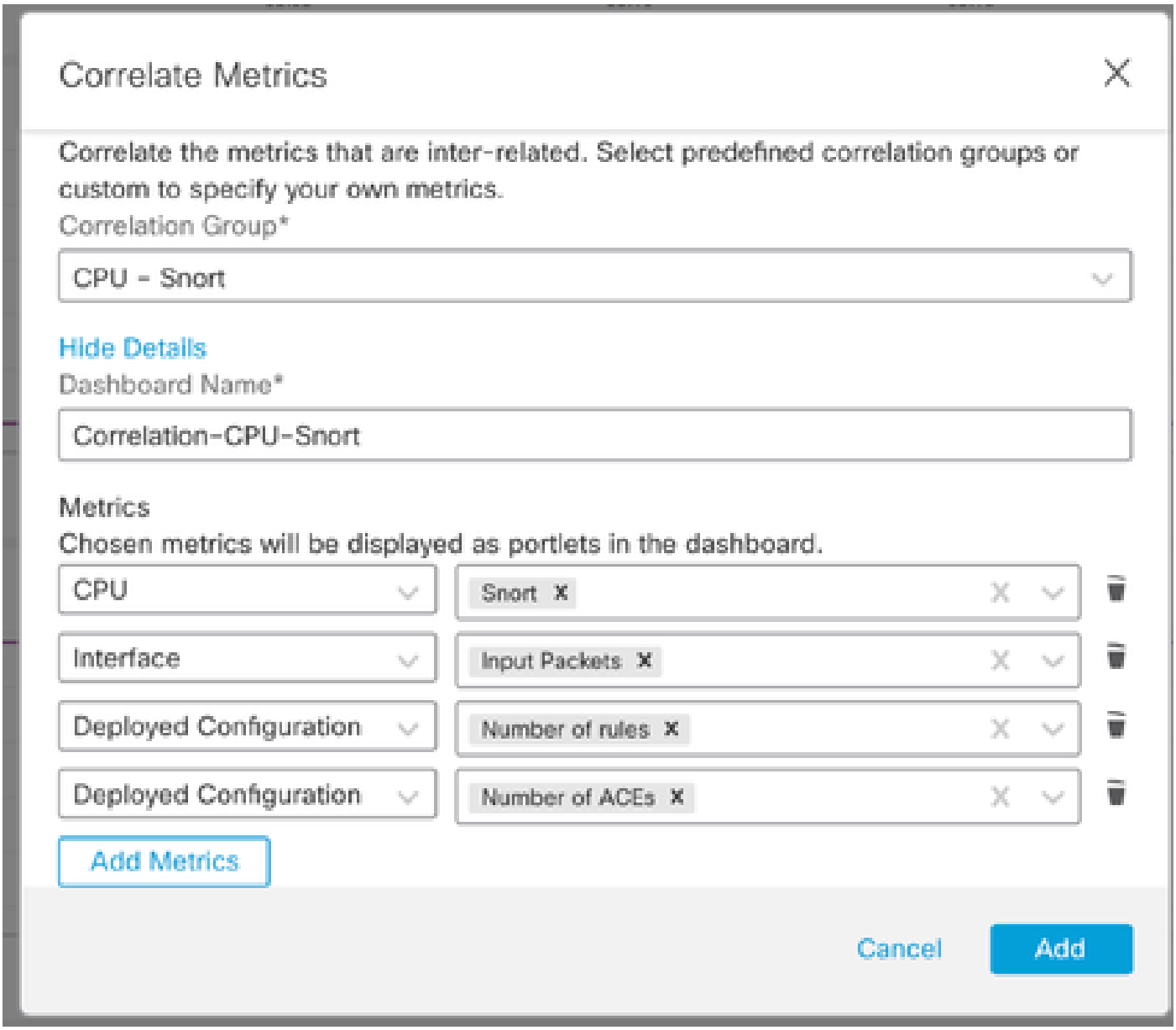
- Dans le tableau de bord personnalisé, un nombre illimité de mesures peut être ajouté.
- En règle générale, un tableau de bord personnalisé est créé si les mesures de différents groupes de mesures peuvent être corrélées pour déterminer la cause première d'un problème.
- En cas de CPU Lina élevé, on peut voir les connexions entrantes par seconde (CPS), les statistiques d'interface (et ainsi de suite) qui peuvent faire monter le CPU.



