Documentation
GCap V2.5.4.1

Version : 1

Date de création : Juin 2025

Date de mise à jour : Juin 2025

Table des matières

Index **123**

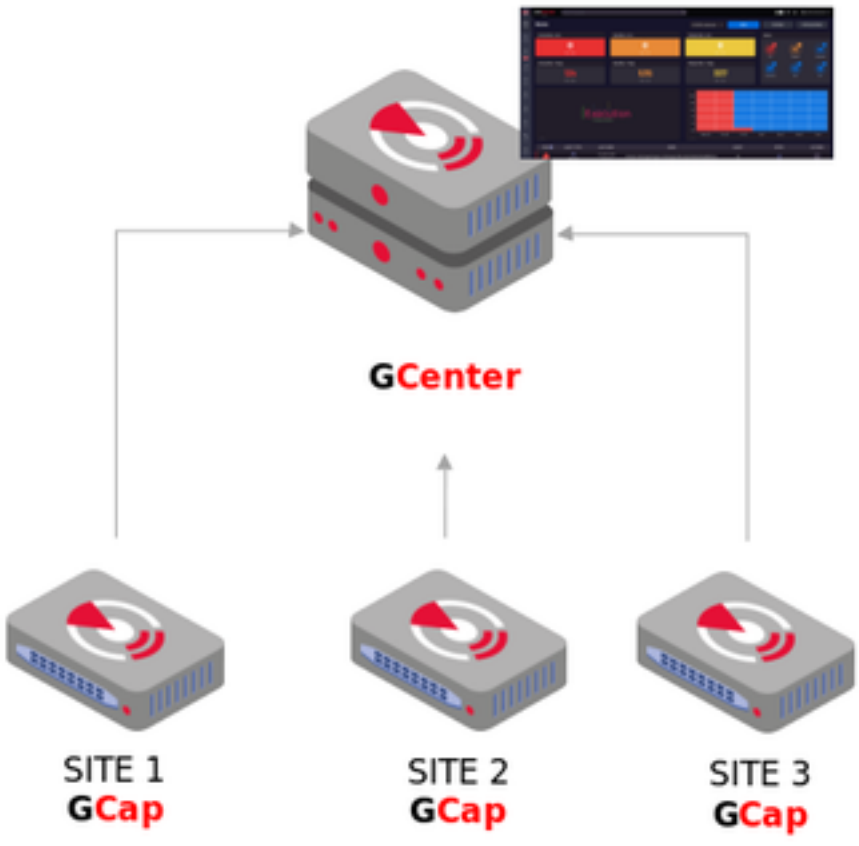
Chapitre 1

Description

1.1 Introduction

La solution AIONIQ est la plateforme de détection des intrusions informatiques – IDS (Intrusion Detection System) proposée par Gatewatcher.
Elle comprend :

- un ou plusieurs TAPS
- un ou plusieurs GCaps
- un GCenter



1.2 Le TAP

Un TAP (Test Access Point) est un dispositif passif qui permet de surveiller un réseau informatique en dupliquant les flux qui transitent et en les redirigeant vers une sonde d'analyse et de détection (le GCap).
Il est possible de connecter plusieurs TAPs à un GCap, ce dernier disposant de plusieurs interfaces de capture.

1.3 Le GCap

Le GCap est un composant de type sonde.
Il permet :

- de capturer et d'analyser le trafic réseau venant des TAPs
- de générer les événements, les alertes et les métadonnées
- de reconstruire les fichiers présents dans le flux
- de communiquer avec le GCenter

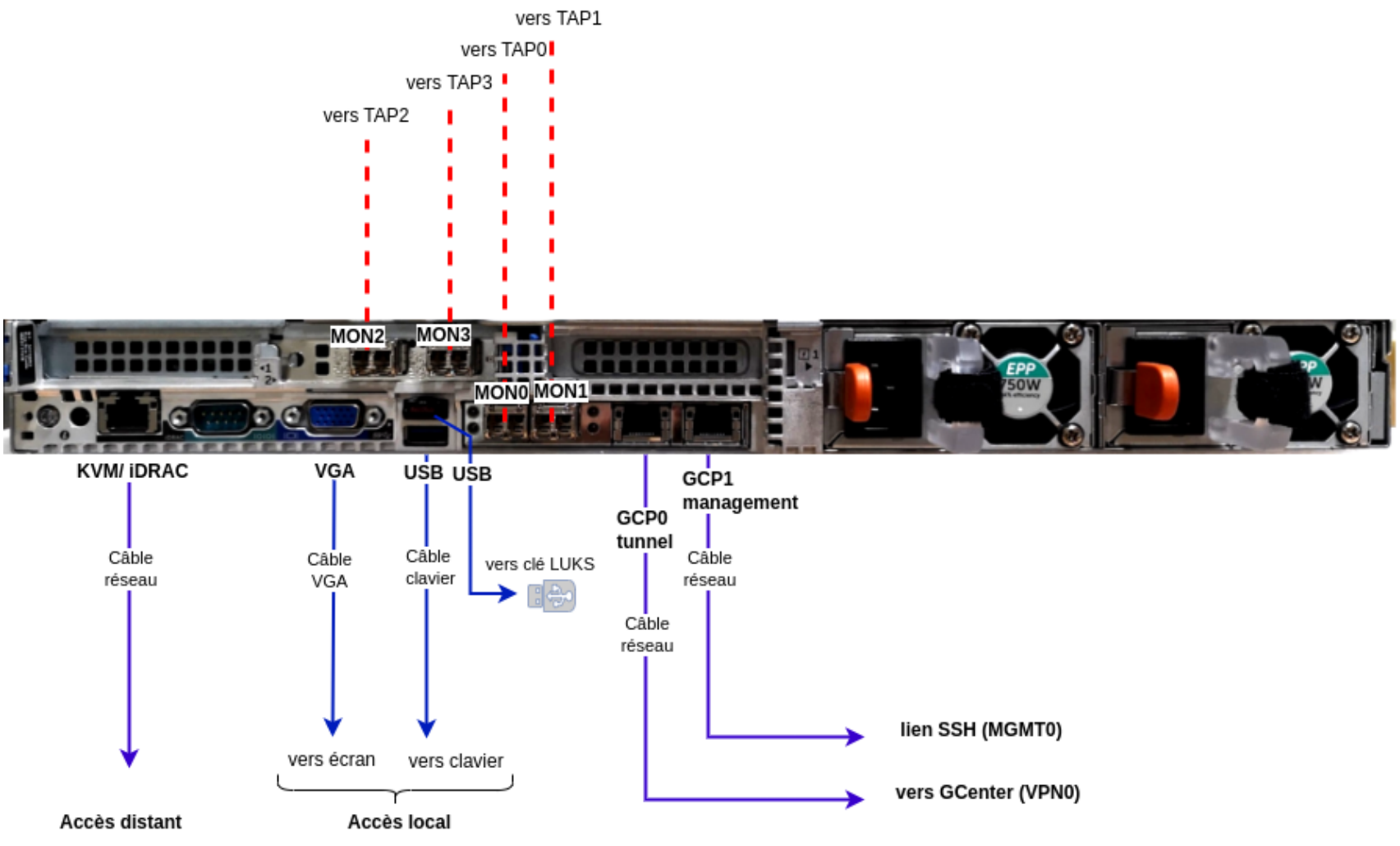
1.3.1 Différents modèles de serveurs

Pour plus d'informations, se référer à la partie *Caractéristiques*.

1.3.2 Description des entrées / sorties du GCap

La sonde de détection GCap possède :

- un connecteur USB et VGA pour accès direct avec un clavier et un écran.
  Ce mode de connexion est déprécié au profit de KVM/IDRAC/XCC et ne doit être utilisé qu'en dernier recours
- un connecteur USB pour accueillir la clé USB permettant le déchiffrement des disques (standard Linux Unified Key Setup)
- un connecteur RJ-45 pour l'accès à l'interface de gestion et de configuration du serveur (KVM/IDRAC/XCC)
- deux connecteurs RJ-45 `management` (`gcp1`) et `tunnel` (`gcp0`)
- des connecteurs RJ-45 et/ou fibre pour la surveillance `mon0` (rôle `capture`)
- deux alimentations électriques



1.3.2.1 Utilisation des connecteurs USB et VGA

Le branchement d'un clavier et d'un écran permet l'accès direct à l'interface console du serveur.

Important :

Ce mode est obsolète.
Il ne doit être utilisé qu'à l'installation initiale et pour du diagnostic avancé.

1.3.2.2 Accès à l'interface de gestion et de configuration du serveur

L'accès à cette interface de gestion se fait en HTTPS :

- sur un serveur Dell, ce connecteur est appelé **iDRAC** et est noté sur le schéma **KVM/IDRAC GCap**
- sur un serveur Lenovo, ce connecteur est appelé **TSM** : ce connecteur est identifiable grâce au symbole d'une clé anglaise présent en dessous

---

1.3.2.3 Interfaces réseau management (`gcp1`) et tunnel (`gcp0`)

Important :

Le concept de rôle est introduit dans la version 2.5.4.0.

Ces interfaces ont les rôles suivants :

- rôle 1 : communication sécurisée entre la sonde et le GCenter au travers d'un tunnel IPSEC afin de :
  - remonter des informations (fichiers, alertes, metadata...), issues de l'analyse des flux surveillés
  - remonter des informations sur l'état de santé de la sonde au GCenter
  - piloter la sonde (règles d'analyses, signatures, etc.)
- rôle 2 : administration distante au travers du protocole SSH avec l'accès :
  - à la CLI de la sonde
  - au menu graphique d'installation/configuration (déprécié)

En **configuration mono-interface**, ces rôles sont portées uniquement par un de ces interfaces.
En **configuration double-interface**, ces rôles sont attribués à l'interface (de préférence, les deux interfaces réseau gigabit ethernet intégrées, anciennement gcp0 et gcp1)

1.3.2.3.1 Configuration des interfaces réseau `management` et `tunnel`

Pour plus d'informations sur ces interfaces et leur configuration, se référer au paragraphe *Interfaces réseau `management` et `tunnel`*.

1.3.2.4 Interfaces de capture et de surveillance

Ces interfaces reçoivent :

- les flux issus des TAPs sur les interfaces indiquées (`mon0` à `monx`),
- le flux venant de fichiers préalablement enregistrés (fichiers pcap) sur un interface dédié `monvirt`.

Note :

Le nombre d'interfaces de capture est variable en fonction des spécificités de chaque modèle.

1.3.2.4.1 Activation des interfaces de capture et de surveillance `monx`

Pour plus d'informations, se référer au paragraphe *Interfaces de capture et de surveillance : activation*.

1.3.2.4.2 Agrégation des interfaces de capture et de surveillance `monx`

Pour plus d'informations, se référer au paragraphe *Interfaces de capture et de surveillance **mon** entre TAP et GCap : possibilité d'agrégation*.

1.3.3 Raccordement électrique

La sonde possède deux alimentations électriques qui ont chacune la puissance nécessaire au bon fonctionnement de l'équipement.
Il est fortement recommandé de raccorder chaque alimentation sur une arrivée électrique distincte.

1.3.4 Connecteur usb et clé LUKS

Lors de l'installation, le contenu des disques (hors /boot) est chiffré grâce au standard LUKS.
Lors de ce processus, une clé de chiffrement unique est générée et placée sur la clé USB connectée à la sonde.
Il est fortement recommandé de faire une copie de cette clé car, en cas de défaillance, les données présentes sur les disques ne seront plus accessibles.
Une fois le système démarré, la clé USB doit être retirée et placée dans un endroit sûr (ex : coffre-fort).

1.4 Le GCenter

Le GCenter est le deuxième composant de la solution qui fonctionne conjointement avec la sonde de détection GCap.
Il a pour fonctions principales :

- le pilotage de la sonde GCap (gestion des règles d'analyse, des signatures, supervision de l'état de santé...)
- l'analyse approfondie des fichiers remontés par la sonde
- l'administration de la solution
- l'affichage du résultat des différentes analyses dans différents tableaux de bord
- le stockage long-terme des données
- l'export des données dans des solutions tierces de type SIEM (Security Information and Entent Management)

Pour plus d'informations, se référer à la documentation du GCenter.

1.5 Interconnexion des sous-ensembles

1.5.1 Rappel des connexions du GCap

Suivant le moment et la configuration choisie et en regardant par l'arrière de gauche à droite, le GCap est connecté via :

- une prise réseau pour connexion d'un KVM / iDRAC
- un connecteur USB et VGA pour le branchement d'un clavier et d'un écran
- les interfaces de capture et de surveillance `mon0`, `mon1`, `mon2`, `monx` pour la connexion des TAPs
- les interfaces réseau intégrées anciennement `gcp0` et `gcp1`
  Suivant la configuration choisie (mono-interface ou double-interface), il est possible d'utiliser ces interfaces réseau pour la connexion vers le GCenter.
- les connecteurs des alimentations électriques du GCap

Pour plus d'information sur la description des connexions, se référer à la *Description des entrées / sorties du GCap*.

Note :

Ne pas oublier de connecter la clé LUKS de déchiffrement sur le port USB.

1.5.2 Interfaces de capture et de surveillance `monx` entre TAP et GCap : possibilité d'agrégation

La sonde GCap doit lire dans un seul flux, le flux réseau qui a été capturé dans les deux sens :

- un lien montant,
- un lien descendant.

Pour cela, il faut agréger les flux de chacun des liens en un seul flux.
Pour cela, il y a deux solutions :

- soit les flux ont été capturés et agrégés par un TAP agrégateur
- soit les flux ont été capturés mais non agrégés par un TAP non agrégateur

---

1.5.2.1 Mode de capture avec un TAP agrégateur

Dans ce cas, le GCap récupère le flux agrégé par le TAP sur une seule interface de capture `monx`.
Cette solution est préférable car c'est celle qui nécessite le moins de ressources du GCap à flux identique.

1.5.2.2 Mode de capture avec un TAP non agrégateur : mode GCap avec agrégation ("cluster")

Cette fonctionnalité est nécessaire si le TAP présent dans l'architecture n'assure pas la fonctionnalité d'agrégation d'interfaces.
Un **TAP qualifié** correspond à minima à un TAP dit passif ou non intelligent (simple).
C'est-à-dire qu'il ne nécessite pas d'alimentation propre et n'interagit pas activement avec les autres composants.
La plupart des TAP passifs n'ont pas de configuration embarquée.

Branchement entre TAP et GCap

Contrairement aux interfaces réseau dont le trafic est à la fois TX (émission) et RX (réception), les interfaces de capture sont unidirectionnelles et donc ne peuvent que recevoir du flux d'où le branchement suivant.
Chaque lien fibre physique gère deux liens :

- un lien montant, c'est-à-dire un lien TX
- un lien descendant, c'est-à-dire un lien RX

Le TAP (sans agrégation) est connecté au réseau via deux liens physiques appelés `commutateur X` et `commutateur Y`.
Le lien `commutateur X` relie le commutateur et le TAP entrée **X** et permet de dupliquer la moitié du flux réseau.
Le lien TX est :

- connecté sur **IN** du connecteur **X**
- le flux du lien TX est copié vers **OUT** du connecteur **Y** : celui-ci est connecté au lien RX du lien physique `commutateur Y`
- le flux du lien TX est aussi copié vers le lien **Xout** qui est envoyé vers le port d'entrée du GCap (lien **IN** du port `mon1`)

Le lien `commutateur Y` relie le commutateur et le TAP entrée **Y** et permet de dupliquer l'autre moitié du flux réseau.
Le lien TX est :

- connecté sur **IN** du connecteur **Y**
- le flux du lien TX est copié vers **OUT** du connecteur **X** : celui-ci est connecté au lien RX du lien physique `commutateur X`
- le flux du lien TX est aussi copié vers le lien **Yout** qui est envoyé vers le port d'entrée du GCap (lien **IN** du port `mon0`)

Agrégation d'interfaces (ou mise en cluster)

En définissant une agrégation de deux interfaces, le GCap agrège ces deux flux en un seul et permet donc d'avoir une interprétation de flux correct.
Si le GCap possède cette fonctionnalité, ceci n'est pas neutre en terme de ressources allouées à ce traitement et donc la configuration avec un TAP agrégateur doit être privilégiée.

