Note de Version
GCap Version 2.5.3.105

Version de la note : V2

Date de création : Septembre, 2022

Date de mise à jour : Septembre, 2022

Contents

Chapter 1

Présentation de la version 2.5.3.105 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 Haute disponibilité

Afin d'augmenter la disponibilité opérationnelle de la solution, Gatewatcher a implémenté un mécanisme de haute disponibilité.

Il permet de ne pas perdre les flux capturés, par exemple, en cas de panne ou d'arrêt d'un GCap, grâce à la mise en place de deux GCap en redondance.

Ces deux GCap capturent le même flux et communiquent avec un unique GCenter.

En cas de problème sur le GCap « leader », le GCap « follower » prend le relais pour assurer une continuité du service pendant l'opération de maintenance.

Les commandes suivantes ont été ajoutées :

- `` `show advanced-configuration high-availability` `` pour visualiser l'état de la redondance (HA),
- `` `set advanced-configuration high-availability` `` pour configurer la redondance (HA).

Pour plus d'informations sur le fonctionnement de ce mécanisme, veuiller se référer à la documentation.

2.2 Authentification par clé SSH

Afin d'augmenter la sécurité d'accès au GCap, l'authentification par clé SSH a été mis en place.

Cette fonctionnalité permet de définir une clé pour un utilisateur donné en garantissant une traçabilité des connexions et une imputabilité des actions.

Le GCap supporte les clés de type RSA, ECDSA et ED25519.

Ce mode est à privilégier au couple login/mot de passe.

L'ajout d'une clé SSH pour un compte est défini via la commande `` `set ssh-keys` ``.

Note:

```
La politique de gestion des mots de passe n'est pas utilisée dans le cas de␣
↪clés SSH.
```

2.3 Statistiques et des informations de santé

2.3.1 Affichage des statistiques et des informations de santé

Afin d'améliorer la supervision du GCap, des nouveaux compteurs sur les statistiques et des informations de santé ont été mis en place, avec les catégories suivantes :

- les compteurs et statistiques liés au matériel (stockages de masse / processeurs / mémoire vive / l'espace d'échange),
- les compteurs liés aux fonctionnalités (emergency mode / GCenter appairé / haute disponibilité (HA)/ disponibilité / initialisation du système),
- les compteurs du moteur de détection Sigflow et de sa charge (Informations sur le moteur / interfaces réseaux / paquets reçus en fonction des cœurs de processeurs / nœud NUMA / charge moyenne du GCap).

Ces compteurs et statistiques sont consultables via la commande `` `show health` ``.

2.3.2 Nouvelles statistiques et informations de santé via Netdata

De nouvelles statistiques et informations de santé sont disponibles via Netdata.

2.4 Améliorations relatives au moteur de détection Sigflow

2.4.1 Nouvelle version du moteur

Le moteur Sigflow a été mis à jour pour prendre en compte de nouvelles fonctionnalités, nouveaux protocoles...

2.4.2 Nouveaux protocoles supportés pour l'analyse

Le tableau ci-après indique les **nouveaux** protocoles supportés.

La détection des prococoles comprends 2 parties :

- le **parsing** :
- il permet d'activer la détection des signatures SIGFLOW pour un protocole donné.
- si le parsing est activé pour un protocole alors le flux identifié par une signature lève une alerte.
- si le parsing est désactivé pour un protocole alors aucune alerte n'est levée.
- le **logging** :
- il permet d'activer la génération de métadonnées pour un protocole donné vers le Gcenter.
- si le logging est activé pour un protocole alors le flux observée génére des métadonnées.
- si le logging est désactivé pour un protocole alors aucune métadonnée n'est générée.

Protocole	Type	Versions du GCAP	
		V2.5.3.104	V2.5.3.105
DCERPC	parsing	supporté	supporté
	logging	non supporté	supporté
ENIP	parsing	non supporté	supporté détection uniquement
	logging	non supporté	non supporté
FTP	parsing	supporté	supporté
	logging	non supporté	supporté
HTTP2	parsing	non supporté	supporté
	logging	non supporté	supporté
IMAP	parsing	non supporté	supporté détection uniquement
	logging	non supporté	non supporté
MQTT	parsing	non supporté	supporté
	logging	non supporté	supporté
RDP	parsing	non supporté	supporté
	logging	non supporté	supporté
RFB	parsing	non supporté	supporté
	logging	non supporté	supporté
SIP	parsing	non supporté	supporté
	logging	non supporté	supporté
SNMP	parsing	non supporté	supporté
	logging	non supporté	supporté

2.4.3 Nouveaux protocoles supportés pour la reconstruction de fichiers

Le tableau ci-après indique les **nouveaux** protocoles supportés.

