

Note de version GCAP V2.5.4.2



Version du manuel : v1

Date de création : Novembre 2025

Date de mise à jour : Novembre 2025

© Droits d'auteur : Novembre 2025  GATEWATCHER

La communication ou la reproduction de ce document, l'exploitation ou la communication de son contenu, sont interdites en l'absence de consentement préalable écrit. Toute infraction donne lieu à des dommages et intérêts.
Tous droits réservés, notamment en cas de demande de brevets ou d'autres enregistrements.

Table des matières

| | |
|---|-----------|
| Table des matières | 3 |
| 1 Présentation de la version 2.5.4.2 du GCap | 4 |
| 2 Nouvelles fonctionnalités | 5 |
| 2.1 Moteur de détection Sigflow | 5 |
| 2.1.1 Mise à jour du moteur | 5 |
| 2.1.2 Filtrage des événements pour le protocole SMB | 5 |
| 2.1.3 Support du 100 Mbps pour les interfaces de capture | 5 |
| 2.2 Installation | 5 |
| 2.2.1 Prérequis du stockage | 5 |
| 2.2.2 Support UEFI | 5 |
| 3 Autres caractéristiques et améliorations | 6 |
| 4 Correctifs | 7 |
| 4.1 Erreur pendant le premier redémarrage suite à une mise à jour en v2.5.4.0 | 7 |
| 4.2 Blocage de la mise à jour en v2.5.4.0 | 7 |
| 4.3 Après la mise à jour, erreur dans l'exécution de commandes avec certaines versions de matériel | 7 |
| 4.4 Sigflow : erreur lors du démarrage du moteur de détection | 7 |
| 4.5 Sigflow : les filtres XDP ne s'appliquent pas correctement | 7 |
| 4.6 Sigflow : la réception de paquets spécifiques du protocole Modbus peut provoquer un redémarrage du moteur | 7 |
| 4.7 Netdata : absence de certaines métriques | 8 |
| 4.8 Sigflow : problème de démarrage du moteur de détection | 8 |
| 4.9 Netdata : valeur erronée | 8 |
| 4.10 Système : paramètres de performance inadaptés | 8 |
| 4.11 Système : installation impossible | 8 |
| 4.12 Sigflow : problème avec les interfaces cluster | 8 |
| 4.13 Sigflow : problème d'allocation mémoire pour certains flux | 8 |
| 4.14 Système : saturation de l'espace de stockage du GCap | 8 |
| 4.15 Système : répartition des CPUs | 9 |
| 4.16 Système : sélection par défaut dans le menu de démarrage | 9 |
| 4.17 Sigflow : options permettant le débogage | 9 |
| 4.18 Mise à jour : problème au redémarrage | 9 |
| 5 Problèmes connus et limitations | 10 |
| 5.1 Netdata : badges des statistiques réseaux | 10 |
| 5.2 Sigflow : reconstruction des fichiers avec le protocole FTP | 10 |
| 6 Compatibilité logicielle | 11 |
| 6.1 Compatibilité avec le GCenter | 11 |
| 7 Comptabilité matérielle | 12 |
| 8 Procédure de mise à jour | 13 |
| 8.1 Prérequis | 13 |
| 8.2 Données conservées | 13 |
| 8.3 Données supprimées | 13 |
| 8.4 Procédure d'installation en passant par le GCenter | 13 |
| 8.5 Procédure d'installation directement depuis le GCap | 14 |

Chapitre 1

Présentation de la version 2.5.4.2 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 les correctifs pour les vulnérabilités critiques publiées précédemment.

2.1.2 Filtrage des événements pour le protocole SMB

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

2.1.3 Support du 100 Mbps pour les interfaces de capture

Le 100 Mbps est supporté pour les interfaces de capture utilisées par le moteur de détection.

2.2 Installation

2.2.1 Prérequis du stockage

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

2.2.2 Support UEFI

Le support de l'UEFI a été amélioré.

Chapitre 3

Autres caractéristiques et améliorations

Section laissée vide intentionnellement

Chapitre 4

Correctifs

4.1 Erreur pendant le premier redémarrage suite à une mise à jour en v2.5.4.0

Dans certains cas, suite à la mise à jour en v2.5.4.0, un problème peut intervenir lors du premier redémarrage.

Ce problème est corrigé en v2.5.4.1.

4.2 Blocage de la mise à jour en v2.5.4.0

Si le /boot est plein, la mise à jour du GCap peut se bloquer.

Ce problème est corrigé en v2.5.4.1.

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

Certaines commandes sont non-fonctionnelles pour certaines version de matériel à la suite d'une mise à jour en 2.5.4.0.

Ce problème est corrigé en v2.5.4.1.

4.4 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 activés.

Ce problème est corrigé en v2.5.4.1.

4.5 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 v2.5.4.1.

4.6 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 v2.5.4.1.

4.7 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 v2.5.4.1.

4.8 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 v2.5.4.2.

4.9 Netdata : valeur erronée

Dans certains cas, Netdata renvoie une valeur erronée pour le statut du moteur de détection.