`Images/GCAP_CLUSTER-v2.png`

1.5.2.3 Utiliser et configurer l'agrégation d'interfaces

Pour mettre en œuvre l'agrégation d'interfaces, se référer à la *Procédure de gestion de l'agrégation d'interfaces de capture*.

1.5.3 Transfert de règles entre GCenter et GCap : single-tenant vs multi-tenant

Pour plus d'informations, se référer au paragraphe *Interfaces de capture et de surveillance : single-tenant vs multi-tenant*.

Chapitre 2

Fonctionnement

2.1 Le GCap

2.1.1 Les fonctions du GCap

Les fonctions du GCap sont les suivantes :

- la connexion au TAP et la récupération des paquets dupliqués du flux réseau vu par le TAP,
- la reconstitution des fichiers à partir des paquets correspondants à l'aide d'un moteur de détection (appelé aussi Sigflow),
- la détection d'intrusions (vulnérabilités...) est effectuée par plusieurs moteurs de détection :
  - le premier est le moteur Sigflow. Il est situé dans le GCap
  - les suivants sont localisés dans le GCenter. Ils récupèrent le flux réseau envoyé par le GCap pour effectuer cette analyse :
    - Shellcode et Malicious Powershell Detect
    - Malcore et Retroanalyzer
    - Beacon Detect
    - Dga Detect
    - Ransomware Detect
    - Retrohunt (optionnel)
    - Active CTI (optionnel)
- la transmission des fichiers, codes, événements vers le GCenter,
- la communication entre GCap et GCenter (y compris la réception des fichiers de configuration, rulesets, etc.).

2.1.2 Le moteur Sigflow

Sigflow réalise donc :

- la récupération de flux réseau entrant dans le Gcap via les interfaces de capture `monx`,
- la détection d'intrusions, l'analyse statistique des flux réseau pour réduire le nombre de faux positifs et repérer d'éventuelles malformations protocolaires, des tentatives d'injection SQL, etc.,
- la création d'alertes ou de fichiers de journalisation.

L'utilisation de règles permet au moteur Sigflow de définir ce qu'il faut surveiller et donc de remonter des alertes.
Pour plus d'informations, se référer au tableau *Gérer le moteur de détection*.

2.1.2.1 Filtrage du flux capturé

Certaines parties du flux capturé ne peuvent être détectées, ni reconstruites : par exemple, les flux cryptés.
Si rien n'est fait, le système va monopoliser des ressources pour aboutir à un résultat connu par avance.
Pour éviter cela, il est possible de créer des règles pour filtrer le flux à capturer.

Note :

La commande `show/set advanced-configuration packet-filtering` a été supprimée.
Le filtrage des paquets doit être configuré dans le menu `GCaps profiles` du GCenter.

2.1.3 Compteurs de l'activité du GCap

Afin de pouvoir visualiser ces informations, la commande *'show eve-stats'* permet de visualiser les compteurs suivants :

- le compteur `Alerts` - Nombre d'alertes Sigflow trouvées
- les compteurs `Files` - Fichiers extraits par Sigflow
- les compteurs `Codebreaker samples` - Fichiers analysés par Codebreaker
- les compteurs `Protocols` - Listes des protocoles vus par Sigflow
- les compteurs `Detection Engine Stats` - Statistiques de Sigflow (*monitoring-engine*)

Pour plus d'informations, se référer au tableau *surveiller le moteur de détection*.

2.2 Configuration d'un GCap

2.2.1 Configuration d'un GCap et de son moteur Sigflow

Pour que le flux capturé soit analysé, les étapes suivantes doivent être réalisées :

- synchroniser la date et heure du GCap sur le GCenter : voir *Présentation de la gestion de la date et heure*
- gérer les interfaces Tunnel (`gcp1`) et Management (`gcp0`) : voir *Présentation de la gestion des interfaces réseau `gcp0` et `gcp1`*
- gérer les interfaces de capture : voir *Présentation de la gestion des interfaces de capture et de surveillance*
- gérer la configuration single-tenant vs multi-tenant des interfaces `monx` : voir *Interfaces de capture et de surveillance : single-tenant vs multi-tenant*
- gérer l'agrégation d'interfaces de capture : voir *Interfaces de capture et de surveillance : agrégation*
- appairage du GCap avec le GCenter
  Un GCap doit obligatoirement être appairé à un GCenter.
  L'échange de données ne commence que lorsque le tunnel VPN (IPsec) est établi entre les deux équipements.
- activation du moteur de détection Sigflow (par défaut, il est désactivé)

2.2.2 Présentation de la gestion de la date et heure

Lors de la première connexion, la date et heure du GCap et du GCenter doivent être identiques afin d'établir le tunnel IPsec.

2.2.2.1 Commandes dans la CLI

L'affichage de la date et heure courante se fait grâce à la commande *show datetime* dans la CLI.
La modification de la date et heure courante se fait grâce à la commande *set datetime* dans la CLI.

2.2.2.2 Procédures dans les cas d'utilisation

Pour la mise en œuvre, se référer à la *Procédure de modification de la date et heure du GCap*.
Par la suite, la date et l'heure du GCap sont synchronisées sur celles du GCenter après établissement du tunnel IPsec.

2.2.3 Présentation de la gestion des interfaces `Management` (`gcp1`) et `Tunnel` (`gcp0`)

Important :

Le concept de rôle est introduit dans la version 2.5.4.0.

Ces interfaces assurent les rôles suivants :

- rôle 1 : appelé `tunnel`, représente la communication sécurisée entre la sonde et le GCenter au travers d'un tunnel IPSEC afin de :
  - remonter des informations (fichiers, alertes, metadata, etc.) issues de l'analyse des flux surveillés
  - remonter des informations sur l'état de santé de la sonde au GCenter
  - piloter la sonde (règles d'analyses, signatures, etc.)
- rôle 2 : appelé `management`, représente l'administration distante au travers du protocole SSH avec l'accès :
  - à la CLI de la sonde
  - au menu graphique d'installation/configuration (obsolète)

2.2.3.1 Commandes dans la CLI

La gestion des interfaces réseau se fait à l'aide de commandes de la CLI dont la liste est donnée dans le tableau *Gérer le réseau*.

2.2.3.2 Visualisation ou configuration

Pour visualiser ou configurer les interfaces réseau, se reporter à la *Procédure de gestion des paramètres réseau des interfaces `Management` et `Tunnel`*.

2.2.3.2.1 Configuration mono-interface.

En **configuration mono-interface**, le rôle 1 et le rôle 2 sont assignés à une interface réseau.
Pour basculer de la configuration double-interface à la configuration mono-interface, se reporter à la *Procédure de basculement vers la configuration mono-interface*.

2.2.3.2.2 Configuration double-interface

Les rôles `Management` et `Tunnel` sont répartis sur deux interfaces réseau.

Important :

Cette configuration double-interface est obligatoire lorsque l'on utilise le **mode LPM** sur le GCenter.

Le but de ce cas de figure est de faire en sorte que le flux de management et le flux d'interconnexion entre le GCap et le GCenter soient isolés l'un de l'autre.

Note :

Depuis la version 2.5.4.0, vous pouvez attribuer un rôle au réseau de votre choix.
Nous recommandons l'utilisation d'interfaces gigabit intégrées (anciennement gcp0 et gcp1).

Pour basculer de la configuration mono-interface à la configuration double-interface, se référer à la *Procédure de basculement vers la configuration double-interface*.

2.2.4 Présentation de la gestion des interfaces de capture et de surveillance

Important :

Les concepts de rôle et de label ont été introduits dans la version 2.5.4.0.

Les interfaces de capture sur le GCap assurent le rôle de `capture` et sont, par défaut, au nombre de quatre.
Ces interfaces reçoivent les flux issus des TAPs sur les interfaces labellisées :

- `mon0` pour le premier TAP
- `mon1` pour le deuxième TAP
- `mon2` pour le troisième TAP
- `mon3` pour le quatrième TAP

Pour plus d'informations concernant les interfaces de capture, se référer au paragraphe *Interfaces de capture et de surveillance*.

Note :

Le nombre d'interfaces de capture est variable en fonction des spécificités de chaque modèle.

Dans certains cas particuliers, il est possible d'utiliser des GCap possédant huit interfaces au lieu de quatre.
De plus, il existe aussi un interface de capture virtuelle labellisée `monvirt`, qui permet le rejeu de fichier `.pcap` directement sur le GCap.
Afin que le GCap puisse capturer du flux, il est nécessaire de procéder à l'activation d'une ou plusieurs interfaces.

2.2.4.1 Commandes dans la CLI

La gestion des interfaces de capture se fait à l'aide de commandes de la CLI dont la liste est donnée dans le tableau *Gérer le réseau*.

2.2.4.2 Procédures dans les cas d'utilisation

Pour visualiser ou configurer les interfaces de capture, se reporter à la *Procédure de gestion des paramètres des interfaces de capture* `monx`.

2.2.5 Interfaces de capture et de surveillance : single-tenant vs multi-tenant

2.2.5.1 Moteur de détection du GCap et règles

SIGFLOW est le nom du moteur de détection du GCap configuré :

- par un ensemble de règles (RULESET) défini sur le GCenter
- par des règles définies localement et donc non connues du GCenter

Ces règles doivent décrire les caractéristiques des attaques qui devront être détectées mais doivent également être optimisées pour réduire les faux positifs.
L'ensemble de règles est composé de signatures regroupées par catégories qui ont été fournies par des sources.
Cette composition est effectuée par l'administrateur sur le GCenter et donc peut être configurée de façon différente en fonction du nombre de GCap et de leurs spécificités.

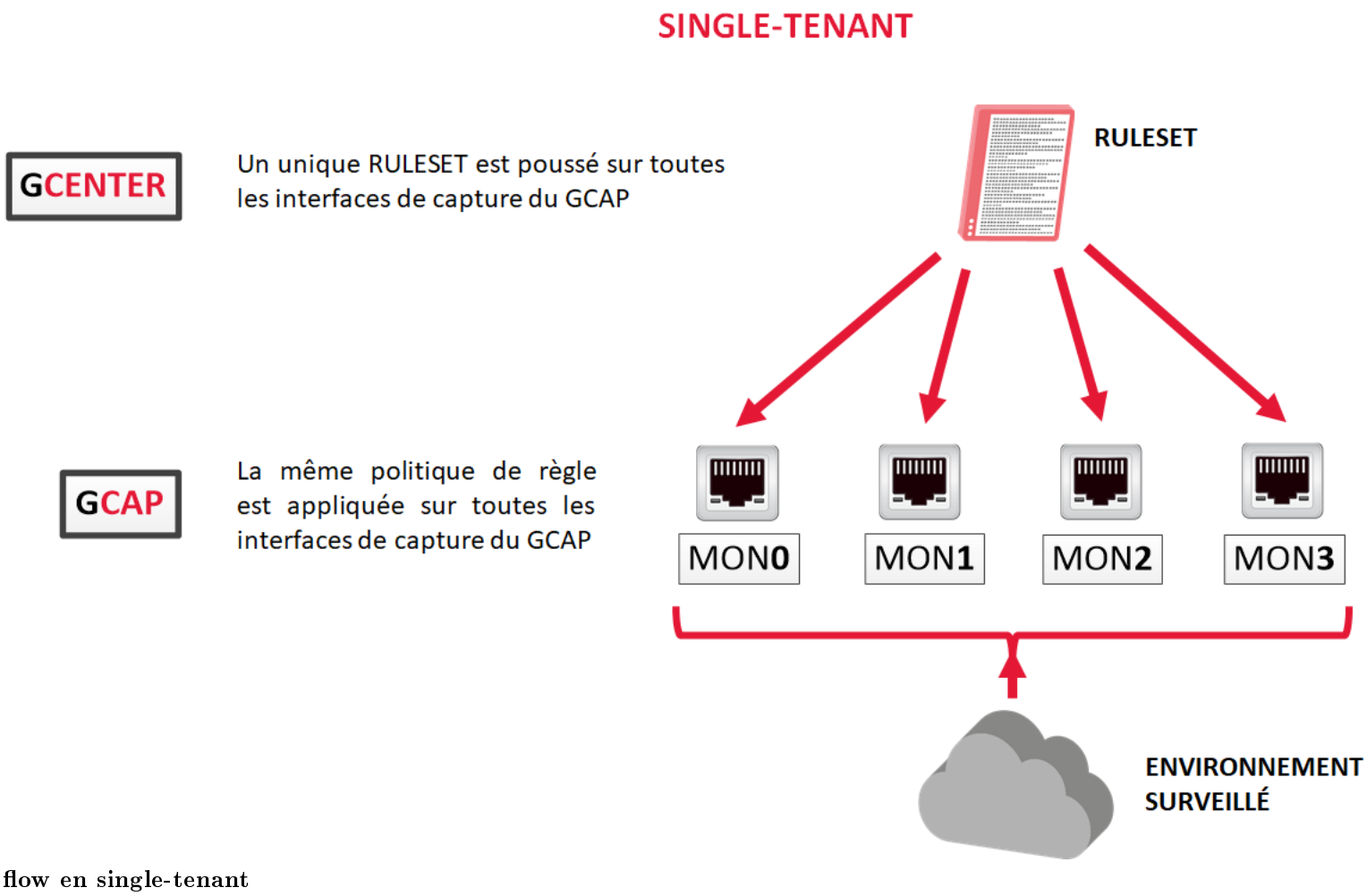
2.2.5.1.1 Commandes dans la CLI

La possibilité de visualiser / créer des règles locales est faite différemment suivant la configuration.
Pour avoir plus d'informations sur les règles, voir le tableau *Gérer le moteur de détection (fonctions avancées)*.

2.2.5.2 Transfert de l'ensemble de règles en mode single-tenant

2.2.5.2.1 Principe du single-tenant

Une fois défini sur le GCenter, un seul ensemble de règles (RULESET) est envoyé au moteur de détection du GCap.
Le moteur de détection du GCap applique cet ensemble de règles à toutes les interfaces de capture : c'est la configuration single-tenant.



