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

Table des matières

Introduction
Informations de fond
Présentation des fonctionnalités
Détails des fonctionnalités 7.0
FTD : mesures introduites dans FP 7.0
Caractéristiques détaillées 6.7

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 soussystèmes 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 soussystèmes 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.

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

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

cisco FMC Monitor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	0	۵ () syed ▼
Monitoring The Home FMC Active FMC Standby FMC Devices (2) 192.168.0.217 9 192.168.0.217		Health S	Catus Conticat Continue Contin	0 warnings	1 normal	1 disabled	C. Filter u	ing device	name	ð		

- 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

Firepower Manage System / Health / Monitor	ement Cer	nter ov	erview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	० 📀 🌣	Ø syed▼		
Monitoring (重) 얇 Home	Health: F View System Overview	MC_Activ & Troubleshoo Process	e 🔒 Critica t Details	al						Sele 2020	ect -12-08 04:04 -	2020-12-08 05:04		
V FMC	High Availa	ability					Manage HA	Event Rate	9					
 Active FMC Standby FMC Devices (2) 192.168.0.216 192.168.0.217 	Primar	Local Degraded Remote Last sync: a few seconds ago Degraded Synchronization incomplete Secondary- Standby								04:29 04:34 04:39	04.39 04.44 04.48 04.54 04.59			
e rozirodioler/	Process H	ealth		(Critical Proce	esses A	II Processes	Event Cap	acity			Configure		
	ActionQ	DCCSM	ESS	Msg Service	Peri MsgHandler	Pruner	RabbitMQ	(Connection 59 days 3 hrs 14 mins Intrusion No Events		526. 0/1M 1.23			
	SFDC SF Da Notifier Corra	SF Data Correlator	Sync D	Torncat	Provisioning Process	Provisioning ADI Disk Process Manager		Security I	ntelligence 57 days 3 hrs 13 mins			100K/1M		
	Mojo Monet DB		Mongo DB	Mongo DB MySQL DB Run HM			SFIP Proxy SF Mgr		Malware No Events		0/1M 0/2M			
	sftunnel	SLA		Sybase Arbiter	Symmetric	s Syb	ase DB		Discovery No Events User No Events		0/1M 0/1M			
	CPU 100% 75% 50% 25% 0% 04:04	04:09 04:14	04:19 04:24	0129 013	4 04:39 04:	Avg CF	U ~	Memory - 100% 50% 25% 0% 0%	Used	04.29 04.34 04.39	04:44 04:49	04:54 04:59		
	Interface - 644.3K 133.2K 11.1K 0 04:04	Interface - Input Rate Output Rate 33.3K 13.3K 11.1K 0 04:04 04:09 04:14 04:19 04:24 04:29 04:34 04:39 04:44 04:49 04:54 04:59					Disk Usag	e Entire Disk		Critical Partition	ns			

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

High Availability	Configure
Local Degraded Last sync: a few seconds ago Primary- Active Degraded- Synchronization incomplete	Remote Secondary- Standby FMC_Standby - Critical Alerts: 2

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

Health: Fl View System 8 Overview	MC OCrit Troubleshoo Process	tical ot Details s						Last 1 hour 2021-02-22 06:32 -	2021-02-22 07:32
Process He	alth			Crit	tical Proce	sses A	II Processes	Event Capacity	Configure
ActionQ	DCCSM	ESS	Msg Service	Perl	Pruner	RabbitMQ	SFDC	Connection 3 days 16 hrs 3 mins Intrusion No Events	1/1M
05.0	00		Devisionis	MsgHandler	Dist		Notifier	File No Events	0/1M
Correlator	Sync D	Tomcat	Provisioning Process	ADI	Manager	Mojo	Monet DB	Security Intelligence No Events	0/1M
Mongo DB	MySQL DB	Run HM	SFIP Proxy	SF Mgr	Sftunnel	SLA	Sybase	Connection Summary No Events	0/1M
Symmetric	Symmetric Sybase DB						Arbiter	Discovery No Events User No Events	0/1M 0/1M
CPU Data coll shown.	Avg CPU Data collection for CPU module is disabled in the health policy, partial or no data may be shown.						U 🗸	Event Rate 5.0k 3.8k 2.5k 1.3k 0.0	
			No Data	Available	e			06:35 06:40 06:45 06:50 06:55 07:00 07:05 07:10 07:15 07:20	07:25 07:30

