Note de version
GCAP V2.5.5.0

GATEWATCHER

Version du manuel : V1

Date de création : Janvier 2026

Date de mise à jour : Janvier 2026

Table des matières

Chapitre 1

Présentation de la version 2.5.5.0 du GCap

Cette note de version décrit :

- les nouvelles fonctionnalités
- les améliorations et autres caractéristiques
- les correctifs
- les problèmes connus
- la comptabilité logicielle
- la compatibilité matérielle
- la procédure de mise à jour

Chapitre 2

Nouvelles fonctionnalités

2.1 Moteur de détection Sigflow

2.1.1 Mise à jour du moteur

Le moteur Sigflow a été mis à jour.
Cette mise à jour contient de nouvelles fonctionnalités et les correctifs pour les vulnérabilités critiques publiées précédemment.

2.1.2 Gestion du multi-tenant

La fonctionnalité de multi-tenant a été améliorée.
Lorsqu'un nouveau ruleset est appliqué, le monteur de détection effectue un rechargement des règles, sans redémarrage.

2.1.3 Support de nouveaux protocoles OT

Le support des protocoles suivants a été ajoutés :

- S7COMM
- OPCUA
- CCSDS
- DICOM
- HL7
- BACnet

2.1.4 Support de l'ERSPAN pour la capture des flux

Il est maintenant possible d'utiliser ERSPAN pour pouvoir créer un tunnel GRE entre une interface de monitoring du GCap et une interface du commutateur afin d'envoyer les flux à inspecter.

Il est possible de filtrer les événements du protocole SMB en fonction des opérations effectuées au travers de ce-dernier.

2.1.5 Shellcode-Detect / Powershell-Detect : ajout du community-id

Le community-id a été ajouté dans les évènements générés par les moteurs Shellcode-Detect et Powershell-Detect.

2.2 Virtualisation de la sonde

2.2.1 Support AWS

Le support d'AWS a été amélioré.

2.3 Système

2.3.1 Mise à jour du système

Le système a été mise à jour.

2.3.2 Gestion des logs

Certains journaux éphémères sont maintenant conservés après redémarrage de la sonde, pour faciliter le diagnostic en cas de problèmes.

2.3.3 Interface ligne de commandes

L'autocomplétion est maintenant disponible pour le nom des interfaces réseaux.

2.4 Installation

2.4.1 Prérequis du stockage

Il est possible d'installer une sonde GCap sur une partition de 100 Go.

2.4.2 Support UEFI

Le support de l'UEFI a été amélioré.

2.5 Processus de mise à jour

Le processus de mise à jour avec un retour arrière possible a été amélioré.

Chapitre 3

Autres caractéristiques et améliorations

Section laissée vide intentionnellement

Chapitre 4

Correctifs

4.1 Après la mise à jour, erreur dans l'exécution de commandes avec certaines versions de matériel

Certaines commandes sont non-fonctionnelles pour certaines versions de matériel à la suite d'une mise à jour en 2.5.4.0.
Ce problème est corrigé en v2.5.5.0.

4.2 Sigflow : erreur lors du démarrage du moteur de détection

Sur certains modèles de GCap, le moteur de détection ne démarre pas si plus de deux interfaces de capture sont activées.
Ce problème est corrigé en v2.5.5.0.

4.3 Sigflow : les filtres XDP ne s'appliquent pas correctement

Dans certains cas, les filtres XDP ne s'appliquent pas correctement.
Ce problème est corrigé en v2.5.5.0.

4.4 Sigflow : la réception de paquets spécifiques du protocole Modbus peut provoquer un redémarrage du moteur

Lors de l'activation du protocole Modbus, la réception d'un paquet spécifique peut provoquer le redémarrage du moteur
Ce problème est corrigé en v2.5.5.0.

4.5 Netdata : absence de certaines métriques

Certaines métriques ne sont plus récupérées par Netdata dans la version 2.5.4.0.
Ce problème est corrigé en v2.5.5.0.

4.6 Sigflow : problème de démarrage du moteur de détection

Dans certains cas, le moteur de détection Sigflow ne démarre pas correctement à l'initialisation du système.
Ce problème est corrigé en v2.5.5.0.