	Versions du GCAP	
Protocole	V2.5.3.104	V2.5.3.105
FTP	supporté via règles définies sur GCAP uniquement	supporté
HTTP2	non supporté	supporté
NFS	non supporté	supporté
SMB	supporté via règles définies sur GCAP uniquement	supporté

2.4.4 Ajout des adresses MAC observées sur le réseau

A partir de la V2.5.3.105, les adresses MAC observées sur le réseau sont enregistrées pour le bon fonctionnement du Network Detection & Response (NDR).

2.4.5 Optimisation de l'analyse des flux chiffrés TLS

Jusqu'à la V2.5.3.104, l'ensemble d'un flux TLS est analysé par le moteur de détection (partie en clair et partie chiffrée).

A partir de la V2.5.3.105 :

- la partie en clair des flux TLS est analysée,
- la partie chiffrée des flux TLS n'est plus analysée grâce à l'ajout d'une règle de bypass dynamique (filtre XDP).

2.4.6 Changement dynamique des assignations des CPU

Jusqu'à la V2.5.3.104, l'assignation des CPU au moteur de détection pouvait provoquer des instabilités et nécessitait donc un redémarrage du GCap après modification.

A partir de la V2.5.3.105, il n'est plus nécessaire d'effectuer ce redémarrage après une nouvelle assignation.

2.4.7 Configuration MTU pour les interfaces *monvirt*, *gcp0* et *gcp1*

A partir de la V2.5.3.105, il est possible de configurer la MTU de l'interface virtuelle *monvirt* et des interfaces physiques *gcp0* et *gcp1* via la commande `set advanced-configuration mtu`.

2.4.8 Activation de l'empreinte des connexions TLS

A partir de la V2.5.3.105, une nouvelle option permettant l'activation de JA3 est disponible.

JA3 va permettre de récupérer des informations échangées lors de la négociation TLS afin de détecter des connexions malveillantes.

Cette option est uniquement disponible en mode de compatibilité v102.

2.4.9 Ajout du community-id pour le hash des flux

L'ajout du community-id, hash basé sur un algorithme 7 tuple, va faciliter l'analyse d'un flux entre plusieurs moteurs de détection.

2.4.10 Ajout du classetype « activehunt »

L'ajout du classetype « activehunt » dans le fichier de classification du moteur de détection a été réalisée afin de prendre en compte la catégorie relative aux règles générées à partir de la CTI LIS.

2.4.11 Période de grâce accordée au démarrage des interfaces de capture

A partir de la V2.5.3.105, la période de grâce accordée au démarrage des interfaces de capture est configurable.

Les commandes suivantes ont été ajoutées :

- `` `show interfaces delay` `` pour visualiser la valeur courante,
- `` `set interfaces delay` `` pour configurer cette valeur.

2.4.12 Assignation manuelle de toutes les interfaces du GCap

Jusqu'à la V2.5.3.104, il est possible de :

- visualiser les interfaces avec la commande `` `show monitoring-interfaces` ``,
- détecter automatiquement les interfaces avec la commande `` `set advanced-configuration rescan-interfaces` ``.

A partir de la V2.5.3.105, la commande suivante vient compléter les actions possibles au niveau de la détection et l'assignation des interfaces :`` `set advanced-configuration interface-names` ``.

Elle permet d'effectuer :

- **l'assignation des interfaces physiques du GCap :**
  - les interfaces de management (*gcp0* et *gcp1*)
  - les interfaces de capture et de détection *mon0* à *monx* ou virtuelle *monvirt*.
- la réinitialisation de l'assignation courante et revenir à une assignation automatique. Cette assignation se fait grâce à la commande `` `set advanced-configuration interface-names reset` ``

2.4.13 Option période de grâce du moteur de détection

Jusqu'à la V2.5.3.104, le délai accordé au démarrage du moteur de détection n'est configurable qu'avec les droits root.

Il est lié aux temps de chargement des règles par le moteur de détection.

A partir de la V2.5.3.105, ce délai (période de grâce) est modifiable.

