Note de version
GCap Version 2.5.4.0

Version: V3

Date de création: Décembre, 2024

Contents

Chapter 1

Présentation de la version 2.5.4.0 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

Chapter 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 Ajout des évènements de type « flow »

La génération d'évènements de type « flow » est maintenant disponible au niveau du moteur Sigflow.

2.1.3 Configuration du multitenant

La configuration du multitenant a été améliorée pour offrir la possibilité de configurer des variables réseaux (port et network variables) spécifiques à chaque tenant.

2.1.4 Ajout de l'empreinte réseau HASSH

Un nouveau champ « hassh » est disponible pour les évènements SSH, afin d'enregistrer les empreintes des clients et serveurs SSH, lorsqu'une transaction utilisant ce protocole est analysé par le moteur Sigflow.

2.1.5 Enregistrement des champs d'un certificat

Il est désormais possible de choisir les champs que l'on souhaite enregistrer lors de l'analyse d'une transaction TLS (phase de négociation).

2.1.6 Ajout d'un nouveau keyword pour les règles de détection

Le keyword `dns.query.name` a été ajouté au moteur Sigflow et peut être utilisé dans les règles de détection relatives au protocole DNS.
C'est un keyword de type sticky buffer qui est utilisé pour regarder le nom dans les requêtes et réponses DNS.

2.1.7 Fichiers pcap de test

Deux nouveaux fichiers pcap ont été ajoutés pour tester les moteurs ransomware-detect et beacon-detect (GCenter v2.3.5.103).

2.2 Virtualisation de la sonde

2.2.1 Support VMware

Le GCap est officiellement supporté sur les hyperviseur ESXi de VMware.

2.2.2 Support AWS

Le GCap est officiellement supporté sur les infrastructures Cloud d'AWS.

2.3 Configuration du réseau de la sonde

2.3.1 Présentation

- Les interfaces sont maintenant identifiées par leur nom système comme dans l'exemple ci-dessous avec l'exécution de la commande `show interfaces`

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
mon0	enp4s0	capture	Available	1500	00:50:56:91:8d:35	1Gb	RJ45	0x8086	0x10d3	04:00.0
tunnel	enp11s0	tunnel	Available	1500	00:50:56:00:03:01	10Gb	RJ45	0x15ad	0x07b0	0b:00.0
mon1	enp12s0	capture	Available	1500	00:50:56:91:d4:30	1Gb	RJ45	0x8086	0x10d3	0c:00.0
management	enp19s0	management	Available	1500	00:50:56:00:03:02	10Gb	RJ45	0x15ad	0x07b0	13:00.0
mon2	enp20s0	capture	Available	1500	00:50:56:91:c3:e3	1Gb	RJ45	0x8086	0x10d3	14:00.0
	enp27s0	inactive	Available	1500	00:50:56:00:03:03	1Gb	RJ45	0x8086	0x10d3	1b:00.0
monvirt	monvirt	capture	Available	1500	N/A	N/A	N/A	N/A	N/A	N/A

- Les interfaces gcpX ont été retirées.

-
- Les **concepts de rôle et de label** ont été introduits dans cette version.
  - Voici la liste des différents rôles :
    - **capture** pour définir une interface de capture du flux
    - **tunnel** pour définir l'interface qui sert au tunnel IPSec entre le GCap et le GCenter
    - **management** pour définir l'interface qui permet d'administrer le GCap (via SSH)
    - **management-tunnel** pour définir l'interface qui porte les deux précédents rôles (management et tunnel)
    - **capture-cluster** pour définir les interfaces de capture du flux en mode cluster
    - **inactive** pour désactiver une interface
  - Voici la liste des labels :
    - **Management**
    - **Tunnel**
    - **MonX**

2.3.2 Commande associée

Pour assigner un rôle spécifique à une interface, la commande suivante doit être exécutée :

```
`set interfaces assign-role {management|tunnel|management-tunnel|capture|capture-cluster|inactive}
```

2.4 Processus de mise à jour

Une fonctionnalité de retour arrière a été implémentée en cas de problèmes durant le processus de mise à jour du système.
Il sera possible de revenir sur la version précédente lors de l'affichage du menu de démarrage du GCap.