Interface utilisateur FMC : créer un tableau de bord personnalisé

Boîte de dialogue Corréler les indicateurs

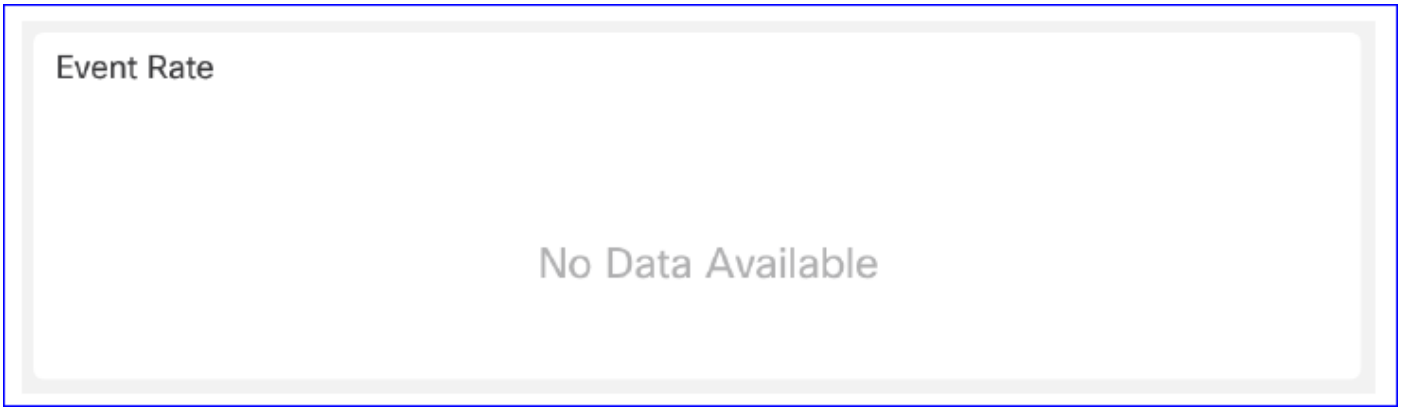
- Lorsqu'un utilisateur clique sur « + » pour créer un tableau de bord personnalisé, la fenêtre Corréler les mesures s'ouvre.
- Un utilisateur peut ajouter différentes mesures qu'il souhaite surveiller ensemble.



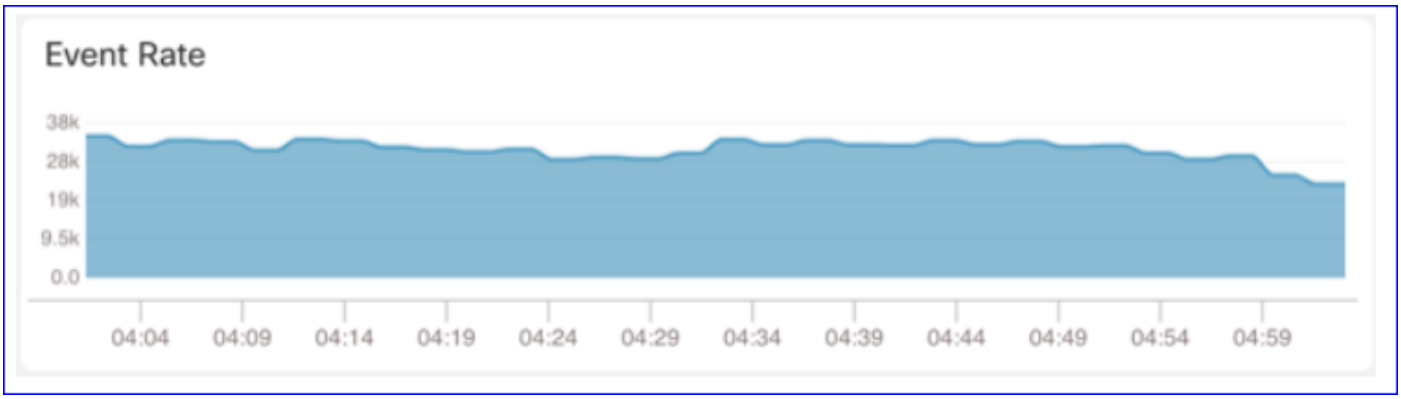
Collecte de données à partir de (périphérique) - GUI

Données d'un intervalle de temps affichées dans l'interface utilisateur graphique

Lorsque le moniteur d'intégrité ne dispose pas de données pour la plage de temps sélectionnée, l'interface utilisateur graphique affiche « Aucune donnée disponible » dans le panneau du tableau de bord :