Les commandes suivantes ont été ajoutées :

- `` `show monitoring-engine start-timeout` `` pour visualiser la valeur courante,
- `` `set monitoring-engine start-timeout` `` pour configurer cette valeur.

2.4.14 Option sanity-checks du moteur de détection

A partir de la V2.5.3.105, le contrôle des prérequis nécessaires au démarrage du moteur de détection peut être activé ou désactivé.

Ce contrôle consiste à vérifier que les interfaces de capture *monx* qui sont activées sont correctement connectées afin d'autoriser le démarrage du moteur.

Les commandes suivantes ont été ajoutées :

- `` `show monitoring-engine sanity-checks` `` pour visualiser l'état courant,

- `set monitoring-engine {disable-sanity-checks|enable-sanity-checks}` pour activer ou désactiver le contrôle.

2.5 Option vpn-link speed pour le tunnel VPN

A partir de la V2.5.3.105, il sera possible de spécifier la qualité du lien entre le GCap et le GCenter afin de s'adapter aux liens à faible débit.

Les commandes suivantes ont été ajoutées :

- `show network-config vpn-link speed` pour visualiser l'état courant,
- `set network-config vpn-link speed {fast|slow}` pour activer ou désactiver le contrôle.

2.6 Ajout d'un mécanisme de redémarrage automatique des services crashés

Jusqu'à la V2.5.3.104, certains services n'étaient pas redémarrés lors qu'ils étaient inopérants.

A partir de la V2.5.3.105, il a été ajouté un mécanisme de redémarrage automatique des services crashés.

2.7 Ajout de la possibilité de passer une commande de la CLI avec la connexion SSH

A partir de la V2.5.3.105, afin de facilité l'automatisation des interactions avec le GCap, il est dorénavant possible en une seule commande :

- de se connecter à distance en SSH,
- d'exécuter une commande,
- d'afficher le résultat de la commande,
- de fermer la connexion à distante.

Chapter 3

Autres caractéristiques et améliorations

3.1 Changement du système d'exploitation

Un refonte complète du système d'exploitation du GCap a eu lieu en V2.5.3.105.

3.2 Changement du langage de développement

Le langage principal de développement a évolué en V2.5.3.105.

3.3 Mise à jour du noyau

Le noyau du système d'exploitation a été mis à jour avec la dernière version LTS (Long-Term Support).

3.4 Amélioration des performances

3.4.1 Amélioration des performances de Codebreaker

A partir de la V2.5.3.105, afin d'améliorer les performances de Codebreaker, un nouveau langage de programmation a été utilisé et le code a été optimisé.

3.4.2 Optimisation de la communication réseau entre le GCap et le GCenter

Jusqu'à la V2.5.3.104, il y a un échange systématique des fichiers entre le GCap et le GCenter.

A partir de la V2.5.3.105 :

- seuls les fichiers mis à jour sont compressés et téléchargés en plusieurs sessions parallélisées et non plus fichier par fichier,
- pour gérer l'envoi des eve-logs entre GCap et GCenter, un nouveau mécanisme d'échange a été mis en place,
- pour télécharger les configurations et fichiers entre le GCenter et le GCap :
  - pour le GCenter en V2.5.3.104, utilisation de rsync,
  - pour le GCenter en V2.5.3.105, mise en place d'un nouveau mécanisme d'échange uniquement compatible avec la version 102 du GCenter (pour les GCenters en version 101 rsync restera la méthode utilisée).

3.4.3 Amélioration de la gestion de la charge des interfaces de capture *monx*

Jusqu'à la V2.5.3.104, l'équilibrage de la charge venant des interfaces de capture *monx* vers les CPU du GCap a été mis en place de façon expérimentale.

A partir de la V2.5.3.105, cette fonctionnalité est arrivée à maturité mais la fonctionnalité est compatible uniquement avec certains modèles de GCap.

Pour plus d'informations sur cette amélioration, veuiller contacter le support technique Gatewatcher.

3.5 Améliorations globales de sécurité

3.5.1 Sécurité réseau

3.5.1.1 Isolation plus stricte du service SSH à l'aide de VRF

A partir de la V2.5.3.105, afin de durcir le service SSH, des VRF sont utilisées pour un meilleur cloisonnement.

3.5.1.2 Refonte des règles internes du pare-feu

A partir de la V2.5.3.105, iptables a été remplacé par nftables pour le filtrage des flux internes du GCap et les règles gérées dynamiquement ont été abondonnées au profit de règles statiques prédéfinies en fonction de l'état du GCap.