Ce problème est corrigé en v2.5.4.2.

4.10 Système : paramètres de performance inadaptés

Certains paramètres du système ne sont pas optimisés pour les performances.

Ce problème est corrigé en v2.5.4.2.

4.11 Système : installation impossible

Dans certains cas, l'installation du GCap n'est pas possible.

Ce problème est corrigé en v2.5.4.2.

4.12 Sigflow : problème avec les interfaces cluster

Lors de l'utilisation d'interface cluster, un drop important de paquets pourrait avoir lieu.

Ce problème est corrigé en v2.5.4.2.

4.13 Sigflow : problème d'allocation mémoire pour certains flux

L'allocation mémoire pour certains flux n'est pas optimisée.

Ce problème est corrigé en v2.5.4.2.

4.14 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 v2.5.4.2.

4.15 Système : répartition des CPUs

Pour certains modèles de GCap la répartition des CPUs n'est pas optimale.
Ce problème est corrigé en v2.5.4.2.

4.16 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 v2.5.4.2.

4.17 Sigflow : options permettant le débogage

Certaines options permettant le débogage du système sont activées par défaut.
Ce problème est corrigé en v2.5.4.2.

4.18 Mise à jour : problème au redémarrage

Un problème peut intervenir au redémarrage du système après une mise à jour.
Ce problème est corrigé en v2.5.4.2.

Chapitre 5

Problèmes connus et limitations

5.1 Netdata : badges des statistiques réseaux

En mode de compatibilité **2.5.3.102**, les statistiques Netdata présentes au niveau du menu **Admin > GCaps Pairing/Status** ne sont plus disponibles.

5.2 Sigflow : reconstruction des fichiers avec le protocole FTP

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

Chapitre 6

Compatibilité logicielle

6.1 Compatibilité avec le GCenter

| Version du GCap | Version du GCenter | Compatibilité |
|-----------------|--------------------|--------------------------------|
| 2.5.4.2 | 2.5.3.102 HF3 | Configuration ok |
| 2.5.4.2 | 2.5.3.103 HFx | Configuration ok (recommandée) |

Chapitre 7

Comptabilité matérielle

La version 2.5.4.2 est compatible avec toutes les versions matérielles des GCap.

| REFERENCE GCAP | STOCKAGE LOCAL | PORTE DE CAPTURE | EXTENSION DE CAPTURE | PORTS | ALIMENTATION | ELEC-TRIQUE |
|----------------|-----------------|------------------|----------------------|-------|--------------|-------------|
| 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 V2.5.4.2 depuis l'interface graphique du GCenter, ce dernier devra être au minimum dans la version **V2.5.3.102-HF3** 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 **V2.5.3.106**, **V2.5.3.107**, **V2.5.3.109**, **V2.5.4.0**, **V2.5.4.1**.

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 :

- le pairing 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/pcaps/ ou /data/cache/pcaps

8.3 Données supprimées

Important :

Les données suivantes vont être supprimées si le GCAP est en version V2.5.3.X :

- Les règles locales de Sigflow (local-rules)
- Les filtres XDP locaux

Veuillez reporter au préalable la configuration de ces filtres au niveau du GCenter à l'aide du menu **GCap Profiles > Packet filters**

8.4 Procédure d'installation en passant par le GCenter

Sur le GCenter :

1. Depuis la plate-forme <https://update.gatewatcher.com/upgrade/> (répertoire 2.5.4.2/gcap/), télécharger :
 - le fichier gwp de la nouvelle version disponible

- le fichier gwp.sha256 du sha256 associé

Important :

Deux versions de GCenter sont disponibles :

- Si le GCenter est en V2.5.3.102 et le GCap en V2.5.3.X, utiliser le package suivant : https://update.gatewatcher.com/upgrade/2.5.4.2/gcap/gcap-bios_2.5.4.2-gcenter_v2.5.3.102.gwp
- Si le GCenter est en V2.5.3.102 et le GCap en version 2.5.4.0, il faut, au préalable, mettre à jour le GCenter en V2.5.3.103
- Si le GCenter est en V2.5.3.103, utiliser le package suivant : https://update.gatewatcher.com/upgrade/2.5.4.2/gcap/gcap-bios_2.5.4.2.gwp pour la version BIOS ou https://update.gatewatcher.com/upgrade/2.5.4.2/gcap/gcap-uefi_2.5.4.2.gwp pour la version UEFI (nouveau matériel de génération 16)

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 deux fois, 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.

8.5 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 2.5.4.2/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).
8. Redémarrer le GCap avec la commande **system restart** (GCAP-CLI).

La session SSH est coupée.
9. Après que le GCap a redémarré deux fois, se connecter en SSH avec le compte **setup** pour voir si la mise à jour a été correctement appliquée.
10. Vérifier la version courante avec la commande **show status** (GCAP-CLI).
11. Démarrer le monitoring-engine avec la commande **monitoring-engine start** (GCAP-CLI).

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