Tableau de bord FMC : capacité des événements

État De Consommation De Capacité En Événement Normal

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

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

rocess He	ealth			Cri	tical Proc	cesses A	ses All Processes			
ActionQ	DCCSM	ESS	Msg Service	g Service Perl MsgHandler			RabbitMC	SFDC Notifier	SF Data Correlator	
Sync D	Tomcat	Provisioning Process	ADI	Disk Manager	Mojo er		Monet DE	3 Mongo DB		
Run HM	Run HM SFIP Proxy SF Mgr		Sftunne	I SLA	Syb		ase ter	Symmetric	Sybase DB	

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

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

Process Health		Crit	tical Processes	All Processes
Process status at: Dec 14, 2020 3:22	M			
Process *	Status	CPU (%)	Mem U	sed
ActionQ	Running	0	66	.23KB
CSD App	Waiting	0		0
CSM Event Server	Running	0.6	18	2.1KB
CloudAgent	Running	0.9	12	.03KB
DCCSM	Running	0	104	.49KB
ESS	Running	0.1	448	.26KB
Event DS	Running	0	34	.59KB

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

CISCO Edit Overview Analy	vsis Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	0	ø	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	Po	Policy Name	Initial_Hea	alth_Policy	2021-01-29 (
Advanced Snort Statistics Appliance Heartbeat	Legacy Ro Run Time	un Time Interva (mins) e Interval (mins)	5								
Automatic Application Bypass Status Backlog Status CPU Usage (per core)	Note : Changes monitoring pro-	s to Run Time Int cess.	ierval will restar	t the health							
CPU Usage Data Plane CPU Usage Snort CPU Usage System					Cancel	Save Policy and Exit					
Card Reset Chassis Status FTD Cluster/Feilover Status											
Configuration Database Connection Statistics											
Critical Process Statistics Deployed Configuration Statistics Disk Status											

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

cisco Edit Overview Analysis	Policies Devices	Objects AM	P Intelligence	Deploy	۹ 🚱	۵	0 s	syed 🔻
Policy Run Time Interval AMP Connection Status AMP Threat Grid Status AMP For Endpoints Status	Editing Policy: Initial_I [en_US/admin:policy_	Health_Policy 202 _last_modified])	20-12-08 08:49:46 (I	Last Modified:				Alerts
AMP for Firepower Status ASP Drop Advanced Sport Statistics	Policy Narr Policy Descriptio	Initial_Health_Pearth_Pearth	olicy 2020-12-08 (
Appliance Heartbeat	Descriptic	Monitors CPU usag cores, threshold se applicable to all the	e on all the t here will be cores					
Automatic Application Bypass Status Backlog Status	Enable Critical Threshold	ed On Off % 90						
CPU Usage (per core) CPU Usage Data Plane	Warning Threshold	% 80						
CPU Usage Snort CPU Usage System			Cancel	Save Policy and Exit				
Card Reset 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								

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

Health: FN View System 8 Overview	Crit Troubleshoo Process	tical ot Details	S	Last 1 hour C 2021-02-22 07:07 - 2021-02-22 08:07
Process Hea	alth		Critical Processes All Processes Event Capacity	Configure
ActionQ	DCCSM	ESS	Add Dashboard	1/1M 0/1M
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	

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.