3.5.1.3 Refonte de la gestion IPsec entre le GCap et le GCenter

A partir de la V2.5.3.105, des modifications en profondeur du service IPSec ont été opérées afin d'améliorer la stabilité et la sécurité des échanges entre le GCap et le GCenter.

3.5.2 Sécurité système

3.5.2.1 Amélioration de la qualité des clés cryptographiques

A partir de la V2.5.3.105, un mécanisme d'injection d'entropie a été mis en place pour améliorer la qualité des clés cryptographiques générées notamment lors du premier démarrage.

3.5.2.2 Durcissement de la configuration du service SSH

En V2.5.3.105, le service SSH a été durci pour suivre les recommandations de l'ANSSI.

3.5.2.3 Amélioration de l'isolation des processus

A partir de la V2.5.3.105, une meilleure isolation des processus est présente grâce à Systemd (limitation des espaces mémoire alloués aux processus, accès en lecture seule...).

3.5.2.4 Politique PAM et gestion des verrouillages de comptes

A partir de la V2.5.3.105, une refonte complète de la politique PAM et de la gestion des verrouillages de comptes a été opérée.

3.5.2.5 Protection des partitions disques en lecture seule

A partir de la V2.5.3.105, les partitions contenant le code du GCap sont montées en lecture seule dès le démarrage du serveur et non lors du démarrage du moteur de détection.

3.5.2.6 Modification de la stratégie du mot de passe root

A partir de la V2.5.3.105, le mot de passe root est généré aléatoirement et n'est plus disponible pour les utilisateurs de la solution.

Pour plus d'information sur ce sujet, veuiller contacter le support technique GATEWATCHER.

3.5.2.7 Sanctuarisation de la gestion de configuration et des droits associés

A partir de la V2.5.3.105, un système central de gestion des droits et des contrôles d'accès a été mis en place ainsi les demandes de modifications de configuration sont soumises à ce système.

3.5.2.8 Réduction des risques sur les droits SUID

A partir de la V2.5.3.105, tous les programmes ayant la propriété SUID et qui ne sont pas utilisés sont soit supprimés soit désactivés.

3.5.2.9 Amélioration du démon en charge des filtres XDP

A partir de la V2.5.3.105, les améliorations suivantes ont été appliquées au démon en charge des filtres XDP :

- réduction de la surface d'attaque (plus de compilation dynamique du code, durcissement du démon..),
- augmentation de ses performances.

3.5.2.10 Amélioration de la sécurité de Netdata

A partir de la V2.5.3.105, les modules natifs de prises de mesures de Netdata sont remplacés par un démon sécurisé, développé par Gatewatcher.

3.5.2.11 Création d'une Image initrd spécifique

A partir de la V2.5.3.105, une image initrd sécurisée, générée par Gatewatcher est dorénavant utilisée.

3.5.2.12 Remplacement du système d'initialisation

A partir de la V2.5.3.105, le système d'initialisation OpenRC est remplacé par systemd.

3.6 Modification sur la CLI

3.6.1 Modification du champ d'action des commandes liées aux interfaces

Jusqu'à la V2.5.3.104, les commandes permettant d'interagir avec les interfaces de détection sont :

- `show monitoring-interfaces`,
- `set monitoring interfaces`.

A partir de la V2.5.3.105, les interfaces de management et les interfaces de détection sont gérées par les mêmes commandes :

- `show interfaces`,
- `set interfaces`.

3.6.2 Sélection des protocoles qui sont analysés par le moteur de détection

Jusqu'à la V2.5.3.104, la sélection des protocoles qui sont analysés par le moteur de détection se fait par la GUI ou la commande `Protocols-selector`.

A partir de la V2.5.3.105, cette fonction est effectuée via les règles du moteur de détection et donc gérée par le GCenter.

La commande `Protocols-selector` a donc été retirée de la CLI.

3.6.3 La GUI de configuration est marquée obsolète

A partir de la V2.5.3.105, la GUI est considérée comme dépréciée (ou obsolète).

Les nouvelles fonctionnalités ne seront donc pleinement utilisables qu'au travers de la CLI.

3.7 Fonctionnalités pour extraction des données de diagnostic à destination du support technique de Gatewatcher

Afin de pouvoir collecter facilement les données nécessaires au diagnostic par le support technique de Gatewatcher, une extraction automatisée des données de fonctionnement du GCap a été développée.