4.7 Netdata : valeur erronée

Dans certains cas, Netdata renvoie une valeur erronée pour le statut du moteur de détection.
Ce problème est corrigé en v2.5.5.0.

4.8 Système : paramètres de performance inadaptés

Certains paramètres du système ne sont pas optimisés pour les performances.
Ce problème est corrigé en v2.5.5.0.

4.9 Système : installation impossible

Dans certains cas, l'installation du GCap n'est pas possible.
Ce problème est corrigé en v2.5.5.0.

4.10 Sigflow : problème avec les interfaces cluster

Lors de l'utilisation d'interface cluster, une perte importante de paquets pourrait avoir lieu.
Ce problème est corrigé en v2.5.5.0.

4.11 Sigflow : problème d'allocation mémoire pour certains flux

L'allocation mémoire pour certains flux n'est pas optimisée.
Ce problème est corrigé en v2.5.5.0.

4.12 Système : saturation de l'espace de stockage du GCap

Lors de l'analyse d'une quantité importante de flux en continue, l'espace de stockage du GCap peut saturer.
Ce problème est corrigé en v2.5.5.0.

4.13 Système : répartition des CPUs

Pour certains modèles de GCap la répartition des CPUs n'est pas optimale.
Ce problème est corrigé en v2.5.5.0.

4.14 Système : sélection par défaut dans le menu de démarrage

Suite à une mise à jour du GCap, il est possible, par inadvertance, de sélectionner l'entrée déclenchant un retour arrière.
Ce problème est corrigé en v2.5.5.0.

4.15 Sigflow : options permettant le débogage

Certaines options permettant le débogage du système sont activées par défaut.
Ce problème est corrigé en v2.5.5.0.

4.16 Mise à jour : problème au redémarrage

Un problème peut intervenir au redémarrage du système après une mise à jour.
Ce problème est corrigé en v2.5.5.0.

4.17 Sigflow : Problème de reconstruction pour le protocole http2

Un problème de reconstruction du protocole HTTP2 peut intervenir dans certains cas.
Ce problème est corrigé en v2.5.5.0.

Chapitre 5

Problèmes connus et limitations

5.1 Sigflow : reconstruction des fichiers avec le protocole FTP

La reconstruction des fichiers n'est pas fonctionnelle avec le protocole FTP.

5.2 Système : politique de mots de passe

La commande *set password-policy previous-check* est inopérante.

5.3 Système : configuration des interfaces

Le passage d'une interface du rôle management-tunnel au rôle management peut entraîner une perte de la connexion.

Chapitre 6

Compatibilité logicielle

6.1 Compatibilité avec le GCenter

Version du GCap	Version du GCenter	Compatibilité
2.5.5.0	2.5.3.102 HF3	Configuration non supportée
2.5.5.0	2.5.3.103 HFx	Configuration ok (recommandé)

Chapitre 7

Comptabilité matérielle

La version 2.5.5.0 est compatible avec toutes les versions matérielles des GCap.

REFERENCE GCAP	STOCKAGE LOCAL	PORTS DE CAPTURE	EXTENSION PORTS DE CAPTURE	ALIMENTATION ELECTRIQUE
GCAP1010HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1020HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1050HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1100HWr2	2 x 600GB RAID1	1 x SFP	N/A	2 x 750W
GCAP1200HWr2	2 x 600GB RAID1	2 x SFP	N/A	2 x 750W
GCAP1400HWr2	2 x 600GB RAID1	4 x SFP	N/A	2 x 750W
GCAP2200HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP2600HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP2800HWr2	4 x 600GB RAID5	4 x SFP	4 x SFP	2 x 750W
GCAP5400HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W
GCAP5600HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W
GCAP5800HWr2	8 x 600GB RAID5	4 x SFP+	4 x SFP+	2 x 1100W

Chapitre 8

Procédure de mise à jour

8.1 Prérequis

Pour déployer la mise à jour du GCap V2.5.5.0 depuis l'interface graphique du GCenter, ce dernier devra être au minimum dans la version **V2.5.3.103-HFX** installée.
Si le GCenter est dans une version inférieure, il faudra préalablement le mettre à jour.