Monitoring 😑	Health Alerts
ଲି HOME	7 total 1 critical 2 warnings 5 normal 0 disabled Search a device X V
 FMC Devices (5) Asia 	FMC Asia ungrouped 192.168.0.26 - Warning
 Bangalore (HA) bangalore-main 	Device Alerts: 9.0 Alerts 9.0 21
bangalore-standby	FNC CFU Usage CFU usad by system
o chennai	bangalore-main Snort Identity Memory Usage
o mumbai ∽ ungrouped	bangalcre-standby local Malware Analysis Local Malware analysis
A 192.168.0.25	> Clickeo view more details
A 192.168.0.26	> 🔕 mumbai
	> 🛕 192.168.0.25
	> ▲ 192.168.0.26

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

>	▲ 192.168.0.25	
~	▲ 192.168.0.26	
	▲ CPU Usage Using CPU03 16%	Jun 23, 2020 2:54 AM
	 Automatic Application Bypass Status No applications were bypassed 	Jun 23, 2020 2:54 AM
	 Cluster/Failover Status Process is running correctly 	Jun 23, 2020 2:54 AM
	 Configuration Database Does not apply to this platform 	Jun 23, 2020 2:54 AM
	CPU Usage Using CPU01 1%	Jun 23, 2020 2:53 AM
	CPU Usage Using CPU02 0%	Jun 23, 2020 2:53 AM
	CPU Usage Using CPU00 0%	Jun 23, 2020 2:54 AM

Interface 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+

Monitoring	Health	Monitor	_			
© 1140 © 1140 © wm-101	0	Applance vlmc-10	Generate Troubleshooting Files Advanced Troubleshooting		Nermal (50.00%)	Module Status Summary Duale Deale
	Alert D	etail (vfmc-10)				
		Alert		Time	Description	
	•	Process Status		2020-06-18 08:50:44	All processes are running correctly	
	•	AMP for Endpoints Status		2020-06-18 08:50:44	Process is running correctly	
	0	AMP for Firepower Status		2020-06-18 08:50:44	Successfully connected to cloud	

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

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
ि HOME	Overview CPU Memory Interfaces Connections Snort	± +
FMC	CPU	Memory
 Devices (5) 	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 % 4.0408 49.7 % - 49.7 % 3.9608 28.1 % - 28.1 % 7.808 68.8 % - 69.4 %
✓ Asia	100	100 Colori.
Bangalore (HA)	80	80
bangalore-main	60	60
bangalore-standby	40	40
😑 chennai	20Wayna	20
⊚ mumbai ∽ ungrouped	0.0 01.45 01.50 01.56 02.00 02.05 02.10 02.15 02.20 02.25 02.39 02.35 02.40	0.0 0146 0150 0155 0200 0205 0210 0215 0220 0225 0230 0225 0240
▲ 192.168.0.25	Throughput Avg Data Interfaces V	Connection Statistics
▲ 192.168.0.26	In sut Rate Avg 0 0 - 0 0 - 0	Connections Avg 0 0+0 NAT Translations Avg 0 0+0
	800 440 320 140 0 0 0 0 0 0 0 0 0 0 0 0 0	100 80 40 20 0.0 0.1/6 01.56 01.56 02.00 02.05 02.10 02.15 02.20 02.25 02.30 02.35 02.49
	Disk Usage	Critical Processes
	9%, Used 15%, Full Disk /ngfw /ngfw/Volume	AMP Java LINA SF Data Correlator Snort01 Snort02

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

	Health: 192.168.0.21 Normal View System & Troubleshoot Details Overview CPU Memory Interfaces Connections Sn	Last 1 hour 2020-06-23 02:26 - 2020-06-23 03:26 ort +
	CPU Snort Avg 0.9 % System Avg 16.0 % 1 core 0.5 % - 1.6 % 2 cores 0.0 % - 8.5 % 1 core 13.0 % - 75.0 % 100	
CPU LINA Avg 2.7 % Snort 1 core 0.5% -7.8% 2 cores 0 100 60 40 20 0.0 0.0 08.30	Avg 3.7 % System Avg 19.1 % 1 core 14.0 % - 30.0 %	CPU LINA Myg 2.7 % Snort Avg 4.3 % System Avg 20.6 % 1 core 0.5 % - 8.2 % 2 cores 0.0 % - 15.5 % System Avg 20.6 % 1 core 140 % - 750 % 100

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.