Règles Sigflow en single-tenant

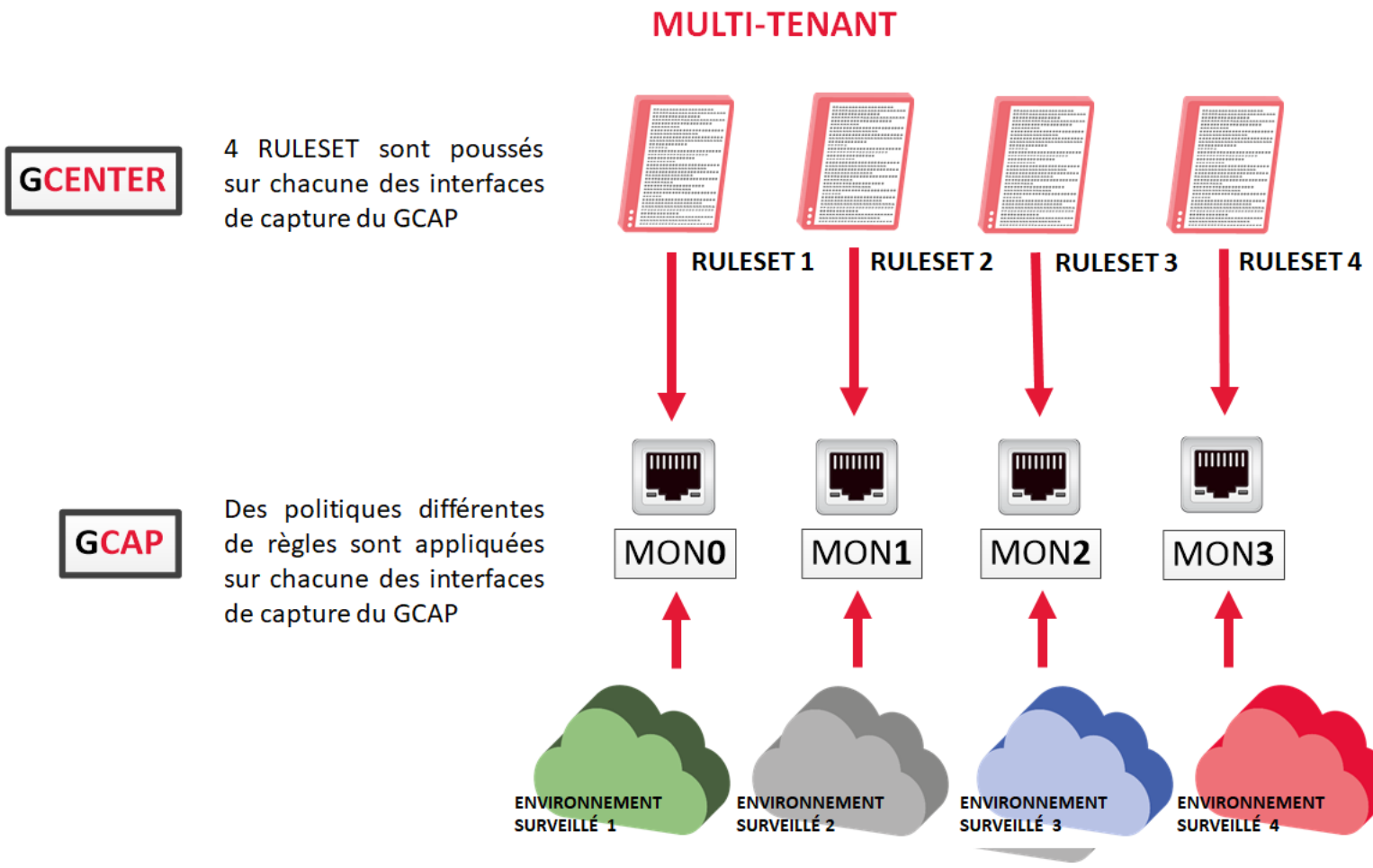
2.2.5.2.2 Configuration du mode single-tenant

Dans l'interface Web du GCenter, dans la partie `SIGFLOW - GCaps Profiles > Detection rulesets`, l'option par défaut est le single-tenant.

2.2.5.3 Transfert de l'ensemble de règles SIGFLOW en mode multi-tenant

2.2.5.3.1 Principe du multi-tenant

Une fois défini sur le GCenter, il est possible de définir un ensemble de règles SIGFLOW différent pour chacune des interfaces de capture.
Ensuite, chacun de ces ensembles de règles sera appliqué à son interface de capture : c'est la configuration **multi-tenant**.



Règles Sigflow en multi-tenant

À l'inverse du single-tenant, le multi-tenant va permettre d'optimiser les ressources et les coûts tout en simplifiant le processus de gestion des règles de détection par environnement.
La flexibilité de l'architecture permet d'affiner efficacement les règles de détection, d'isoler plus facilement les menaces et de personnaliser la capture.

2.2.5.3.2 Configuration du mode multi-tenant

Dans l'interface web du GCenter, dans la partie `SIGFLOW - GCaps Profiles > Detection rulesets`, l'option par défaut est le single-tenant.
Il est aussi possible de choisir deux autres options :

- 'Multi-tenant by interfaces' ou
- 'Multi-tenant by VLAN'

Dans le cas où une de ces options est sélectionnée, cela offre la possibilité d'attribuer des ruleset SIGFLOW différents pour :

- chacune des interfaces du GCap ou
- pour les différents VLAN...

...et ainsi avoir une supervision différente sur des réseaux différents.

Une optimisation des règles SIGFLOW au préalable est fortement conseillée avant de choisir cette option de configuration.
Les règles doivent en effet être adaptées à l'environnement surveillé.
Cette version du GCap permet d'être compatible avec le GCenter.

2.2.6 Interfaces de capture et de surveillance : agrégation

2.2.6.1 Principe de l'agrégation ("cluster")

Pour plus d'information, se référer à *Interfaces de capture et de surveillance entre TAP et GCap*.

2.2.6.2 Commandes dans la CLI

L'affichage de l'agrégation courante se fait grâce à la commande *show interfaces*.
La configuration de l'agrégation se fait grâce à la commande *set interfaces*.

2.2.6.3 Procédures dans les cas d'utilisation

Pour la mise en œuvre, se référer à la *Procédure de gestion de l'agrégation d'interfaces de capture*.

2.2.6.4 Configuration de l'agrégation

La création de l'agrégation se fait via l'invite de commande (CLI) du GCap.

2.2.6.5 Impact sur les autres fonctionnalités

La fonctionnalité de mise en agrégation des interfaces de capture sur le GCap a pour conséquence de dégrader certaines fonctions associées :

- la MTU (Maximum Transmission Unit) : la taille maximale d'un paquet pouvant être transmis en une seule fois sans fragmentation.
  La *MTU* prend la valeur la plus grande des interfaces qui composent l'agrégation.
- les règles statiques de filtrage des flux capturés par interface de monitoring : fonction Filtre XDP (eXpress Data Path).
  Filtre XDP : le filtrage XDP ne s'applique pas par défaut sur l'agrégation créée mais sur les interfaces qui le composent.

2.2.7 Moteur de détection Sigflow

Pour que le flux capturé soit analysé, les étapes suivantes doivent être réalisées :

- activer une ou plusieurs interfaces de capture sur le GCap
- appairer le GCap avec le GCenter
- activer le moteur de détection Sigflow (par défaut, il est désactivé)

2.2.7.1 Activation d'une ou plusieurs interfaces de capture et de surveillance sur le GCap

2.2.7.1.1 Commandes dans la

La gestion des interfaces de capture se fait à l'aide de commandes de la CLI dont la liste est donnée dans le tableau *Gérer le réseau*.

2.2.7.1.2 Procédures dans les cas d'utilisation

Pour visualiser ou configurer les interfaces de capture, se reporter à la *Procédure de gestion des paramètres des interfaces de capture* `monx`.

2.2.7.2 Agrégation des interfaces de capture et de surveillance `monx`

Pour plus d'informations sur cette agrégation, se référer au paragraphe *Interfaces de capture et de surveillance* ***monx*** *entre TAP et GCap : possibilité d'agrégation*.
Pour plus d'informations sur la configuration de cette agrégation, se référer au paragraphe Configuration des interfaces de capture et de surveillance : *agrégation*.

2.2.7.3 Appairage du GCap avec le GCenter

Une fois le paramétrage réseau fait, il est nécessaire d'appairer le GCap avec le GCenter.
Pour plus d'informations sur l'appairage, se référer à la procédure *Appairage entre un GCap et un GCenter*.

2.2.7.4 Activation du moteur d'analyse Sigflow

Par défaut, le moteur d'analyse du GCap est désactivé.

2.2.7.4.1 Vérification de l'état du moteur d'analyse Sigflow (procédure d'activation)

Il est possible de vérifier l'état du moteur avec la commande `show status`.

2.2.7.4.2 Démarrage du moteur d'analyse Sigflow

Il est indispensable de démarrer le moteur d'analyse Sigflow (moteur de détection).
La capture du flux n'est faite qu'après ce démarrage.
Pour cela :

- entrer la commande *monitoring-engine start*
- valider

```
(gcap-cli) monitoring-engine start
```

Le système affiche le message suivant indiquant que le moteur a été démarré.

```
Starting Detection Engine...
This operation may take a while... Please wait.
Detection Engine has been successfully started.
```

Une fois le moteur d'analyse activé, les possibilités de configuration de la sonde GCap changent.
Certaines ne sont plus paramétrables tant que le moteur est actif.

Note :

La commande *eve-stats* du sous-groupe *show* permet d'afficher les statistiques de Sigflow (*monitoring-engine*).

2.2.7.4.3 Période de grâce

La période de grâce est la somme de :

- la durée maximale de démarrage
- la durée maximale d'arrêt

Afin de pouvoir charger les règles du moteur de détection avant de démarrer le moteur, le moteur ne peut démarrer avant un certain temps appelé durée maximale de démarrage ou période de grâce du démarrage (start-timeout).

- La visualisation de la valeur courante se fait via la commande *show monitoring-engine start-timeout*.
- Si le nombre de règles chargées par le moteur d'analyse est important, alors la durée maximale de démarrage doit être modifiée via la commande *set monitoring-engine start-timeout*.

De la même façon, il existe la durée maximale d'arrêt ou période de grâce lors de l'arrêt du moteur (stop-timeout).

- La visualisation de la valeur courante se fait via la commande *show monitoring-engine stop-timeout*.
- La modification de la valeur courante se fait via la commande *set monitoring-engine stop-timeout*.

2.2.7.5 Désactivation du moteur de détection Sigflow

2.2.7.5.1 Vérification de l'état du moteur de détection Sigflow (procédure de désactivation)

Il est possible de vérifier l'état du moteur avec la commande `show status`.

2.2.7.5.2 Arrêt du moteur de détection Sigflow

De la même façon, l'arrêt s'effectue avec la commande *monitoring-engine stop* :

```
(gcap-cli) monitoring-engine stop
```

Le système affiche le message suivant indiquant que le moteur a été arrêté.

```
Stopping Detection Engine...
This operation may take a while... Please wait.
Detection Engine has been successfully stopped.
```

2.2.7.6 Mode de compatibilité

Le mode de compatibilité entre le GCap et le GCenter doit être renseigné via la *CLI*.

2.2.7.7 MTU

La MTU (Maximum Transfert Unit) de chaque interface de capture du GCap peut être ajustée via la CLI.
En effet la taille maximale d'un paquet pouvant être capturé en une seule fois sur une interface est paramétrable.

2.2.7.7.1 Affichage de la valeur courante de la MTU

Il est possible d'afficher la valeur de la MTU avec la commande *show interfaces* :

```
(gcap-cli) 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
```

L'administrateur peut modifier la valeur en octets de la MTU des interfaces de capture du GCap.
Cette valeur doit se trouver entre 1280 et 9000 octets.

Note :

A noter que la fonctionnalité de Filtrage XDP n'est pas supportée lorsque la MTU > 3000.

2.2.7.7.2 Modification de la valeur courante de la MTU

Concernant la modification de la MTU, cela se fait avec la commande *set advanced-configuration mtu* suivie des paramètres :

- nom de l'interface, par exemple enp4s0
- valeur, par exemple 1300

Note :

Pour modifier la MTU de l'interface `enp4s0` à 1300 :
- entrer la commande *set advanced-configuration mtu enp4s0 1300*
- valider

```
(gcap-cli) set advanced-configuration mtu enp4s0 1300
```

Le système affiche les informations de la mise à jour du paramètre.

```
Updating Monitoring Network MTU configuration to:
        - enp4s0: 1300
```

2.2.7.8 Reconstruction de fichiers

La reconstruction de fichiers a lieu sur le GCap grâce à son moteur de détection (Sigflow).
Ces fichiers sont reconstruits à certaines conditions paramétrables depuis le GCenter.
Ces conditions sont les suivantes :

- la taille du fichier observé
- le type de fichier observé (basé soit sur l'extension, soit sur le filemagic)

De plus, la reconstruction de fichier n'est possible que sur certains protocoles dont la liste diffère en fonction des différentes versions du GCap.
Voici la liste des protocoles supportés par le GCap :

- HTTP
- SMTP
- SMB

D'autres protocoles sont disponibles depuis le GCenter. Pour en savoir plus, se référer à la documentation du GCenter.

Note :

À savoir que les protocoles sur lesquels il est possible de reconstruire dépendent du GCap et non du GCenter. Si la configuration du GCenter spécifie au GCap de reconstruire un certain type de fichier mais que ce dernier n'en est pas capable, la reconstruction n'aura pas lieu.

2.3 GCaps en redondance : haute disponibilité

Note :

Cette fonctionnalité est obsolète.
Veuillez contacter Gatewatcher si vous voulez déployer une architecture redondante.

Chapitre 3

Caractéristiques

3.1 Caractéristiques mécaniques des GCaps

REFERENCE	DIMENSIONS (H x L x P)	RACKAGE	POIDS (KG)
GCAP1010HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP1020HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP1050HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP1100HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP1200HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP1400HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP2200HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP2600HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP2800HWr2	42,8 x 482 x 808,5 mm	1 U	21,9
GCAP5400HWr2	86,8 x 434 x 836 mm	2 U	36,6
GCAP5600HWr2	86,8 x 434 x 836 mm	2 U	36,6
GCAP5800HWr2	86,8 x 434 x 836 mm	2 U	36,6

3.2 Caractéristiques électriques des GCaps

REFERENCE	STOCKAGE LOCAL	PORTS DE CAPTURE	EXTENSION PORTS DE CAPTURE	ALIMENTATION ÉLECTRIQUE
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

3.3 Caractéristiques fonctionnelles des GCaps

3.3.1 Caractéristiques fonctionnelles

REFERENCE	DEBIT MAX	NOMBRE DE FICHIERS RECONSTRUITS MAX PAR S	NOMBRE DE SESSIONS MAX	NOMBRE DE NOUVELLES SESSIONS MAX PAR S	EPS MAX
GCAP1010HWr2	10 MBPS	1	1000	20	100
GCAP1020HWr2	20 MBPS	2	2000	50	100
GCAP1050HWr2	50 MBPS	2	5000	100	100
GCAP1100HWr2	100 MBPS	5	20000	1000	200
GCAP1200HWr2	200 MBPS	10	40000	2000	300
GCAP1400HWr2	400 MBPS	10	40000	2000	400
GCAP2200HWr2	1 GBPS	20	150 000	5 000	2000
GCAP2600HWr2	2 GBPS	30	200 000	10 000	3000
GCAP2800HWr2	4 GBPS	30	250 000	20 000	4000
GCAP5400HWr2	10 GBPS	50	500 000	50 000	8000
GCAP5600HWr2	20 GBPS	50	750 000	75 000	8000
GCAP5800HWr2	40 GBPS	50	1 000 000	100 000	8000

3.3.2 Liste des protocoles sélectionnables pour l'analyse

La détection des protocoles comprend deux 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.
  - 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.

Pour chaque interface, il est possible de :

- activer le parsing et le logging
- activer le parsing seulement
- désactiver le parsing et le logging

PROTOCOLE	PARSING	LOGGING
DCE-RPC	supporté	supporté
DHCP	supporté	supporté
DNP3	supporté	supporté
DNS_udp	supporté	supporté
DNS_tcp	supporté	supporté
ENIP	supporté	non supporté
FTP	supporté	supporté
HTTP	supporté	supporté
HTTP2	supporté	supporté
IKEv2	supporté	supporté
IMAP	parsing détection uniquement	non supporté
Kerberos (KRB5)	supporté	supporté
MODBUS	supporté	non supporté
MQTT	supporté	supporté
NETFLOW	non supporté	supporté
NFS	supporté	supporté
NTP	supporté	non supporté
RDP	supporté	supporté
RFB	supporté	supporté
SIP	supporté	supporté
SMB	supporté	supporté
SMTP	supporté	supporté
SNMP	supporté	supporté
SHH	supporté	supporté
TFTP	supporté	supporté
TLS	supporté	supporté

Ces options dépendent de la version du GCenter et donc de la compatibilité sélectionnée.
Pour plus d'informations, se référer à la documentation du GCenter.