Cette extraction est effectuée grâce à la commande `tech-support` du sous-groupe `show`.

3.8 Modification de la stratégie de rechargement des pilotes

Jusqu'à la V2.5.3.104, c'est un redémarrage qui est effectué (arrêt des pilotes puis redémarrage services + chargement des fichiers) : commande `` `system restart-drivers` ``.

A partir de la V2.5.3.105, c'est un rechargement des fichiers de configuration qui est effectué) : `` `commande system reload-drivers` ``.

3.9 Modification de la stratégie de la gestion des situations de crises (emergency mode)

A partir de la V2.5.3.105, une gestion des espaces disques a été ajoutée avec la mise en place de quota pour éviter la saturation de ces espaces qui renderaient le GCap inopérant.

Lorsque ces quotas sont dépassés l'emergency mode est déclenché et va modifier dynamiquement la durée de rétention des données du GCap pour la passer à 2 min.

Ainsi tous les fichiers plus vieux que cette durée de rétention sont supprimés, en commençant par les plus anciens jusqu'à la sortie de l'emergency mode.

Pour plus d'informations sur cette fonctionnalité, veuiller consulter la documentation.

Chapter 4

Correctifs

4.1 Eve-log tronqués automatiquement si taille > 65536 octets

Jusqu'à la V2.5.3.104, le moteur de détection tronque automatiquement les eve-logs dont la taille est supérieure à 65536 octets et le fait de façon brutale ce qui corrompt l'eve-log suivant.

A partir de la V2.5.3.105, cette troncature est faite de façon correcte. Conséquence, l'eve-log tronqué n'est pas traitable mais ne corromps plus l'eve-log suivant.

4.2 Transactions TCP et fichiers extraits (« unknown »)

Les sessions TCP qui fonctionnent de la manière suivante empêchent le GCap de remonter un fichier reconstruit correctement au GCenter :

- Initial 3-way handshake,
- Envoi du fichier dans son intégralité avec le drapeau PUSH sans ACK intermédiaire,
- ACK de l'ensemble des segments et fermeture de la connexion par RST.

Ce rapport erroné perturbe le fonctionnement du GCap qui n'envoie pas correctement le fichier au GCenter.

Un correctif partiel était présent dans les versions supérieures ou égales à V2.5.3.104 (fichier « unknown »).

Ce problème est complètement corrigé en V2.5.3.105.

4.3 Utilisation de protocole RELP et ajout d'une file d'attente entre GCap et GCenter

Lors d'un problème de communication entre le GCap et le GCenter, l'envoi des journaux système pouvait être perturbé (perte d'informations).

L'utilisation du protocole RELP et ajout d'une file d'attente pour l'envoi de ces journaux permet de pallier ce problème en V2.5.3.105.

4.4 Protection du mécanisme d'authentification (anti-bruteforce)

Le compteur de tentatives d'authentification est incrémenté dès qu'une tentative d'ouverture de session a lieu, même si aucun mot de passe n'est entré par l'utilisateur.

Ce problème est complètement corrigé en V2.5.3.105.

4.5 Problème de parsing du protocole HTTP

Certaines requêtes HTTP analysées par le moteur Sigflow ne sont pas correctement parsées ce qui entraîne une perte d'informations dans les données remontées au GCenter par le GCap.

La mise à jour du parseur corrige ce problème dans en V2.5.3.105.

4.6 Problème lors du rejeu de certains fichiers pcap

Dans certains cas le rejeu de fichiers pcap au travers de l'interface *monvirt* ne s'effectue pas correctement à cause d'un problème de MTU.

La possibilité de configurer la MTU de l'interface *monvirt* en V2.5.3.105 corrige ce problème.

4.7 Problème lors du rejeu de fichiers pcap avec le multi-tenancy activé

La fonction « replay pcap » n'est pas opérationnelle lorsque le multi-tenancy par interface est activé.

Ce problème est corrigé en V2.5.3.105.

4.8 Affichage de l'état du GCap en « undetermined » dans l'interface de gestion du GCenter

L'affichage erroné de l'état du GCap dans l'interface du GCenter peut être causée par différents problèmes.

L'une des causes est le crash d'un service (gcap-heartbeat) qui n'est pas redémarré.

Le changement dans la gestion des services du GCap avec la mise en place d'un redémarrage automatique des services corrige ce problème en V2.5.3.105.