Le GCap devra être dans l'une des versions suivantes **V2.5.4.0**, **V2.5.4.1**, **V2.5.4.2**, **V2.5.4.3**

Pour toute question sur ces éléments, veuillez contacter le support technique de Gatewatcher.

Important :

Il est fortement recommandé d'avoir une connexion de type iDRAC afin de pouvoir se connecter post-mise à jour si un problème survient pendant le processus.
Dans le cas contraire, il faudra avoir un accès physique à l'équipement (écran, clavier).

8.2 Données conservées

Les données et configurations suivantes sont conservées :

- l'appairage avec le GCenter
- la configuration réseau
- la clé SSH du compte root
- le mot de passe du compte root
- les fichiers de logs
- les fichiers pcap présents dans le répertoire /data/cache/pcaps

8.3 Procédure d'installation en passant par le GCenter

Sur le GCenter :

1. Depuis la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.5.0/gcap/), télécharger :
   - le fichier gwp de la nouvelle version disponible
   - le fichier gwp.sha256 du sha256 associé
2. Vérifier l'image (commande sha256sum) et vérifier la valeur obtenue avec le contenu du fichier gwp.sha256
3. Se connecter à la WebUI du GCenter via un navigateur web et aller dans le menu **Administration-Updates / Software Update**.
4. Téléverser le package du GCap.
   - Une barre de progression est affichée.
   - S'il y a un problème, veuillez essayer avec un autre navigateur.

Sur le GCap :

1. Ouvrir un terminal et se connecter en SSH sur le GCap avec le compte **setup**.
2. Arrêter le monitoring-engine avec la commande **monitoring-engine stop** (GCAP-CLI) et attendre que les fichiers soient traités.

Important :

Si le GCap est chargé, il est nécessaire d'attendre avant de lancer la mise à jour.
Vérifier au niveau du GCenter dans le menu **Hunting > Network Metadata** qu'il n'y a plus de traitement.
Pour toutes questions sur ces éléments, veuillez contacter le support technique de Gatewatcher.

3. Exécuter la commande **system upgrade list** (GCAP-CLI) pour lister les packages disponibles sur le GCenter.
4. Exécuter la commande **system upgrade apply '[nom_de_l'image]' confirm** (GCAP-CLI).
   - Le GCap redémarre automatiquement
   - La session SSH est coupée
5. Après que le GCap a redémarré, se connecter en SSH avec le compte **setup** pour voir si la mise à jour a été correctement appliquée.
6. Vérifier la version courante avec la commande **show status** (GCAP-CLI).
7. Redémarrer le monitoring-engine avec la commande **monitoring-engine start** (GCAP-CLI).

En cas de problème, veuillez contacter le support technique de Gatewatcher.

8.4 Procédure d'installation directement depuis le GCap

1. Télécharger la nouvelle version disponible et le sha256 associé depuis la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.5.0/gcap/).
2. Faire la vérification de l'image (commande sha256sum) et vérifier la valeur obtenue avec le contenu du fichier gwp.sha256.
3. Copier l'image (.gwp) dans le répertoire /data/ du GCap avec un compte à privilège.
4. Ouvrir un terminal et se connecter en SSH sur le GCap avec le compte **setup**.
5. Arrêter le monitoring engine avec la commande **monitoring-engine stop** (GCAP-CLI).

Important :

Si le GCap est chargé il est nécessaire d'attendre avant de lancer la mise à jour.
Vérifier au niveau du GCenter dans le menu **Hunting > Network Metadata** qu'il n'y a plus de traitement.
Pour toutes questions sur ces éléments, veuillez contacter le support technique de Gatewatcher.

6. Ouvrir un terminal et se connecter en SSH sur le GCap avec un compte à privilège.
7. Lancer la mise à jour avec la commande **gcap-upgrade /data/nom_du_fichier** (SHELL).
   - Le GCap redémarre automatiquement
   - La session SSH est coupée
8. Après que le GCap a redémarré, se connecter en SSH avec le compte **setup** pour voir si la mise à jour a été correctement appliquée.
9. Vérifier la version courante avec la commande **show status** (GCAP-CLI).
10. Démarrer le monitoring-engine avec la commande **monitoring-engine start** (GCAP-CLI).

En cas de problème, veuillez contacter le support technique de Gatewatcher.

PDF documentation