3.3.3 Liste des protocoles sélectionnables pour la reconstruction de fichiers

PROTOCOLE	SUPPORTÉ
FTP	supporté
HTTP	supporté
HTTP2	supporté
NFS	supporté
SMB	supporté
SMTP	supporté

Ces options dépendent de la version du GCenter et donc de la compatibilité sélectionnée.
Pour plus d'informations, se référer à la documentation du GCenter.

Chapitre 4

Les comptes

4.1 Liste des comptes

Les accès distants ou locaux à l'interface d'administration du GCap sont protégés par une authentification.
Trois comptes génériques ont été définis avec des niveaux de droits différents :

Compte...	destiné à un...
gview	opérateur
gviewadm	responsable
setup	administrateur système

4.2 Principes associés

4.2.1 Mode d'authentification

L'authentification d'un utilisateur peut s'effectuer de deux façons différentes :

- identifiant / mot de passe
- clé SSH

Important :

La connexion simultanée de plusieurs comptes n'est pas possible.

4.2.2 Gestion des mots de passe

Le compte courant gère son propre de mot de passe mais potentiellement aussi d'autres comptes.
Le détail est donné dans le tableau ci-après :

Utilisateur	peut modifier le mot de passe		
	setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

La commande *show passwords* permet d'afficher la liste des utilisateurs gérés par le niveau courant.
La commande *set passwords* permet de modifier le mot de passe géré par le niveau courant.

4.2.3 Gestion de la politique des mots de passe

Les mots de passe saisis doivent correspondre à la politique de gestion des mots de passe.
La politique de gestion par défaut est la suivante :

Critère	Valeur par défaut
Nombre de caractères différents pour qu'un mot de passe soit considéré comme différent	2
Longueur minimum du mot de passe	12 caractères
Présence d'au moins une minuscule	oui
Présence d'au moins une minuscule	oui
Présence d'au moins une majuscule	oui
Présence d'au moins un chiffre (0 à 9)	oui
Présence d'au moins un symbole (c.à.d ni un chiffre ni une lettre)	oui

Cette politique est :

- visualisable via la commande *show password-policy*
- modifiable via la commande *set password-policy*

4.2.4 Clé SSH

L'authentification des connexions SSH pour administrer le GCap peut s'effectuer via une clé SSH.
L'ensemble des clés SSH autorisées pour un compte et la liste des différents types de chiffrement sont définis via la commande *set ssh-keys*.
Ce mode est à privilégier au couple login/mot de passe.
En effet, il permet de définir une clé par collaborateur, assurant ainsi une traçabilité des connexions et une imputabilité des actions.

4.2.5 Droits associés à chaque compte

Les droits associés à chaque compte sont listés dans la présentation de chaque compte.

4.3 Profil gview

Pour se connecter avec le compte **gview**, le mot de passe par défaut est : default

Note :

Il est nécessaire de modifier le mot de passe dès la première connexion et de le conserver dans un endroit sûr, par exemple, avec les clefs de chiffrement des **GCap**.

Depuis le compte **gview**, il sera possible :

- d'accéder aux commandes de l'ensemble `show` pour :
  - afficher la disposition du clavier (`show keymap`)
  - afficher la liste des utilisateurs gérés par le niveau courant (`show passwords`)
  - afficher l'état courant du GCap (`show status`)
  - afficher les statistiques du moteur de détection Sigflow (`show eve-stats`)
  - afficher la politique de mot de passe pour les comptes (`show password-policy`)
- d'accéder aux commandes de l'ensemble `set` pour :
  - changer le mot de passe de l'utilisateur courant et du niveau inférieur (`set passwords`)
  - changer la configuration du clavier (`set keymap`)
  - changer les clés SSH pour l'utilisateur courant et le niveau inférieur (`set ssh-keys`)

Ce compte correspond à un profil d'opérateur, membre d'un service de détection en charge de l'exploitation du service.

Note :

Les commandes présentes dans le compte **gview** sont aussi présentes sur les autres comptes **gviewadm** et **setup**.

4.4 Profil gviewadm

Pour se connecter avec le compte **gviewadm**, le mot de passe par défaut est : default

Note :

Il est nécessaire de modifier le mot de passe dès la première connexion, et de le conserver dans un endroit sûr, par exemple, avec les clefs de chiffrement des **GCap**.

En plus des fonctions communes de **gview**, le compte **gviewadm** a les fonctions supplémentaires suivantes :

- accéder aux commandes de l'ensemble `show` pour afficher des statistiques et des informations de santé du GCap (`show health`)
- démarrer, arrêter, visualiser l'état du moteur de détection (`monitoring-engine`)

Ce compte correspond à un profil d'administrateur, membre du service de détection disposant de droits privilégiés lui permettant d'assurer le bon fonctionnement des dispositifs du service de détection.

Note :

Les commandes présentes dans le compte **gviewadm** sont aussi présentes sur le compte **setup**.

4.5 Profil setup

Pour se connecter avec le compte **setup**, le mot de passe par défaut est : default

Note :

Il est nécessaire de modifier le mot de passe dès la première connexion, et de le conserver dans un endroit sûr, par exemple, avec les clefs de chiffrement des **GCap**.

En plus des fonctions communes de **gviewadm**, le compte **setup** a les fonctions supplémentaires suivantes :

- accéder aux commandes de l'ensemble `show` pour afficher :
  - les informations sur les interfaces de capture disponibles (`show interfaces`)
  - le mode de compatibilité utilisé pour interagir avec le GCenter (`show compatibility-mode`)
  - la date et l'heure du GCap (`show datetime`)
  - la politique du système de protection (`show bruteforce-protection`)
  - le temps d'inactivité avant la déconnexion d'une session utilisateur (`show session-timeout`)
  - l'adresse IP du GCenter avec lequel le GCap est appairé (`show gcenter-ip`)
  - les options avancées de la configuration du moteur de détection (`show monitoring-engine`)
  - les informations du GCap demandées par le support technique (`show tech-support`)
- accéder aux commandes avancées de l'ensemble `show advanced-configuration` pour afficher :
  - les règles statiques de filtrage du flux (`show advanced-configuration packet-filtering`)
- accéder aux commandes de l'ensemble `set` pour :
  - gérer le système de protection contre les attaques par force brute (`set bruteforce-protection`)
  - configurer l'agrégation sur les interfaces de capture du GCap (`set clusters`)
  - modifier le mode de compatibilité utilisé pour interagir avec le GCenter (`set compatibility-mode`)
  - ajuster la date et l'heure (`set datetime`)
  - spécifier l'adresse IP du GCenter auquel le GCap sera appairé (`set gcenter-ip`)
  - administrer les interfaces de capture réseau (`set interfaces`)
  - changer la configuration du clavier (`set keymap`)
  - appliquer une configuration avancée pour le moteur de détection de la sonde GCap (`set monitoring-engine`)
  - modifier la configuration réseau (`set network-config`)
  - définir une politique de mot de passe pour les comptes (`set password-policy`)
  - configurer le temps d'inactivité avant la déconnexion (`set session-timeout`)
- accéder aux commandes avancées de l'ensemble `set advanced-configuration` pour :
  - modifier la valeur de la MTU des interfaces de capture activées (`set advanced-configuration mtu`)
- accéder aux commandes de l'ensemble `system` pour gérer le serveur :
  - redémarrer le GCap (`system restart`)
  - éteindre le GCap (`system shutdown`)
  - réinitialiser le verrouillage des comptes `gview`, `gviewadm` et `setup` suite à des tentatives d'authentification infructueuses (`system unlock`)
- accéder aux commandes `pairing` pour associer un GCap à un GCenter :
  - appairer un GCap (`pairing`)
  - supprimer un appairage existant (`unpair`)

Ce compte correspond à un profil d'administrateur, membre du service de détection disposant de droits privilégiés lui permettant d'assurer le bon fonctionnement des dispositifs du service de détection.

4.6 Liste des fonctions par niveau et par thème

4.6.1 Configurer le GCap

Tableau 1 – Configurer le GCap

Fonction par niveau	setup	gviewadm	gview
Configuration du clavier : afficher	show keymap	show keymap	show keymap
Configuration du clavier : modifier	set keymap	set keymap	set keymap
Date et heure : afficher	show datetime	N/A	N/A
Date et heure : modifier	set datetime	N/A	N/A
Couleurs : activer ou désactiver pour l'instance en cours	colour	colour	colour
Mode de compatibilité avec le GCenter : afficher	show compatibility-mode	N/A	N/A
Mode de compatibilité avec le GCenter : modifier	set compatibility-mode	N/A	N/A
Appairage avec le GCenter	pairing	N/A	N/A
Désapparier le GCap	unpair	N/A	N/A

4.6.2 Gérer les comptes

Tableau 2 – Gérer les comptes

Fonction par niveau	setup	gviewadm	gview
Authentification : afficher la liste des utilisateurs	show passwords	show passwords	show passwords
Authentification : modifier les mots de passe	set passwords	set passwords	set passwords
Authentification : modifier les clés SSH	set ssh-keys	set ssh-keys	set ssh-keys
Authentification : afficher la politique de mot de passe	show password-policy	show password-policy	N/A
Authentification : déverrouiller les comptes bloqués	system unlock	N/A	N/A
Authentification : définir une politique de mot de passe	set password-policy	N/A	N/A
Authentification : afficher la politique de protection contre les attaques par force brute	show bruteforce-protection	N/A	N/A
Authentification : modifier la politique de protection contre les attaques par force brute	set bruteforce-protection	N/A	N/A
Session : afficher la durée d'inactivité avant la déconnexion	show session-timeout	N/A	N/A
Session : modifier la durée d'inactivité avant la déconnexion	set session-timeout	N/A	N/A

4.6.3 Gérer le moteur de détection

Tableau 3 – Gérer le moteur de détection

Fonction par niveau	setup	gviewadm	gview
Configuration de Sigflow : afficher les options avancées	show monitoring-engine	N/A	N/A
Configuration de Sigflow : appliquer une configuration avancée	set monitoring-engine	N/A	N/A
Configuration de Sigflow : démarrer le moteur de détection	monitoring-engine start	monitoring-engine start	N/A
Configuration de Sigflow : arrêter le moteur de détection	monitoring-engine stop	monitoring-engine stop	N/A
Configuration de Sigflow : afficher l'état	monitoring-engine status	monitoring-engine status	N/A
Génération de trafic : rejouer un fichier pcap	replay	replay	N/A

4.6.4 Gérer le réseau

Tableau 4 – Gérer le réseau

Fonction par niveau	setup	gviewadm	gview
Configuration réseau : consulter la configuration réseau (adresses IP, nom, domaine...)	show network-config	N/A	N/A
Configuration réseau : modifier la configuration	set network-config	N/A	N/A
Adresse IP du GCenter : afficher l'adresse IP du GCenter avec lequel le GCap est appairé	show gcenter-ip	N/A	N/A
Adresse IP du GCenter : spécifier l'adresse IP du GCenter auquel le GCap sera appairé	set gcenter-ip	N/A	N/A
Interfaces de détection : afficher les informations	show interfaces	N/A	N/A
Interfaces de détection : configurer	set interfaces	N/A	N/A
Interfaces de détection : afficher la valeur de la MTU	show advanced-configuration mtu	N/A	N/A
Interfaces de détection : modifier la valeur de la MTU	set advanced-configuration mtu	N/A	N/A
Agrégation des interfaces de détection : afficher les informations	show clusters	N/A	N/A
Agrégation des interfaces de détection : configurer	set clusters	N/A	N/A

4.6.5 Gérer le serveur

Tableau 5 – Gérer le serveur

Fonction par niveau	setup	gviewadm	gview
Afficher l'aide sur les commandes	help	help	help
Quitter la session en cours ou quitter la session SSH	exit	system restart	system restart
Système : éteindre le GCap	system shutdown	N/A	N/A

4.6.6 Surveiller le GCAP

Tableau 6 – Surveiller le GCAP

Fonction par niveau	setup	gviewadm	gview
Surveillance : afficher l'état courant du GCap	show status	show status	show status
Surveillance : afficher les statistiques du moteur de détection Sigflow	show eve-stats	show eve-stats	show eve-stats
Surveillance : afficher les statistiques et les informations de santé	show health	show health	N/A
Surveillance : extraire les informations du GCap demandées par le support technique	show tech-support	N/A	N/A

Chapitre 5

Cas d'utilisation

5.1 Introduction

Pour la configuration initiale du GCap et pour faire des configurations ou vérifications avancées, il est nécessaire d'utiliser la CLI.
Pour la plupart des fonctions, l'utilisation de cette interface est suffisante.
Les tableaux listés dans la section *Liste des procédures* permettent d'avoir une vision générale sur les actes courants.

5.2 Comment se connecter au Gcap ?

L'accès au GCap peut être fait :

- soit par une connexion directe (se connecter directement au serveur)
- soit par une connexion à distance HTTP (fonction iDRAC pour un serveur Dell)
- soit par une connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série
- soit par une connexion à distance à la CLI en SSH via une interface avec le rôle `management` (anciennement `gcp0` ou `gcp1`)

L'accès au système d'exploitation et à la CLI pour gérer le GCap peut être fait à distance via une connexion SSH ou HTTP.

Note :

La liste des connecteurs physiques à utiliser a été décrite dans la partie PRESENTATION - Généralités.

5.2.1 Connexion directe et configuration

Aucune configuration spécifique n'est requise, si ce n'est de connaître le nom d'utilisateur et le mot de passe de l'iDRAC.
Cet accès peut être fait pour configurer la connexion réseau de l'iDRAC entre autres.
Pour la mise en œuvre, se référer à la *Procédure de connexion directe au GCap*.

Note :

L'identifiant et le mot de passe par défaut sont indiqués dans la documentation du fabricant du serveur.

5.2.2 Connexion à distance à l'iDRAC en HTTP (serveur DELL)

L'accès distant se fait :

- via la connexion réseau connectée sur le port iDRAC du GCap
- en utilisant un navigateur WEB

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- que la configuration réseau ait été faite (adresse IP de l'iDRAC connue)

Cette connexion n'est pas la façon normale d'accéder au GCap mais permet d'accéder au GCap en cas de problèmes.
Pour la mise en œuvre, se référer à la *Procédure de connexion à distance en HTTP à l'iDRAC*.

5.2.3 Connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série

L'accès distant se fait :

- via la connexion réseau connectée sur le port iDRAC du GCap
- en utilisant un outil de connexion via SSH

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- que la configuration réseau ait été faite (adresse IP de l'iDRAC connue)

Cette connexion n'est pas la façon normale d'accéder au GCap mais permet d'accéder au GCap en cas de problèmes.
Pour la mise en œuvre, se référer à la *Procédure de connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série*.

5.2.4 Connexion à distance à la CLI en SSH via les interfaces réseau avec le rôle `management` (anciennement `gcp0`ou `gcp1`)

L'accès distant à la CLI du GCap se fait via la connexion réseau connectée sur le port :

- avec le rôle `management` (configuration double-interface - anciennement gcp1)
- avec le rôle `management-tunnel` (configuration mono-interface - anciennement gcp0)

Cette connexion est la façon nominale d'accéder au GCap.
Pour plus d'informations, voir la *Procédure de connexion sur le GCap via SSH*.

5.3 Connexion à distance au GCenter

L'accès distant au GCenter se fait soit :

- en SSH pour configurer le GCenter. Pour plus d'informations, se référer à la documentation du GCenter.
- via un navigateur web pour pouvoir appairer le GCap. Pour plus d'informations, voir la *Procédure de connexion au GCenter via un navigateur web*.