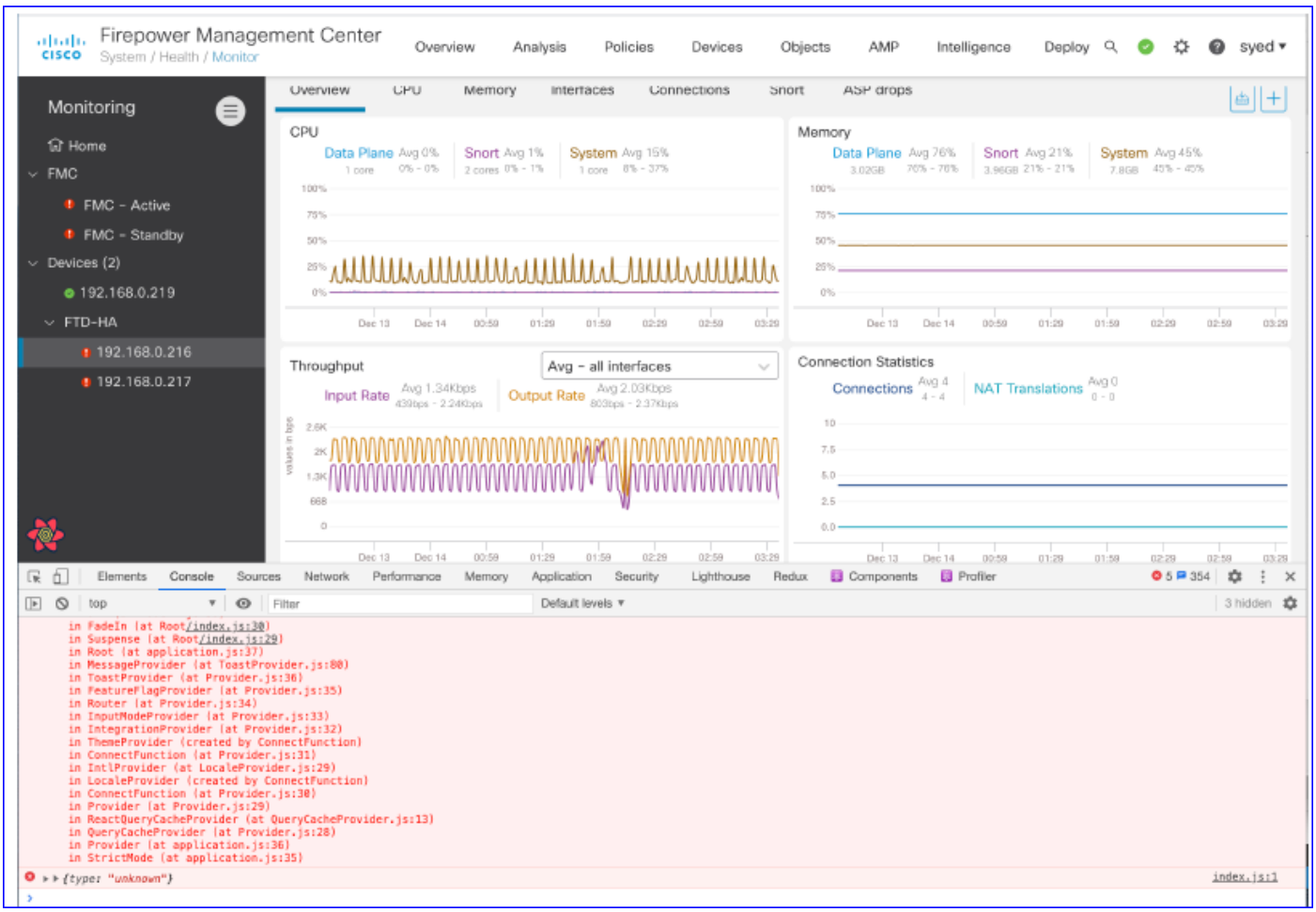
Si des données sont disponibles, le graphique apparaît comme suit :



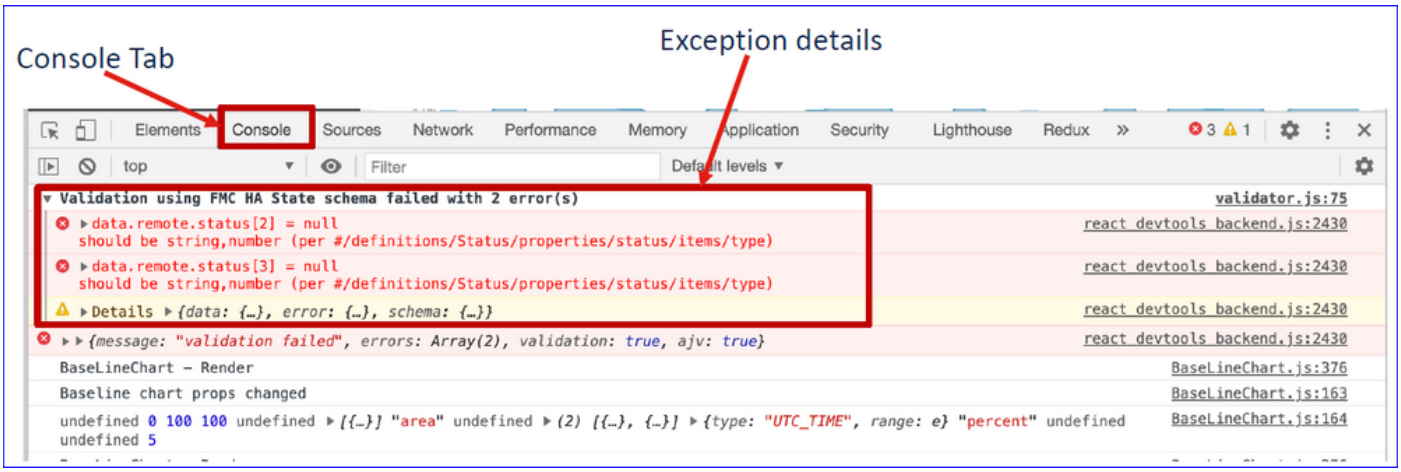
Utiliser les onglets Console et Réseau du navigateur

Journal de la console du navigateur et journal des appels réseau

- Dans cet exemple, la console de développement du navigateur Chrome est affichée
- En cas d'erreur, les détails des exceptions sont affichés dans le journal de la console



Exemple de journal de console de navigateur



Références

[Surveillance de l'état de santé FMC - 6.7]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.