4.9 Affichage erroné de l'état des interfaces de monitoring

Dans certains cas, l'état des interfaces de monitoring ne s'affiche pas correctement dans l'utilitaire de configuration. Ce problème est corrigé en V2.5.3.105.

Chapter 5

Problèmes connus et limitations

5.1 Netdata: affichage des informations dans la WebUI du GCenter v101

La refonte et l'ajout de nouvelles informations au niveau de Netdata rend inopérant les graphiques et statistiques affichées dans la WebUI du GCenter 101.

Les données sont cependant toujours consultables via l'API de Netdata.

5.2 Modification de la MTU d'un interface et tunnel VPN

La modification de la MTU d'une interface du GCap entraîne une ré-application de la configuration réseau de l'ensemble des interfaces.

Cela a pour incidence la perte de la connectivité entre le GCap et le GCenter (VPN IPsec) pour une durée d'environ 4 minutes.

5.3 Restauration de la sauvegarde sur le GCenter.

Lors d'une restauration de la sauvegarde sur le GCenter, le pairing avec les GCaps doit être à nouveau réalisé.

Chapter 6

Compatibilité logicielle

6.1 Compatibilité avec un autre GCap

Dans le cas d'utilisation avec la haute disponibilité (HA), les deux GCap doivent avoir la même version.

6.2 Compatibilité avec le GCenter

version du GCap	version du GCenter	Compatibilité
2.5.3.105	2.5.3.100 HF7	Configuration non supportée : GCenter à migrer vers une version plus récente
2.5.3.105	2.5.3.101 HF2	Configuration ok (limitation durant le processus d'installation de la nouvelle version du GCap)
2.5.3.105	2.5.3.101 HF3	Configuration ok
2.5.3.105	2.5.3.102	Configuration ok

Chapter 7

Comptabilité matérielle

La version 2.5.3.105 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 V2.5.3.105 depuis l'interface graphique du GCenter, ce-dernier devra être dans la version **V2.5.3.101-HF3** installée.

Si le GCenter est dans une version inférieure, il faudra le mettre à jour (pour les versions inférieures à la **V2.5.3.101**) ou avoir les privilèges nécessaires au niveau du GCap pour pouvoir déployer l'image directement en ligne de commande (pour la version **V2.5.3.101-HF2**).

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

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 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 Procédure d'installation en passant par le GCenter

1. Télécharger la nouvelle version disponible et le sha256 associé sur la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.3.105).
2. Faire la vérification de l'image avec le sha256 associé.
3. Se connecter à la WebUI du GCenter et aller dans le menu **Administrators** > **GUM** > **Upgrade**.
4. Dans la section **Upload an upgrade**, cliquer sur **choisir un fichier** puis sélectionner l'image précédemment téléchargée pour la mettre à disposition sur le GCenter. Si vous rencontrez un problème lors de la mise à disposition de l'image, veuiller essayer avec un autre navigateur.
5. Se connecter en SSH sur le GCap avec le compte **SETUP**.
6. Lancer l'utilitaire de configuration graphique avec la commande **gui**.
7. Désactiver le monitoring-engine et vérifier qu'il n'y ait plus d'eve-logs et fichiers à transmettre au GCenter.
8. Aller dans le menu **Upgrade**.
9. Valider la mise à jour en sélectionnant **"Yes, upgrade this GCap"**. Le GCap doit redémarrer automatiquement.
10. Se connecter en SSH avec le compte **SETUP** pour voir si la mise à jour a été correctement appliquée.
11. Réactiver le monitoring-engine avec la commande **monitoring-engine start** (GCAP-CLI).

En cas de problème, veuiller 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 sur la plate-forme https://update.gatewatcher.com/upgrade/ (répertoire 2.5.3.105).
2. Faire la vérification de l'image avec le sha256 associé.
3. Copier l'image (.gwp) dans le répertoire /tmp/ du GCap avec un compte à privilège.
4. Arrêter le monitoring engine avec la commande **monitoring-engine stop** (GCAP-CLI).
5. Lancer la mise à jour avec la commande **gcap-upgrade /tmp/nom_du_fichier** (SHELL).
6. Redémarrer le GCap avec la commande **system restart** (GCAP-CLI) : attention, la connexion en SSH va être interrompue.
7. Se connecter en SSH avec le compte **SETUP** pour voir si la mise à jour a été correctement appliquée.
8. Réactiver le monitoring-engine avec la commande **monitoring-engine start** (GCAP-CLI).

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

`PDF Note de version`