5.4 Comment utiliser les procédures

5.4.1 Accéder au GCap et au GCenter

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Première connexion au GCap par une connexion directe	1	*Connexion directe au GCap avec clavier et écran*
Connexion à distance à l'iDRAC en HTTP	1	*Connexion à distance à l'iDRAC en HTTP*
Connexion à distance en SSH en mode redirection du port série	1	*Connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série*
Connexion au GCenter via un navigateur web	1	*Connexion au GCenter via un navigateur web*

5.4.2 Configurer le GCap

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
La première installation du GCap	1	*Configuration du GCap lors de la première connexion*
	2	*Mise en exploitation d'un GCap*
Configuration du clavier	1	Afficher : utiliser la commande *show keymap*
	2	Modifier : utiliser la commande *set keymap*
Configurer l'interface GCap : (GUI ou CLI)	1	Afficher : utiliser la commande *show setup-mode*
	2	Modifier : utiliser la commande *set setup-mode*
Date et l'heure	1	Afficher : utiliser la commande *show datetime*
	2	Modifier : utiliser la procédure *Modification de la date et heure du GCap*
Couleurs dans l'affichage	1	Activer ou désactiver : utiliser la commande *colour*
Mode de compatibilité avec le GCenter	1	Afficher : utiliser la commande *show compatibility-mode*
	2	Modifier : utiliser la commande *set compatibility-mode*
Appairage avec le GCenter	1	Utiliser la procédure *Appairage entre un GCap et un GCenter*

5.4.3 Gérer les comptes

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Authentification : la liste des utilisateurs	1	Afficher la liste : utiliser la commande *show passwords*
	2	Modifier les mots de passe : utiliser la commande *set passwords*
Authentification : modifier les clés SSH	1	Utiliser la commande *set ssh-keys*
Authentification : afficher la politique de mot de passe	1	Utiliser la commande *show password-policy*
Authentification : déverrouiller les comptes bloqués	1	Utiliser la commande *system unlock*
Authentification : définir une politique de mot de passe	1	Utiliser la commande *set password-policy*
Authentification : afficher la politique de protection contre les attaques par force brute	1	Utiliser la commande *show bruteforce-protection*
Authentification : modifier la politique de protection contre les attaques par force brute	1	Utiliser la commande *set bruteforce-protection*
Session : afficher la durée d'inactivité avant la déconnexion	1	Utiliser la commande *show session-timeout*
Session : modifier la durée d'inactivité avant la déconnexion	1	Utiliser la commande *set session-timeout*

5.4.4 Gérer le réseau

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Gérer les interfaces Tunnel (gcp0) et Management (gcp1)	1	Utiliser la procédure *Gestion des paramètres réseau des interfaces gcp0 et gcp1*
Adresse IP du GCenter : afficher l'adresse IP du GCenter	1	Utiliser la commande *show gcenter-ip*
Adresse IP du GCenter : modifier l'adresse IP du GCenter	1	Utiliser la commande *set gcenter-ip*
Gérer les interfaces de capture monx	1	Utiliser la procédure *Gestion des paramètres des interfaces de capture monx*
Gérer l'agrégation d'interfaces de capture	1	Utiliser la procédure *Gestion de l'agrégation d'interfaces de capture*
Basculer vers la configuration simple-interface	1	Utiliser la procédure *Basculement vers la configuration simple-interface*
Basculer vers la configuration double-interface	1	Utiliser la procédure *Basculement vers la configuration double-interface*

5.4.5 Gérer le moteur de détection

Tableau 1 – Fonctions de base

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Afficher les options avancées	1	Utiliser la commande *show monitoring-engine*
Appliquer une configuration avancée	1	Utiliser la commande *set monitoring-engine*
Démarrer le moteur de détection	1	Utiliser la commande *monitoring-engine start*
Arrêter le moteur de détection	1	Utiliser la commande *monitoring-engine stop*
Afficher l'état du moteur de détection	1	Utiliser la commande *monitoring-engine status*
Génération de trafic : rejouer un fichier pcap	1	Utiliser la commande *replay*

5.4.6 Gérer le serveur

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Quitter la session en cours ou quitter la session SSH	1	Utiliser la commande *exit*
Système : redémarrer le GCap	1	Utiliser la commande *system restart*
Système : éteindre le GCap	1	Utiliser la commande *system shutdown*

5.4.7 Surveiller le GCAP

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Surveillance : afficher l'état courant du GCap	1	Utiliser la commande *show status*
Surveillance : afficher les statistiques du moteur de détection Sigflow	1	Utiliser la commande *show eve-stats*
Surveillance : afficher des statistiques et des informations de santé	1	Utiliser la commande *show health*
Surveillance : extraire les informations du GCap demandée par le support technique	1	Utiliser la commande *show tech-support*

5.5 Liste des procédures

5.5.1 Configuration du GCap lors de la première connexion

5.5.1.1 Introduction

La procédure décrite ici indique comment configurer le GCap lors de la première installation.

5.5.1.2 Prérequis

- **Utilisateur :** setup

5.5.1.3 Opérations préliminaires

- Vérifier que la clé LUKS soit bien connectée sur le GCap.

Note :

S'il n y a pas de clé LUKS ou si ce n'est pas la bonne, le système d'exploitation ne pourra pas accéder au contenu des disques durs.
En cas de problèmes, vérifier :

- que la clé soit bien la bonne (et non celle d'un autre GCap...)
- le bon fonctionnement du port USB : changer de port USB

- Se connecter sur le GCap.
- Suivant le cas :
  - soit se connecter directement au GCap via clavier et écran (voir *Procédure de connexion directe au GCap*)
  - soit se connecter au GCap via l'iDRAC (voir *Procédure de connexion au GCap via l'iDRAC*)
- Se connecter en tant que **setup**.

Note :

Lors de la première connexion au GCap, une invitation à changer le mot de passe est affichée.
Faire attention à la configuration du clavier (version fr ou en).

5.5.1.4 Procédure

- Gérer les mots de passe (mots de passe, clé SSH, etc.) : voir le tableau *Gérer les comptes*.
- Gérer les interfaces réseau avec les rôles `Tunnel` (`gcp0`) et `Management` (`gcp1`) : voir le tableau *Gérer le réseau*.
  - configurer l'adressage IP
  - entrer le nom du GCap et le nom du domaine
  - configurer la valeur de la MTU si besoin
    Pour ce faire, voir la *Procédure de gestion des paramètres réseau des interfaces `gcp0` et `gcp1`*.
  - Se connecter au GCap via une connexion distante via un tunnel SSH (voir *Connexion à distance au GCap via un tunnel SSH*).
  - définir le mode de fonctionnement pour le lien SSH en simple-interface ou double-interface
    Pour ce faire, voir la *Procédure de basculement vers la configuration simple-interface* ou la *Procédure de basculement vers la configuration double-interface*.
- Gérer la date et heure du GCap : voir la *Procédure de modification de la date et heure du GCap*.

- Gérer les interfaces de capture : voir le tableau *Gérer le réseau*.
  - activer les interfaces souhaitées
  - configurer la valeur de la MTU
    Pour ce faire, voir la *Procédure de gestion des paramètres des interfaces de capture monx*.
- Si besoin, gérer l'agrégation d'interfaces de détection : voir la *Procédure de gestion de l'agrégation d'interfaces de capture*.
- Si besoin, gérer la haute disponibilité des GCaps : voir la *Procédure de gestion de la haute disponibilité de GCaps*.
- Appairer le GCap avec le GCenter : voir la *Procédure d'appairage entre un GCap et un GCenter*.
  - sur le GCenter,
    - se connecter en SSH
    - connaître l'adresse IP du GCenter
  - sur le GCap, saisir l'adresse IP du GCenter
  - sur le GCenter, déclarer le GCap et générer l'OTP (One Time Password)
  - sur le GCap, appairer le GCap et le GCenter
- Mettre en exploitation le GCap : voir la *Procédure de mise en exploitation d'un GCap*.

5.5.2 Mise en exploitation d'un GCap

5.5.2.1 Introduction

Après avoir configuré le GCap, cette procédure indique comment mettre en exploitation le GCap.

5.5.2.2 Prérequis

- **Utilisateur :** setup

5.5.2.3 Opérations préliminaires

- Effectuer la *Procédure de première connexion au GCap*.
- Activer les interfaces de capture nécessaires (`monx`) : voir la *Procédure de gestion des paramètres des interfaces de capture monx*.

5.5.2.4 Procédure à effectuer sur le GCap

- Lancer le moteur de détection : voir tableau *Gérer le moteur de détection*.
  Le système affiche l'invite de commande suivant :

```
Monitoring DOWN gcap-name (gcap-cli)
```

L'invite de commande indique l'état du moteur de détection : ici il est arrêté.

- Entrer la commande suivante.

```
(gcap-cli) monitoring-engine start
```

- Valider.
- Attendre que le moteur soit lancé.
- Vérifier l'état du moteur de détection.
  Le système affiche l'invite de commande suivant :

```
[Monitoring UP] gcap-name (gcap-cli)
```

L'invite de commande indique l'état du moteur de détection : ici il est démarré.

5.5.2.5 Procédure à effectuer sur le GCenter

- Appliquer un ruleset au GCap.
- Activer ou non la détection des shellcodes.
- Activer ou non la détection des powershells.
- Configurer les paramètres propres à Sigflow (à savoir Base variables, Net variables et File rules management).

5.5.3 Connexion directe au GCap avec clavier et écran

5.5.3.1 Introduction

La première connexion au GCap peut s'effectuer par une connexion directe (avec clavier et écran).
Cela est nécessaire lorsque la configuration réseau n'est pas encore effectuée sur le GCap (ou en cas de non connaissance de l'adresse réseau).

5.5.3.2 Opérations préliminaires

- Connecter les câbles d'alimentation du GCap.
- Connecter les câbles réseau du GCap (*voir partie Description / Le GCap*).

5.5.3.3 Procédure de connexion de l'écran et clavier

- Connecter l'écran sur le connecteur VGA du GCap.
- Connecter le clavier sur le connecteur USB du GCap.
- Mettre sous tension le serveur.

5.5.3.4 Procédure pour connaître les paramètres réseau via le BIOS

- Appuyer sur **F2** pendant l'auto-test de démarrage (POST).
- Sur la page `System Setup Main Menu` (menu principal de la configuration du système), cliquer sur `iDRAC Settings` (Paramètres iDRAC).
  La page `Paramètres iDRAC` s'affiche.
- Cliquer sur `Réseau`.
  La page Réseau s'affiche.
- Noter les paramètres réseaux dans les paramètres `Network Settings`.
- Après avoir noté la configuration réseau, sortir du BIOS.
- Cliquer successivement sur `Retour`, `Terminer` et `Non`.

5.5.3.5 Procédure pour accès à la CLI

L'invite de commande est affichée :

```
gcap-protor login:
```

- Entrer l'identifiant et le mot de passe correspondant.
  L'invite de commande suivante est affichée :

```
gcap-protor (gcap-cli)
```

Note :

Lors de la première connexion au GCap, une invitation à changer le mot de passe est affichée.

Note :

- Appuyer sur **Tab** pour afficher toutes les commandes disponibles.
- Appuyer sur **Entrée** pour afficher toutes les commandes disponibles et une courte explication.

Astuce :

- En cas d'erreur de mot de passe, le système de protection va être activé.
- Pour visualiser la politique définie sur le GCap, utiliser la commande `show bruteforce-protection`.
  Après un certain nombre d'échecs, le compte sera verrouillé.
- Pour le déverrouiller : soit attendre, soit utiliser la commande `system unlock` à utiliser avec un compte de niveau de privilège supérieur.

5.5.4 Connexion à distance à l'iDRAC en HTTP (serveur DELL)

5.5.4.1 Introduction

Cette procédure décrit la connexion distante depuis un PC distant en utilisant :

- la connexion réseau connectée sur le port iDRAC du GCap
- un navigateur WEB

Cette connexion n'est pas la façon normale d'accéder au GCap mais permet d'accéder au GCap en cas de problèmes.
Pour effectuer cette procédure , il est nécessaire :

- que l'iDRAC possède une IP accessible afin de pouvoir s'y connecter
- de connaître les nom et mot de passe d'accès à l'iDRAC

Depuis la page Web de l'iDRAC, il est possible de :

- visualiser les ressources matériels et leur état et les configurations BIOS
- interagir avec le serveur pour l'allumer, l'éteindre ou le redémarrer
- se connecter en console CLI au GCap

Astuce :

- En cas d'erreur de mot de passe, le système de protection va être activé.
- Pour visualiser la politique définie sur le GCap, utiliser la commande `show bruteforce-protection`.
  Après un certain nombre d'échecs, le compte sera verrouillé.
- Pour le déverrouiller : soit attendre, soit utiliser la commande `system unlock` à utiliser avec un compte de niveau de privilège supérieur.

5.5.4.2 Opérations préliminaires

- Effectuer la configuration réseau (adresse IP de l'iDRAC) : si ce n'est pas le cas, utiliser la *Procédure de connexion directe au GCap* pour se connecter au GCap.

5.5.4.3 Procédure

- Sur le PC distant, ouvrir un navigateur internet.
- Entrer l'adresse IP de l'interface iDRAC du GCap puis valider.
  La fenêtre `Login` est affichée.
- Entrer les paramètres demandés :
  - `Username` : identifiant
  - `Password` : mot de passe de l'identifiant saisi
  - `Domain` : sélectionner `This IDRA`
- Cliquer sur le bouton `Submit`.
- Lancer la console virtuelle (zone `Virtual console Preview`, bouton `Launch`).
  A la suite de cette action, une nouvelle page s'ouvre et il sera possible d'interagir avec le GCap.
- Se connecter à la CLI (commande `gcap-cli`).
  Après connexion, le message suivant est affiché :

```
(gcap-cli)
```

Note :

- Appuyer sur **Tab** pour afficher toutes les commandes disponibles.
- Appuyer sur **Entrée** pour afficher toutes les commandes disponibles et une courte explication.

5.5.4.4 Cas particuliers

Il est possible d'ouvrir une connexion SSH, d'exécuter une ligne de commande de la CLI puis de fermer cette connexion.
Pour cela :

- entrer la commande

```
~$ ssh -t setup@x.x.xx.x show status
```

- valider
  Le système :
  - ouvre la connexion SSH
  - exécute la commande (ici `show status`) puis
  - referme la connexion SSH

```
GCAP Name         :
Version           : z.z.z
Paired on GCenter : Not paired
Tunnel status     : Down
Detection Engine  : Up and running
© Copyright GATEWATCHER 202
Connection to x.x.x.x closed.
```

5.5.5 Connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série

5.5.5.1 Introduction

Cette procédure décrit la connexion distante depuis un PC distant en utilisant :

- la connexion réseau connectée sur le port iDRAC du GCap
- un outil de connexion via SSH

Cette connexion n'est pas la façon normale d'accéder au GCap mais permet d'accéder au GCap en cas de problèmes.
Pour effectuer cette procédure , il est nécessaire :

- que l'iDRAC possède une IP accessible afin de pouvoir s'y connecter
- de connaître les nom et mot de passe d'accès à l'iDRAC

Depuis l'interface, il est possible de :

- visualiser les messages du système d'exploitation
- se connecter en console CLI au GCap

Astuce :

- En cas d'erreur de mot de passe, le système de protection va être activé.
- Pour visualiser la politique définie sur le GCap, utiliser la commande `show bruteforce-protection`.
  Après un certain nombre d'échecs, le compte sera verrouillé.
- Pour le déverrouiller : soit attendre, soit utiliser la commande `system unlock` à utiliser avec un compte de niveau de privilège supérieur.

5.5.5.2 Opérations préliminaires

- Effectuer la configuration réseau (adresse IP de l'iDRAC).
  Si ce n'est pas le cas, utiliser la *Procédure de connexion directe au GCap* pour se connecter au GCap.