2.5 Support matériel

2.5.1 Support des serveurs DELL

Cette version est compatible avec la 16 ème génération de serveurs DELL.

2.5.2 Support de l'UEFI

Cette version introduit le support de l'UEFI.

Chapter 3

Autres caractéristiques et améliorations

3.1 Performances

Les performances de la sonde GCap ont été optimisées avec une allocation dynamique des ressources au premier démarrage et une meilleure répartition des flux lors de la capture.

3.2 Processus d'association de la sonde

La commande `unpair` est maintenant disponible pour supprimer la configuration du pairing présente sur la sonde.

3.3 Suppression des données métier

La commande `system delete-data` est maintenant disponible pour supprimer les données métiers présentes sur la sonde.

3.4 Commande `show status`

Des informations supplémentaires sont disponibles dans le résultat de la commande `system delete-data` :

```
Gcap FQDN          : gcap.gatewatcher.com
Version            : 2.5.4.0
Overall status     : Running
Tunnel             : Up
Detection Engine   : Up and running
Configuration      : Complete

Gcap name              : gcap
```

(suite sur la page suivante)

(suite de la page précédente)

```
Domain name           : gatewatcher.com
Tunnel interface      : 192.168.2.2
Management interface  : 192.168.1.2
Gcenter version       : 2.5.3.103
Gcenter IP            : 192.168.2.3
Paired on Gcenter     : Yes
Monitoring interfaces : mon0,mon2,mon4,monvirt

  © Copyright GATEWATCHER ...
```

3.5 Mises à jour du système

Le système d'exploitation de la sonde GCap ainsi que le noyau ont été mis à jour.

3.6 Mode de compatibilité

Un nouveau mode de compatibilité est disponible pour le support de la version v2.5.3.103 du GCenter.

3.7 Connexion IPSec

La configuration du service IPSec a été optimisée pour améliorer la robustesse de la connexion entre le GCap et le GCenter.

3.8 Visualisation de la configuration en mode CLI

L'ensemble des commandes show sont disponibles lorsque le moteur de détection est démarré.

3.9 Fonctionnalités et commandes dépréciées

3.9.1 Haute-disponibilité

La fonctionnalité de haute disponibilité a été retirée de cette version.
Pour mettre en place une architecture redondante, contacter le support technique Gatewatcher.

3.9.2 Sigflow: Règles locales

Les règles locales ne sont plus supportées dans cette version.

3.9.3 Génération du fichier techsupport

La génération du fichier techsupport se réalise exclusivement avec une session SSH en mode non-interatif:

- Depuis un poste Linux

  `ssh -t setup@GCapX show tech-support large > /tmp/tech-supp-GCapX`

- Depuis un poste Windows

  `ssh -t setup@GCapX "show tech-support large" > C:\Temp\tech-supp-GCap`

3.9.4 Commandes retirées

Les commandes suivantes ont été retirées :

- La commande `set advanced-configuration packet-filter` permettant de configurer des filtres XDP en local
  La configuration des filtres XDP s'effectue exclusivement sur le GCenter.
- La commande `show advanced-configuration cpu-config` permettant de visualiser la configuration des CPU
- La commande `show/set advanced-configuration interfaces-names` permettant de visualiser ou de configurer le nom des interfaces
- La commande `show/set advanced-configuration load-balancing`` permettant de visualiser ou de configurer l'équilibrage de charge pour les interfaces de capture
- La commande `show/set advanced-configuration local-rules` permettant de visualiser ou de configurer des règles locales
- La commande `show advanced-configuration memory-settings` permettant de visualiser la configuration de la mémoire du moteur de détection
- La commande `system reload-drivers` permettant de recharger les pilotes des cartes réseaux
- La commande `show/set clusters` permettant de visualiser ou de configurer les interfaces clusters
  Les interfaces cluster se configure via la commande `set interfaces [interface-name] assign-role capture-cluster`
- La commande `gui` permettant d'accéder au menu de configuration graphique
- La commande `show/set setup-mode` permettant de visualiser ou de configurer le mode par défaut de l'interface de configuration
- La commande `show configuration` permettant la visualisation de la configuration de Sigflow
- La commande `show logs` permettant la visualisation des logs