Hea	Health: wm-101 Normal View System & Troubleshoot Details									
Ov	erview	CPU	Memory	Interfaces	Connections	Snort				
Inte	erface - Ir	put Bytes, (Output Bytes							
8	1.6K									
values	1.2K									
	800									
	400									
	0									
		07:45		07:50	07	:55	08:00			
Inte	erface - Ir	put Packets	s, Output Pack	ets, Drop Pack	ets					
10	0									
ŧ	30									

Mémoire FTD Snort - D'où provient-elle ?

Firepower Manage CISCO System / Health / Monitor	ement Cent	er _{Overviev}	v Analysis	Policies	Devices	Objects	AMP I	ntelligence		Depk	by Q	6 ⁰⁰ ¢	Global \ mzafeiro ¥
Monitoring	Health: m: View System &	zafeiro_FTD1 Troubleshoot Detai	150-1 (Active) (Normal							La 202	st 1 week 1-10-05 10:	✓ ○ ▲ 59 - 2021-10-12 10:59
යි Home	Overview	CPU N	femory Inte	rfaces Co	onnections	Snort A	SP drops						a +
FMC	Memory - I	Maximum Data Pl	ane. Data Plane										
 Devices (8) 	57.08												
∨ cisco	4.9 GB												
mzafeiro_FP4100_8	4.1 GB												
✓ GTS-FTD-IPS-CLUSTER	3.3 GB												
A 10.62.148.228	2.5 G8												
mzafeiro_4125-1	12:00	Oct 08	12:00	Oct 07 1.	2:00 Oct	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12
KSEC-FPR4145-1-2	Memory -	Maximum Snort. :	Snort										
v mzafeiro_FP1150-HA	20.2 GB						2021	-10-08 22:15 CES	T				
e mzafeiro_FTD1150-1 Ac	16.3 GB						M Sr	aximum Snort 20.2 nort 4.7	GB GB				
mzafeiro_FTD1150-2 s	12.5 GB												
mzafeiro_FTD4115-2	8.8 GB												
Sami_10.62.148.194	1.1 00												
	12:00	Oct 08	12:00	Oct 07 1.	2:00 Oct	12:00	Oct 09	12:00	Oct 10	12:00	Oct 11	12:00	Oct 12
	Memory -	System Used, Tot	al										
	31.4 GB												
	25.8 GB												
	20.2 GB												-

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.

Correlate Metrics			×
Correlate the metrics that are inf custom to specify your own met Correlation Group*	er-related. Select predefined co rics.	orrelation gro	oups or
CPU - Snort			~
Hide Details Dashboard Name*			
Correlation-CPU-Snort			
Metrics Chosen metrics will be displayed	d as portlets in the dashboard.		
CPU 🗸	Snort X	2	× v T
Interface \lor	Input Packets X		× v T
Deployed Configuration \lor	Number of rules X		× v T
Deployed Configuration \lor	Number of ACEs X	3	× v 🗑
Add Metrics			
		Cancel	Add

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 :

Event Rate	
	No Data Available

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

Console Tab Exception details	S			
Elements Console Sources Network Performance Memory Application Security	ity Lighthouse Redux » 🛛 🔉 🗛 1 🔯 🗄 🗙			
🕩 🚫 top 🔻 🕢 Filter Defailt levels 🔻	\$			
v Validation using FMC HA State schema failed with 2 error(s)				
<pre>> bdata.remote.status[2] = null should be string,number (per #/definitions/Status/properties/status/items/type)</pre>				
<pre> bedata.remote.status[3] = null should be string,number (per #/definitions/Status/properties/status/items/type) react devtools backend.js:24 </pre>				
▲ ▶ Details ▶ {data: {}, error: {}, schema: {}}	react devtools backend.js:2430			
S ► ► {message: "validation failed", errors: Array(2), validation: true, ajv: true}				
BaseLineChart - Render BaseLineChart.js:376				
Baseline chart props changed BaselineChart.js:10				
undefined 0 100 undefined > [{}] "area" undefined > (2) [{}, {}] > {type: "UTC_TIME", range: e} "percent" undefined undefined 5				
	- ··· ·· · · · · · · · · · · · · · · ·			

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.