5.5.5.3 Procédure

- Sur le PC distant sous Linux :
  - ouvrir une invite de commande
  - entrer la commande `ssh identifiant@adresse_ip`
    Par exemple, `ssh setup@x.x.x.x` où
    - `setup` est l'identifiant et
    - x.x.x.x est l'adresse IP du port iDRAC du GCap.
  - valider la commande
  - entrer le mot de passe de l'identifiant saisi
  - appuyer sur **Enter** pour afficher toutes les commandes disponibles et une courte explication
- Sur un PC sous Windows :

- ouvrir un logiciel client SSH, type Putty
- entrer l'adresse IP de l'interface iDRAC du GCap puis valider

- Entrer la commande suivante `racadm>>console com2`.
- Valider.
  Le système affiche désormais l'interface graphique de l'appliance.
  A la suite de cette action, une nouvelle page s'ouvre et il sera possible d'interagir avec le GCap.
- Se connecter à la CLI (commande gcap-cli). Après connexion, le message suivant est affiché :

```
(gcap-cli)
```

Note :

- Appuyer sur **Tab** pour afficher toutes les commandes disponibles.
- Appuyer sur **Entrée** pour afficher toutes les commandes disponibles et une courte explication.

5.5.5.4 Cas particuliers

Il est possible d'ouvrir une connexion SSH, d'exécuter une ligne de commande de la CLI puis de fermer cette connexion.
Pour cela :

- entrer la commande

```
~$ ssh -t setup@x.x.xx.x show status
```

- valider
  Le système :
  - ouvre la connexion SSH
  - exécute la commande (ici `show status`) puis
  - referme la connexion SSH

```
GCAP Name         :
Version           : z.z.z
Paired on GCenter : Not paired
Tunnel status     : Down
Detection Engine  : Up and running
© Copyright GATEWATCHER 202
Connection to x.x.x.x closed.
```

5.5.6 Connexion à distance au GCap via un tunnel SSH

5.5.6.1 Introduction

Cette procédure décrit la connexion depuis un PC distant de façon sécurisée en utilisant un tunnel SSH.

Astuce :

- En cas d'erreur de mot de passe, le système de protection va être activé.
- Pour visualiser la politique définie sur le GCap, utiliser la commande `show bruteforce-protection`.
  Après un certain nombre d'échecs, le compte sera verrouillé.
- Pour le déverrouiller : soit attendre, soit utiliser la commande `system unlock` à utiliser avec un compte de niveau de privilège supérieur.

5.5.6.2 Opérations préliminaires

- Effectuer une première connexion sur le GCap (voir *Procédure de connexion directe au GCap*).
- Connaître le nom du GCap ou son adresse IP (*voir Procédure de visualisation des paramètres des interfaces `Tunnel` et `Management`*).

5.5.6.3 Procédure

- Sur le PC distant sous Linux :
  - ouvrir une invite de commande
  - entrer la commande `ssh identifiant@adresse_ip_GCap` ou `ssh identifiant@FQDN_GCap`
    Par exemple, `ssh setup@gcap` où :
    - l'identifiant est `setup` et
    - le FQDN est `gcap`.
  - valider la commande
  - entrer le mot de passe de l'identifiant saisi
- Sur un PC sous Windows :
  - ouvrir un logiciel client SSH, type Putty
  - entrer l'adresse IP de l'interface GCap puis valider

L'invite de commande est affichée.
`[Monitoring DOWN] GCap name (gcap-cli)`

Note :

- Appuyer sur **Tab** pour afficher toutes les commandes disponibles.
- Appuyer sur **Entrée** pour afficher toutes les commandes disponibles et une courte explication.

5.5.7 Connexion au GCenter via un navigateur web

5.5.7.1 Introduction

Cette procédure décrit la connexion depuis un PC distant au GCenter via un navigateur web.

5.5.7.2 Opérations préliminaires

- Connaître le nom du GCenter ou son adresse IP.
- Se connecter sur un PC connecté sur le réseau du GCap et du GCenter.

5.5.7.3 Procédure

Sur le PC distant :

- Ouvrir un navigateur web.
- Entrer l'URL suivant :
  - `ssh identifiant@adresse_ip`
  - ou `ssh identifiant@FQDN`

  Par exemple : `ssh setup@gcenter.domain.com` avec :
  - *l'identifiant est `setup`*
  - *le FQDN est `gcenter.domain.com`*
- Valider.
  La fenêtre de connexion du GCenter est affichée.
  - Entrer l'identifiant.
  - Entrer le mot de passe.
  - Valider.

L'interface graphique du GCenter est affichée.

Note :

Se référer à la documentation du GCenter pour l'utiliser.

5.5.8 Modification de la date et heure du GCap

5.5.8.1 Introduction

Avant appairage entre GCap et GCenter, il est nécessaire de s'assurer que les deux systèmes soient à la même heure.
Une fois l'appairage fonctionnel, le GCenter fait office de serveur NTP pour le GCap afin que les horloges des équipements soient synchronisés.
Lors de votre première connexion, ces éléments doivent être définis via la commande *datetime* de la CLI.
L'ajustement est nécessaire pour l'établissement du tunnel IPSec.
Il faut que les heures du GCap et du GCenter soient les mêmes à 1 minute près.

Important :

En cas d'écart, c'est l'heure du GCap qu'il faut changer.

5.5.8.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show datetime*
  - *set datetime*

5.5.8.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
- Se connecter en tant que **setup**.

5.5.8.4 Procédure pour visualiser la date et heure sur le GCap et sur le GCenter

- Entrer la commande `show datetime` puis valider.
  La commande `datetime` du sous-groupe `show` permet d'afficher la date et l'heure du GCap au format YYYY-MM-DD HH :MM :SS.

```
(gcap-cli) show datetime
Current datetime is 2022-01-26 16:10:44
```

- Se connecter au GCenter.
- Afficher la date et heure du GCenter et les noter.
  En cas d'écart entre le GCap et le GCenter, c'est l'heure du GCap qu'il faut changer.
- Pour ce faire, appliquer la procédure suivante.

5.5.8.5 Procédure pour modifier les date et heure du GCap

- Entrer la commande *set datetime* suivi des paramètres dans l'ordre suivant {YYYY-MM-DDThh :mm :ssZ}.
  Exemple : set datetime 2022-01-26T16 :00 :00Z
  - YYYY indique une année à quatre chiffres de 0000 à 9999.
  - MM indique un mois à deux chiffres de 01 à 12.
  - DD indique un jour à deux chiffres du mois 01 au 31.
  - T indique le début du champ définissant le format de l'heure
  - hh indique l'heure à deux chiffres de 00 à 23.
  - mm indique les minutes à deux chiffres de 00 à 59.
  - ss indique les secondes à deux chiffres de 00 à 59.
  - Z indique l'heure UTC (Coordinated Universal Time)

```
(gcap-cli) set datetime 2022-01-26T16:00:00Z
```

- Valider.
  Le système affiche une fenêtre de confirmation.

```
Date successfully changed to Wed Jan 26 2022 16:00:00
```

5.5.9 Gestion des paramètres réseau des interfaces `Tunnel` et `Management`

5.5.9.1 Introduction

Cette procédure décrit :

- la visualisation des paramètres réseau et
- la modification de ces paramètres.

Pour...	utiliser la commande	décrite dans la procédure
avoir une vue générale des informations sur toutes les interfaces réseau	*show network-config configuration*	Procédure A
afficher pour chaque interface : l'adresse MAC, la présence de la porteuse (carrier) la vitesse et le type de connexion	*show network-config status*	Procédure B
afficher ou modifier le nom du domaine	*show network-config domain* ou *set network-config domain*	Procédure C
afficher ou modifier le nom du système	*show network-config hostname* ou *set network-config hostname*	Procédure D
afficher ou modifier l'interface utilisée en SSH pour l'administration du GCap et le lien GCap GCenter	*show network-config ssh* ou *set network-config ssh*	Procédure E
afficher ou modifier la valeur MTU des interfaces	*show advanced-configuration mtu* ou *set advanced-configuration mtu*	Procédure F
afficher ou modifier les paramètres TCP/IP des interfaces Management / Tunnel	*show network-config gcp0*	Procédure G

5.5.9.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
- *show network-config configuration*
- *show interfaces*
- *show network-config domain*
- *set network-config domain*
- *show network-config hostname*
- *set network-config hostname*
- *show network-config ssh*
- *set interfaces assign-role*
- *set advanced-configuration mtu*
- *show network-config management*
- *set network-config management*

5.5.9.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
- Arrêter le moteur de détection (voir *monitoring-engine*)

5.5.9.4 Procédure A : afficher la configuration réseau

- Entrer la commande `show network-config configuration` puis valider.
  Le système affiche les informations de toutes les interfaces réseau.
  Dans cette procédure, seules les informations sur les interfaces réseau management et tunnel sont détaillées.
  Pour les informations sur les interfaces de capture `monx`, se référer à la *Procédure de gestion des paramètres des interfaces de capture `monx`*.
  Le système affiche les informations suivantes :
  - nom du système (**hostname**)
  - nom du domaine (**domain_name**)
  - détails des paramètres TCP/IP de chaque interface réseau (`management` et `tunnel`)
  - activation ou non de l'interface

```
(gcap-cli) show network-config configuration

{
    "hostname": "GCap",
    "domain_name": "domain.local",
    "tunnel": {
        "ip_address": "192.168.1.1",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.254",
    },
    "management": {
        "ip_address": "192.168.2.1",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.2.254",
    },
```

Note :

La configuration dans l'exemple ci-dessus est en double-interface.

5.5.9.5 Procédure B : afficher l'état des interfaces réseau du GCap

- Entrer la commande suivante.

```
(gcap-cli) show network-config status
```

- Valider.
  Le système affiche l'état des interfaces réseau du GCap.

```
Label       Name      Role        Capture capability MTU   Physical Address   Speed   Type   Vendor ID   Device ID   PCI bus
            enp4s0    inactive    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
            enp12s0   inactive    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
```

Pour chaque interface, les informations suivantes sont affichées :

- `Label` : le nom de label de l'interface
- `Name` : le nom de système de l'interface
- `Role` : le rôle assigné à l'interface
- `Capture capability` : si l'interface peut capturer du trafic
- `MTU` : Le MTU de l'interface
- `Physical address` : l'adresse MAC de l'interface
- `Speed` : la vitesse de l'interface
- `Type` : le type de câble/sfp connecté au port physique
- `Vendor ID` : l'ID du fournisseur de la carte réseau
- `Device ID` : l'ID de la carte réseau
- `PCI bus` : Numéro du bus PCI utilisé par la carte réseau

5.5.9.6 Procédure C : afficher/ modifier le nom du domaine du GCap

- Pour afficher le nom courant :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config domain
```

  - Valider.
    Le système affiche le nom du domaine.

```
Current domain name: gatewatcher.com
```

- Pour modifier le nom courant :
  - Entrer la commande suivante

```
(gcap-cli) set network-config domain-name gatewatcher.com
```

  - Valider

```
Setting hostname/domain name to:
   - Hostname: gcap-int-129-dag
   - Domain name: gatewatcher.com
Do you want to apply this new configuration? (y/N)
```

- Appuyer sur **y** puis valider

```
Applying configuration...
Procedure completed with success
```

- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante

```
(gcap-cli) show network-config domain
```

  - Valider
    Le système affiche le nom du domaine.

```
Current domain name: gatewatcher.com
```

5.5.9.7 Procédure D : afficher ou modifier le nom du GCap

- Pour afficher le nom courant :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config hostname
```

  - Valider.
    Le système affiche l'interface le nom d'hôte du GCap.

```
Current hostname: GCap-name
```

- Pour modifier le nom courant :
  - Entrer la commande suivante.

```
(gcap-cli) set network-config hostname gcap-name
```

  - Valider.

```
 Setting hostname/domain name to:
  - Hostname: gcap-name
  - Domain name: gatewatcher.com
 Do you want to apply this new configuration? (y/N)
```

  - Appuyer sur **y** puis valider

```
Applying configuration...
Procedure completed with success
```

- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config hostname
```

  - Valider.
    Le système affiche le nom d'hôte du GCap.

```
Current hostname: GCap-name
```

5.5.9.8 Procédure E : afficher ou modifier l'interface utilisée pour gérer le GCap en SSH

- Pour afficher la configuration courante :
  - Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

  - Valider.
    Le système affiche le rôle des différentes interfaces du GCap (`management` pour une connection en SSH, `tunnel` pour un tunnel IPSec, `management-tunnel` pour les deux).
    - Dans le cas de la configuration mono-interface, le système affiche :

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
	enp4s0	inactive	Available	1500	00:50:56:91:8d:35	1Gb	RJ45	0x8086	0x10d3	04:00.0
	enp11s0	inactive	Available	1500	00:50:56:00:03:01	10Gb	RJ45	0x15ad	0x07b0	0b:00.0
	enp12s0	inactive	Available	1500	00:50:56:91:d4:30	1Gb	RJ45	0x8086	0x10d3	0c:00.0
management	enp19s0	management-tunnel	Available	1500	00:50:56:00:03:02	10Gb	RJ45	0x15ad	0x07b0	13:00.0

    - Dans le cas de la configuration double-interface, le système affiche :

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
	enp4s0	inactive	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
	enp12s0	inactive	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

- Pour configurer l'interface `enpXXXX` en SSH et l'interface `enpYYYY` pour IPSec :
  - Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enpXXXX management
```

  - Valider.
  - Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enpYYYY tunnel
```

  - Valider.
  - Entrer la commande suivante.

```
(gcap-cli) set network-config management ip-address X.X.X.X gateway X.X.X.X mask X.X.X.X
```

  - Valider.
  - Entrer la commande suivante :

```
(gcap-cli) set network-config tunnel ip-address Y.Y.Y.Y gateway Y.Y.Y.Y mask Y.Y.Y.Y confirm
```

- Valider.
- Pour configurer l'interface `enpXXXX` en SSH et IPSec :

Note :

Aucune autre interface n'est utilisée.

- Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enpXXXX management-tunnel
```

- Valider.
- Entrer la commande suivante.

```
(gcap-cli) set network-config management ip-address X.X.X.X gateway X.X.X.X mask X.X.X.X confirm
```

- Valider.

5.5.9.9 Procédure F : afficher ou modifier la valeur de la MTU

- Pour afficher la configuration courante des interfaces actives :
  - Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

  - Valider.
    Le système affiche le résultat.

```
Label       Name      Role               Capture capability MTU   Physical Address  Speed  Type   Vendor ID  Device ID  PCI bus
            enp4s0    inactive           Available          1500  00:50:56:91:8d:35 1Gb    RJ45   0x8086     0x10d3     04:00.0
            enp11s0   inactive           Available          1500  00:50:56:00:03:01 10Gb   RJ45   0x15ad     0x07b0     0b:00.0
            enp12s0   inactive           Available          1500  00:50:56:91:d4:30 1Gb    RJ45   0x8086     0x10d3     0c:00.0
management  enp19s0   management-tunnel  Available          1500  00:50:56:00:03:02 10Gb   RJ45   0x15ad     0x07b0     13:00.0
```

    Les valeurs sont affichées pour toutes les interfaces réseau actives.
- Pour modifier la configuration courante des interfaces actives : par exemple, pour modifier la valeur de la MTU de l'interface `management` :
  - Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration mtu enp19s0 2000
```

  - Valider.
    Le système affiche le résultat.