Les commandes relatives à la gestion des services ont été retirées :

- `services start/stop/show {eve-generation|eve-upload|file-extraction|file-upload|filter-filein

---

Chapter 4

Correctifs

4.1 IPSec : La commande `pairing reload-tunnel` ne redémarre pas complètement le service

Dans certains cas, la commande `pairing reload-tunnel` ne permet pas de rendre fonctionnel le tunnel IPSec entre le GCap et le GCenter.
Ce problème est corrigé en V2.5.4.0.

4.2 Netdata: Approximation dans les métriques Sigflow

Certaines métriques Sigflow sont approximatives.
Ce problème est corrigé en V2.5.4.0.

4.3 Sigflow: Certains paquets sont comptés deux fois

Dans certains cas, les paquets sont comptés deux fois dans les statistiques de la carte réseau remontées par le moteur Sigflow.
Ce problème est corrigé en V2.5.4.0.

Chapter 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.

5.3 Mise à jour: problème durant l'opération

Durant la mise à jour en 2.5.4.0, si le GCap est chargé, la mise à jour pourrait échouée.

Contournement

Après avoir stoppé le moteur de détection, attendre avant de lancer la mise à jour.
Vérifier au niveau du GCenter dans le menu **Hunting** > **Metadata** qu'il n'y a plus de traitement.
Si vous êtes des questions sur ces éléments, veuillez contacter le support technique de Gatewatcher.

Chapter 6

Compatibilité logicielle

6.1 Compatibilité avec le GCenter

Version du GCap	Version du GCenter	Compatibilité
2.5.4.0	2.5.3.101 HF4	Configuration non-supportée. GCenter à mettre à jour à une version plus récente
2.5.4.0	2.5.3.102 HF3	Configuration ok

Chapter 7

Comptabilité matérielle

La version 2.5.4.0 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

Chapter 8

Procédure de mise à jour

8.1 Prérequis

Pour déployer la mise à jour du GCap V2.5.4.0 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 en version **V2.5.3.106** ou **V2.5.3.107**

Si vous êtes des questions 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/

8.3 Données supprimées

Important:

Les données suivantes vont être supprimées:

- 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 2.5.4.0/gcap/), télécharger :
   - le fichier gwp de la nouvelle version disponible
   - le fichier gwp.sha256 du sha256 associé
2. Faire la vérification de 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 **Admin** > **Gum** > **Software Update**.
4. Dans la section **Upload a software update**, cliquer sur **Parcourir** puis sélectionner le fichier .gwp (image précédemment téléchargée) pour la mettre à disposition sur le GCenter.
5. Valider en cliquant sur le bouton **Choisir**.
6. Valider le téléchargement en cliquant sur le bouton **Submit**.
   - Une barre de progression est affichée.
   - Si vous rencontrez un problème lors de la mise à disposition de l'image, 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** > **Metadata** qu'il n'y a plus de traitement.

   Si vous êtes des questions sur ces éléments, veuillez contacter le support technique de Gatewatcher.

3. Executer la commande **system upgrade list** pour lister les packages disponibles sur le GCenter
4. Executer la commande **system upgrade apply [nom_de_l'image] confirm**
   - Le GCap doit redémarrer automatiquement.
   - La session SSH est coupée
5. Une fois 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 sur la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.4.0/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 /tmp/ 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** > **Metadata** qu'il n'y a plus de traitement.
Si vous êtes des 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 /tmp/nom_du_fichier** (SHELL).
8. Redémarrer le GCap avec la commande **system restart** (GCAP-CLI).
   La session SSH est coupée.
9. Une fois 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.

PDF Note de version