```
Updating Network MTU configuration to:
   - enp19s0: 2000
```

5.5.9.10 Procédure G : afficher ou modifier les paramètres TCP/IP d'une interface `management` et/ou d'une interface `tunnel`

- Pour afficher la configuration de l'interface **management** et de l'interface **tunnel** :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config management
```

  - Valider.

```
(gcap-cli) show network-config configuration

{
    "hostname": "GCap",
    "domain_name": "domain.local",
    "tunnel": {
        "ip_address": "192.168.1.1",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.254",
    },
    "management": {
        "ip_address": "192.168.2.1",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.2.254",
    },
```

- Pour modifier la configuration de l'adresse de l'interface **management** :
  - Entrer la commande suivante.

```
(gcap-cli) set network-config management ip-address x.x.x.x gateway y.y.y.y mask z.z.z.z
```

  - Valider.
    Le système affiche la configuration de l'interface **management**.

```
Setting interface management to configuration :
   - IP Address: X.X.X.X
   - Mask: Y.Y.Y.Y
   - Gateway: Z.Z.Z.Z
Do you want to apply this new configuration? (y/N)
```

  - Appuyer sur **y** puis valider.

5.5.10 Gestion des paramètres des interfaces de capture `monx`

5.5.10.1 Introduction

Cette procédure décrit :

- la visualisation des paramètres réseau
- la modification de ces paramètres

Pour...	utiliser la commande	décrite dans la procédure
avoir une vue générale des informations sur toutes les interfaces réseau	*show network-config configuration*	Procédure A
afficher la valeur MTU des interfaces	*show advanced-configuration mtu*	Procédure B
modifier la valeur MTU des interfaces	*set advanced-configuration mtu*	Procédure B
afficher les interfaces de détection disponibles	*show interfaces*	Procédure C
administrer les interfaces de détection disponibles	*set interfaces*	Procédure C

5.5.10.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show network-config configuration*
  - *show advanced-configuration mtu*
  - *set advanced-configuration mtu*
  - *show interfaces*
  - *set interfaces*

5.5.10.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
- Arrêter le moteur de détection (voir *monitoring-engine*).

5.5.10.4 Procédure A : afficher la configuration réseau

- Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

- Valider.
  Le système affiche les informations de toutes les interfaces réseau.

```
(gcap-cli) 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
```

Note :

Les interfaces `mon0`, `mon1`, `mon2` sont actives (champ : **role**, valeur : **capture**). L'interface `enp27s0`` est inactive (champ : **role**, valeur : **inactive**).

5.5.10.5 Procédure B : afficher / modifier la valeur de la MTU

- Pour afficher la configuration courante des interfaces actives :
  - Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

  - Valider.
    Le système affiche le résultat.

```
(gcap-cli) 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 valeurs sont affichées pour toutes les interfaces réseau actives (champ *MTU*)
```

- Dans notre exemple, pour modifier la configuration courante des interfaces actives : par exemple pour modifier la valeur de la MTU de l'interface `mon0`
  - Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration mtu mon1 2000
```

  - Valider.
    Le système affiche le résultat.

```
Updating Network MTU configuration to:
        - enp4s0: 2000
```

5.5.10.6 Procédure C : afficher ou modifier les interfaces de détection disponibles

- Pour afficher les informations sur les interfaces de détection :
  - Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

  - Valider.
    Le système affiche les interfaces de détection disponibles.

```
(gcap-cli) 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 informations affichées sont :
```

- `Label` : le nom de label de l'interface
- `Name` : le nom de système de l'interface
- `Role` : le rôle attribué à l'interface
- `Capture capability` : si l'interface peut capturer du trafic
- `MTU` : le MTU de l'interface
- `Physical Address` : l'adresse MAC de l'interface
- `Speed` : la vitesse de l'interface
- `Type` : le type de câble/sfp connecté au port physique
- `Vendor ID` : l'identifiant du fournisseur de la carte réseau
- `Device ID` : l'identifiant de la carte réseau
- `PCI bus` : le numéro de bus PCI utilisé par la carte réseau
- Dans notre exemple, mon0, mon1 et mon2 sont actifs (champ : **role**, valeur : **capture**).
- Pour activer une interface (ici enp27s0 par exemple) :
  - Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enp27s0 capture
```

  - Valider.
  - Ensuite, pour vérifier la nouvelle configuration

```
(gcap-cli) show interfaces
```

    - Valider.
      Le système affiche les interfaces de détection disponibles.

```
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
mon4        enp27s0   capture     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
```

- Pour désactiver une interface (ici mon0 par exemple) :
  - Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enp27s0 inactive
```

  - Valider.
- Pour modifier le délai de démarrage des interfaces (ici 5s par exemple)
  - Entrer la commande suivante.

```
(gcap-cli) set interfaces delay 5
```

  - Valider.

5.5.11 Basculement vers la configuration simple-interface

5.5.11.1 Introduction

En configuration mono-interface, la connexion SSH pour la gestion du GCap et la communication VPN sont gérées par une interface avec le rôle `management-tunnel`.
En configuration double-interface :

- la communication VPN est gérée par une interface avec le rôle `tunnel`
- la connexion SSH pour la gestion du GCap est gérée par une interfae avec le rôle `management`

Cette procédure décrit le basculement de la configuration double-interface vers la configuration mono-interface.

L'utilisateur va perdre la session si la connexion entre le GCap et le PC de l'utilisateur est effectuée à distance en SSH.
Afin d'éviter cette déconnexion, se connecter au GCap :

- soit par une connexion directe (se connecter directement au serveur)
- soit par une connexion à distance HTTP (fonction iDRAC pour un serveur Dell)
- soit par une connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série

---

5.5.11.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show interfaces*
  - *show network-config*
  - *set network-config*
  - *set interfaces assign-role*
  - *unpair*

5.5.11.3 Opérations préliminaires

- Suivant le cas, se référer à :
  - la *Procédure de connexion directe au GCap*.
  - la *Procédure de connexion à distance en HTTP à l'iDRAC*.
  - la *Procédure de connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série*.
- Arrêter le moteur de détection (voir *monitoring-engine*)

5.5.11.4 Procédure pour afficher la configuration courante

- Pour afficher la configuration des interfaces `management` et `tunnel` :
  - Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

  - Valider.
    Le système affiche la configuration des interfaces `management` et `tunnel`.
    - **Configuration mono-interface**
      Les connexions SSH et VPN sont gérées par l'interface `enp19s0`.
      Dans ce cas, le système affiche :

```
Label       Name      Role               Capture capability MTU   Physical Address  Speed  Type  Vendor ID  Device ID  PCI bus
            enp4s0    inactive           Available          1500  00:50:56:91:8d:35 1Gb    RJ45  0x8086     0x10d3     04:00.0
            enp11s0   inactive           Available          1500  00:50:56:00:03:01 10Gb   RJ45  0x15ad     0x07b0     0b:00.0
            enp12s0   inactive           Available          1500  00:50:56:91:d4:30 1Gb    RJ45  0x8086     0x10d3     0c:00.0
management  enp19s0   management-tunnel  Available          1500  00:50:56:00:03:02 10Gb   RJ45  0x15ad     0x07b0     13:00.0
```

      Dans notre exemple, la configuration courante est mono-interface (champ : role, valeur : management-tunnel)
      Dans ce cas, il n'y a rien à faire.
    - **Configuration double-interface**
      La communication VPN est gérée par l'interface `enp11s0`.
      La connexion SSH pour la gestion du GCap est gérée par l'interface `enp19s0`.
      Dans ce cas, le système affiche :

```
Label       Name      Role        Capture capability MTU   Physical Address  Speed  Type  Vendor ID  Device ID  PCI bus
            enp4s0    inactive    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
            enp12s0   inactive    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
```

      Le rôle tunnel et le rôle management indiquent que la configuration courante est double-interface.

- Dans ce cas, il faut continuer cette procédure.

5.5.11.5 Procédure pour basculer de la configuration double-interface en mono-interface

- Premièrement, entrer la commande suivante pour désapparier le GCap :

```
(gcap-cli) unpair
```

- Si vous souhaitez utiliser la même configuration IP que l'interface avec le rôle `management` :
  - Entrer la commande suivante pour désactiver la configuration de l'interface `tunnel` courante :

```
(gcap-cli) set interfaces assign-role enp11s0 inactive
```

- Valider.
  Entrer ensuite la commande suivante pour attribuer le rôle `management-tunnel` à l'interface `management` courante :

```
(gcap-cli) set interfaces assign-role enp19s0 management-tunnel
```

- Valider.
- Si vous souhaitez utiliser une autre configuration IP que celle de l'interface avec le rôle `management` :
  - Entrer la commande suivante pour reconfigurer l'interface management :

```
(gcap-cli) set network-config management ip-address X.X.X.X gateway X.X.X.X mask X.X.X.X
```

  - Valider.
  - Entrer la commande suivante pour désactiver la configuration de l'interface `tunnel` courante :

```
(gcap-cli) set interfaces assign-role enp11s0 inactive
```

  - Valider.
    Entrer ensuite la commande suivante pour attribuer le rôle `management-tunnel` à l'interface `management` courante :

```
(gcap-cli) set interfaces assign-role enp19s0 management-tunnel
```

  - Valider.

Note :

Si vous souhaitez appliquer la configuration IP de l'interface tunnel actuelle à l'interface management actuelle, vous devez configurer l'interface tunnel actuelle avec une autre configuration réseau avant de configurer l'interface management.

- Rebrancher les câbles réseau du GCap si nécessaire.

Note :

Il est nécessaire d'ajouter l'attribut de commande 'confirm' à la fin de la commande (set network-config management) si l'appairage avec le GCenter est actif.

5.5.12 Basculement vers la configuration double-interface

5.5.12.1 Introduction

En configuration simple-interface, la connexion SSH pour la gestion du GCap et la communication VPN sont gérées par une interface avec le rôle `management-tunnel`.
En configuration double-interface :

- la communication VPN est gérée par une interface avec le rôle `tunnel`
- la connexion SSH pour la gestion du GCap est gérée par une interface avec le rôle `management`

Cette procédure décrit le basculement de la configuration simple-interface vers la configuration double-interface.

Important :

L'utilisateur va perdre la session si la connexion entre le GCap et le PC de l'utilisateur est effectuée à distance en SSH.
Afin d'éviter cette déconnexion, se connecter au GCap :

- soit par une connexion directe (se connecter directement devant le serveur)
- soit par une connexion à distance HTTP (fonction iDRAC pour un serveur Dell)
- soit par une connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série

---

5.5.12.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show interfaces*
  - *show network-config*
  - *set network-config*
  - *set interfaces assign-role*
  - *unpair*

5.5.12.3 Opérations préliminaires

- Suivant le cas, se référer à :
  - la *Procédure de connexion directe au GCap*.
  - la *Procédure de connexion à distance en HTTP à l'iDRAC*.
  - la *Procédure de connexion à distance à la CLI en SSH via l'interface iDRAC en mode redirection du port série*.
- Arrêter le moteur de détection (voir *monitoring-engine*)

5.5.12.4 Procédure pour afficher la configuration courante

- Pour afficher la configuration des interfaces `management` et `tunnel` :
- Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

- Valider.
  Le système affiche la configuration des interfaces `management` et `tunnel`.
- **Configuration double-interface**
  La communication VPN est gérée par l'interface `enp11s0`.
  La connexion SSH pour la gestion du GCap est gérée par l'interface `enp19s0`.
  Dans ce cas, le système affiche :

```
Label       Name     Role        Capture capability MTU   Physical Address   Speed   Type   Vendor ID   Device ID   PCI bus
            enp4s0   inactive    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
            enp12s0  inactive    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
```

Les rôles tunnel et management indiquent que la configuration courante est en double-interface
Dans ce cas, il n'y a rien à faire.

- **Configuration simple-interface**
  Les connexions SSH et VPN sont gérées par l'interface `enp19s0`.
  Dans ce cas, le système affiche :

```
Label       Name     Role             Capture capability MTU   Physical Address   Speed   Type   Vendor ID   Device ID   PCI bus
            enp4s0   inactive         Available          1500  00:50:56:91:8d:35  1Gb     RJ45   0x8086      0x10d3      04:00.0
            enp11s0  inactive         Available          1500  00:50:56:00:03:01  10Gb    RJ45   0x15ad      0x07b0      0b:00.0
            enp12s0  inactive         Available          1500  00:50:56:91:d4:30  1Gb     RJ45   0x8086      0x10d3      0c:00.0
management  enp19s0  management-tunnel  Available          1500  00:50:56:00:03:02  10Gb    RJ45   0x15ad      0x07b0      13:00.0
```

Dans cet exemple, la configuration courante est simple-interface (champ : rôle, valeur : management-tunnel)
Dans ce cas, il faut continuer avec la procédure suivante.

5.5.12.5 Procédure pour basculer de la configuration simple-interface en double-interface

- Entrer la commande suivante pour désapparier le GCap :

```
(gcap-cli) unpair
```

- Entrer la commande suivante pour configurer l'interface `management-tunnel` avec le rôle `management` :

```
(gcap-cli) set interfaces assign-role enp19s0 management
```

- Valider.
- Entrer la commande suivante pour configurer l'interface sélectionnée avec le rôle `tunnel` :

```
(gcap-cli) set interfaces assign-role enp11s0 tunnel
```

- Valider.

- Entrer la commande suivante la configuration de l'IP de l'interface tunnel :

```
(gcap-cli) set network-config tunnel ip-address Y.Y.Y.Y gateway Y.Y.Y.Y mask Y.Y.Y.Y confirm
```

- Valider.
- Rebrancher les câbles réseau du GCap si nécessaire.

5.5.13 Gestion de l'agrégation d'interfaces de capture

5.5.13.1 Introduction

Cette procédure décrit l'agrégation d'interfaces de capture.
Pour plus d'informations sur l'agrégation, se référer au paragraphe *Interfaces de capture et de surveillance monx entre TAP et GCap : possibilité d'agrégation*.
La fonctionnalité de mise en agrégation des interfaces de capture sur le GCap a pour conséquence d'impacter certaines fonctions associées :

- la MTU (Maximum Transmission Unit) : la taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation).
  MTU : prend la valeur la plus grande des interfaces qui composent l'agrégation.
- les règles statiques de filtrage des flux capturés par interface de capture : fonction Filtre XDP (eXpress Data Path).
  Le filtrage XDP ne s'applique pas par défaut sur l'agrégation créée mais sur les interfaces qui le composent.
  Il doit donc être appliqué individuellement sur chaque interface agrégée.
- les règles de reconstitution des fichiers.
  Règle de reconstruction : lors de l'activation de l'agrégation des interfaces et de la détection par multi-tenant, les règles de reconstruction des fichiers ne sont pas générées.

Pour créer une agrégation d'interfaces, utiliser la commande *set clusters add interfaces mon0 mon1*.

5.5.13.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show interfaces*
  - *set interfaces assign-role*

5.5.13.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
- Arrêter le moteur de détection (voir *monitoring-engine*)

5.5.13.4 Procédure pour afficher l'agrégation d'interfaces de capture

- Entrer la commande `show interfaces` puis valider.
  Le système affiche les informations de toutes les interfaces réseau.

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
	enp4s0	inactive	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
	enp12s0	inactive	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
mon0	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

  Un rôle spécifique est disponible pour le cluster : `capture-cluster`.
  Dans notre exemple, on ne voit pas ce rôle, il n'y a donc pas de cluster.

5.5.13.5 Procédure pour créer une agrégation d'interfaces

- Dans notre cas, nous allons créer un cluster avec `enp4s0` et `enp12s0`.
- Entrer la commande suivante.

```
(gcap-cli) set interfaces assign-role enp4s0 capture-cluster
(gcap-cli) set interfaces assign-role enp12s0 capture-cluster
```

- Valider.

5.5.13.6 Procédure pour afficher l'état de l'agrégation créée

- Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

- Valider.
  Le système affiche l'agrégation créée.

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
cluster0	enp4s0	capture-cluster	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
cluster0	enp12s0	capture-cluster	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
mon0	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

- Dans cet exemple, `enp4s0` et `enp27s0` sont désormais regroupés avec le rôle `capture-cluster` dans `cluster0`.

5.5.14 Appairage entre un GCap et un GCenter

5.5.14.1 Introduction

Cette procédure décrit l'appairage entre un GCap et un GCenter.
Les opérations suivantes doivent être réalisées :

- sur le GCenter, obtenir l'adresse IP du GCenter
- sur le GCap, saisir l'adresse IP du GCenter
- sur le GCenter, déclarer le GCap et générer l'OTP (One Time Password)
- sur le GCap, appairer le GCap et le GCenter

5.5.14.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show compatibility-mode*
  - *set compatibility-mode*
  - *show gcenter-ip*
  - *set gcenter-ip*
  - *show status*
  - *pairing otp*
  - *unpair*

5.5.14.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*.
- Connaître le FQDN du GCap et son adresse IP.
- Connaître le FQDN du GCenter et son adresse IP.
- Vérifier la concordance de la date et heure du GCenter et du GCap : se référer à la *Procédure de modification de la date et heure du GCap*.

5.5.14.4 Procédure pour afficher l'adresse IP du GCenter

- Se connecter au GCenter et afficher les paramètres réseau du GCenter.
  Pour plus d'informations, se référer à la documentation du GCenter.

5.5.14.5 Procédure pour définir le mode de compatibilité sur le GCap

- Pour afficher la version du logiciel du GCenter :
  - Se connecter au GCenter et regarder le numéro de version du GCenter.
    L'information est localisée en bas et gauche de la page du GCenter (GCenter v2.5.3.101-7173-HF3).
- Pour afficher le mode de compatibilité courant entre le GCap et le GCenter :
  - se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*)
  - entrer la commande suivante.

```
(gcap-cli) show compatibility-mode
```

  - valider.
    Le système affiche le mode de compatibilité courant.

```
Current compatibility mode: 2.5.3.101
```

  - Comparer la version entre celle affichée sur le GCap et celle du GCenter.
    Dans ce cas :
    - sur le GCenter, la version est : v2.5.3.101
    - sur le GCap, le mode est : 2.5.3.101

    Donc le Gcap est bien configuré.
    Dans cet exemple, il n'est donc pas nécessaire de modifier le mode de compatibilité.
    Mais s'il est nécessaire de modifier le mode, appliquer la procédure suivante.
- Pour modifier le mode de compatibilité du GCap :
  - entrer la commande suivante (par exemple pour la version 2.5.3.102)

```
(gcap-cli) set compatibility-mode 2.5.3.102
```

  - valider.

5.5.14.6 Procédure pour définir l'IP du GCenter sur le GCap

- Pour afficher la version courante de l'IP du GCenter :
  - se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
  - entrer la commande suivante

```
(gcap-cli) show gcenter-ip
```

  - valider.
    Le système affiche l'adresse IP du GCenter courant : à vérifier que c'est bien celle de l'IP du GCenter à appairer.

```
Current GCenter IP: X.X.X.X
```

  S'il n'y a pas de GCenter appairé alors le message suivant est affiché :

```
Current GCenter IP: None
```

  - Vérifier que l'adresse IP affichée est bien celle du GCenter à appairer. En cas de modification, continuer cette procédure.
- Pour modifier la version courante de l'IP du GCenter :
  - entrer la commande *set gcenter-ip* suivie du paramètre IP du GCenter
    Exemple : set gcenter-ip 10.2.10.234
  - valider. Le système affiche la nouvelle adresse IP du GCenter.

```
Setting GCenter IP to 10.2.19.218
```

5.5.14.7 Procédure pour déclarer le GCap dans le GCenter

- Récupérer le FQDN (hostname.domain) du GCap via la commande `show status`.
- Se connecter au GCenter via un navigateur web.
- Saisir le FQDN (se référer à la documentation du GCenter).
- Appuyer sur le bouton `Start Pairing`.
  L'OTP (One Time Password) est affiché en haut et à gauche de la page web.
  Par exemple : pcmqsnf7iyo34ianzzi7gbgrr
- Copier l'OTP.

5.5.14.8 Procédure pour appairer le GCap et le GCenter

- Se connecter sur la CLI du GCap.
- Entrer la commande suivante.

```
(gcap-cli) pairing otp
```

- Coller l'OTP précédemment généré par le GCenter après avoir positionné le curseur après le texte.

```
(gcap-cli) pairing otp pcmqsnf7iyo34ianzzi7gbgrr
```

- Valider.
  Le GCap se connecte au GCenter via l'adresse IP du GCenter définie plus tôt sur le GCap.
  Puis le GCap calcule le fingerprint à l'aide du FQDN du GCap.
  Il demande à l'utilisateur de le comparer à celui calculé par le GCenter, lui même calculé à l'aide du FQDN saisi.
  Le système affiche le message suivant :

```
Resetting any previous GCenter pairing...
Generating IPSec certificates for the GCenter pairing...
Probing for GCenter SSH fingerprint...

Fingerprint for GCenter x is
e655bc02553e2291a486a32bdce3943a315f830de70b2c627c39884e80
0f08b2. Is it correct? (y/N)
```

- Comparer le fingerprint du GCenter récupéré par le GCap dans la CLI avec celui présent dans la partie `GCaps pairing..` sous le texte `GcenterSSH fingerprint` dans l'interface web GCenter sur le navigateur web.
  - Si les fingerprints ne sont pas identiques :
    - vérifier l'adresse IP du GCenter et la valeur saisie dans le GCap
    - vérifier le FQDN du GCap et le nom saisi dans le GCenter
  - S'ils sont identiques, répondre **Y** puis valider.

```
Sending OTP to GCenter...
Operation successful
```

- Sur la Web UI du GCenter, vérifier que le GCap est à présent Online dans la page du menu `GCaps pairing and status`.
  Pour plus d'information se référer à la documentation du GCenter.
  Sur le GCap, cette information est visible avec la commande `show status`.

```
(gcap-cli) show status

 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
 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 2024
```

Le champ `Paired on GCenter` prend la valeur `Yes`ou `No`

5.5.14.9 Procédure pour supprimer l'appairage entre le GCap et le GCenter

- Se connecter sur la CLI du GCap.
- Entrer la commande suivante.

```
(gcap-cli) unpair
```

- Valider.

5.5.15 Gestion de la haute disponibilité de GCaps

Note :

Cette fonctionnalité est obsolète
Veuillez contacter Gatewatcher si vous souhaitez déployer une architecture redondante.

5.5.16 Optimiser les performances

5.5.16.1 Introduction

L'optimisation des performances peut être faite suivant les possibilités suivantes :

- **sujet 1 : adaptation du GCap aux caractéristiques du réseau**
  - incohérence entre la MTU définie sur le GCap et celle des trames capturées.
    Pour modifier la MTU, voir la Procédure pour ajuster la taille du paquet capturé.
  - vérification de la bonne adéquation entre les caractéristiques du GCap (débit max, nombre de sessions, etc.) et celui du réseau à surveiller.
    Pour cela, consulter les datasheets du GCap.
- **sujet 2 : optimisation des ressources du GCap**
  - le nombre de CPU dédié au moteur de détection est trop faible.
    Les CPUs peuvent être surchargés et potentiellement des paquets sont non analysés et donc perdus (droppés).
  - préférer utiliser un TAP agrégateur par opposition à la fonction agrégation ("cluster") du GCap.
    La solution avec un TAP agrégateur est préférable car c'est celle qui nécessite le moins de ressources du GCap à flux identique.
- **sujet 3 : optimisation du flux réseau à analyser**
  - un ou des CPU sont surchargés car il y a trop de paquets analysés.
    - Pour diminuer la taille du réseau capturé, il est possible de supprimer le flux analysé inutilement.
    - Pour gérer ce filtrage de paquets, voir la procédure de définition des règles de filtrage du flux.
  - un CPU uniquement est surchargé. Dans ce cas, il y a mauvaise répartition de la charge du flux entre les CPU.
    - Pour changer cela, il est possible de définir une règle ou plus certainement modifier une règle existante.
      Il a été défini un flux mais de façon trop large, il faut donc le subdiviser pour que chaque partie soit analysée par plusieurs CPU.
    - Pour modifier les règles, voir la procédure de définition des règles statiques de filtrage des paquets.
  - modifier les protocoles analysés.
    - Pour modifier cette liste, il est nécessaire d'effectuer cette action sur le GCenter appairé.
      Se référer à la documentation du GCenter.
- **sujet 4 : optimisation des règles du moteur de détection**
  Les règles définissent :
  - les règles de détection
  - les règles de reconstruction de fichiers
  - les règles définissant les seuils ou les limites dans la rubrique threshold

  Voir la documentation du GCenter pour plus d'informations.
- **sujet 5 : supervision de la solution**
  Un service de supervision nommé Netdata, embarqué dans le GCenter, permet de relever des informations en temps réel sur l'état des CPU, la charge, les disques, les moteurs de détection ou encore le filtrage.
  Cette fonctionnalité est disponible depuis l'adresse suivante : https ://Nom_du_GCenter/gstats.
  Sur le GCap, Netdata permet d'avoir plus d'information sur les compteurs par protocole, le nombre de sessions, le flux ou encore l'état des tables de hachage depuis 'Stats.log'.

5.5.16.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show interfaces*
  - *set advanced-configuration mtu*
  - *show advanced-configuration packet-filtering*

5.5.16.3 Opérations préliminaires

- Se connecter sur le GCap (voir *Procédure de connexion sur le GCap via SSH*).
- Arrêter le moteur de détection (voir *monitoring-engine*)

5.5.16.4 Procédure pour ajuster la taille du paquet capturé

Ce réglage permet d'ajuster la taille du paquet capturé pour le mettre conforme à la taille des paquets circulant sur le réseau.

Danger :

La fonctionnalité de Filtrage XDP n'est pas supportée lorsque la MTU > 3000.

- Utiliser la commande *show interfaces* pour afficher la valeur en octets de la MTU de toutes les interfaces réseau activées
- Utiliser la commande *set advanced-configuration mtu* pour modifier le nombre de CPU dédié.

5.5.16.5 Procédure de définition des règles de filtrage du flux

Astuce :

Le(s) CPU présent(s) est surchargé et une partie du flux ne peut être analysée, un certain nombre de paquets sont droppés :

- pour visualiser le nombre de paquets perdus (dropped) par cœur cpu, utiliser la commande *show health*, détails des compteurs softnet - Statistiques sur les paquets reçus en fonction des cœurs de processeurs.

  Une partie du flux capturé ne peut être détectée, ni reconstruite : par exemple, les flux cryptés.

Si rien n'est fait, le système va monopoliser des ressources pour aboutir à un résultat connu par avance.
Pour éviter cela, il est possible de créer des règles pour filtrer le flux à capturer.

- Utiliser la commande *show advanced-configuration packet-filtering* pour afficher les règles statiques de filtrage des paquets.

Chapitre 6

CLI

6.1 Présentation de la CLI

6.1.1 Introduction à la CLI

La CLI (Command Line Interface) est le moyen utilisé pour administrer et configurer le GCap.
Il est donc nécessaire de saisir des commandes en mode texte à la suite de l'invite de commande.

6.1.2 Présentation de l'invite de commande

```
[Monitoring DOWN] gcap-name (gcap-cli)
```

Elle comprend :

- l'état du moteur de détection Sigflow (ici `Monitoring down`)
- le nom du GCap (ici `gcap-name`)
- l'information du niveau dans l'arborescence :
  - ici (`gcap-cli`) : signifie l'invite de commande est à la racine des commandes
  - par exemple (`gcap-cli show`) : signifie l'invite de commande est dans l'ensemble `show`

6.1.3 Commandes accessibles groupées par ensemble

Les commandes sont regroupées par ensemble (show, set...).
La liste détaillée des commandes est donnée dans la partie CLI.

L'ensemble...	sert à...
show	afficher la configuration du système
set	modifier la configuration du système
system	gérer les opérations du système

Ces ensembles sont accessibles depuis la racine.

Note :

L'ensemble des commandes de la CLI du GCap est calculé dynamiquement. La liste des commandes dépend :
- du type d'utilisateur courant
- de l'état du GCap

Ces informations sont indiquées dans la documentation.

Note :

- si une commande est saisie dans un ensemble qui n'est pas le bon ou
- si le niveau d'accès n'est pas le bon

... alors la commande n'est pas reconnue et le message `` `Command `X` is not recognized ` `` est affiché.

Note :

Le type d'utilisateur ou les éléments de contexte sont précisés lorsque cela est nécessaire.

6.1.4 Commandes accessibles directement

Les commandes ci-dessous sont accessibles directement :

Utiliser la commande...	pour...
monitoring engine	gérer le moteur de détection
pairing	appairer le GCap et le GCenter
unpair	appairer le GCap et le GCenter
help	obtenir de l'aide concernant les commandes disponibles
colour	activer ou désactiver les couleurs pour la session CLI courante
exit	revenir à la racine de la CLI ou de sortir de la CLI

6.1.5 Complétion

Pour compléter le nom d'une commande ou d'un argument, il est possible d'utiliser la complétion c'est à dire :

- commencer par saisir une commande puis
- utiliser la touche tabulation du clavier

Le système propose les valeurs possibles.
Exemple : en demandant une complétion sur la commande ci-dessous, le système affiche les valeurs de `set keymap` supportées :

```
(gcap-cli) set keymap

fr us
```

6.1.6 Navigation dans l'arborescence des commandes

6.1.6.1 Pour aller de la racine à un ensemble

Pour accéder aux commandes d'un ensemble depuis la racine, entrer le nom de l'ensemble.
Exemple :

```
(gcap-cli)
```

- Entrer la commande `show`.

```
(gcap-cli show)
```

Le prompt change pour informer que l'utilisateur que l'ensemble a changé.
Les commandes de l'ensemble `show` sont maintenant accessibles.
Les commandes sont aussi accessibles directement depuis l'invite **(gcap-cli)** en lançant la commande complète : par exemple `show interfaces` pour la commande `interfaces` de l'ensemble `show`.

6.1.6.2 Pour revenir à la racine

Pour sortir de l'ensemble courant et revenir à la **racine**, entrer la commande `exit`.
Exemple :

```
(gcap-cli show)
```

Seules les commandes de l'ensemble show sont accessibles.

- Entrer la commande `exit`.

  ```
  (gcap-cli)
  ```

  Le prompt change pour informer l'utilisateur que l'invite de commande est à la racine.
  A ce niveau, tous les ensembles de commandes sont accessibles.
  Le raccourci **CTRL** + **D** permet d'appeler la commande `exit`.

6.1.7 Lancement d'une commande

Une commande peut être lancée de deux façons différentes :

- soit avec seulement le nom de la commande mais l'invite de commande doit être au niveau de l'ensemble
- soit depuis la racine mais il faut saisir le nom de l'ensemble suivi du nom de la commande

---

6.1.7.1 Exemple de lancement depuis la racine pour la commande `show interfaces`

```
(gcap-cli)
```

- Entrer la commande `show interfaces` puis valider.

6.1.7.2 Exemple de lancement de la commande `show interfaces` depuis l'ensemble `show`

```
(gcap-cli show)
```

- Entrer la commande `interfaces` puis valider.

6.1.8 Obtenir des informations sur les commandes via l'Aide

Pour obtenir de l'aide concernant les commandes disponibles, il est possible d'utiliser la commande `?` ou `help`.
Pour obtenir de l'aide concernant une commande spécifique, il est possible :

- de la préfixer par `help` (exemple `help pairing`)
- de suffixer la commande par `?` (exemple `pairing?`)

Pour plus d'information sur l'aide, se référer au paragraphe *help*.

6.1.9 Exit

Lorsque la CLI interactive du GCap est utilisée, il faut utiliser la commande `exit` pour revenir à la racine de l'arborescence des commandes.
Pour plus d'informations sur la commande `exit`, se référer au paragraphe *exit*.

6.2 cli

6.2.1 show

6.2.1.1 alerts

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.2 bruteforce-protection

6.2.1.2.1 Introduction

La commande `bruteforce-protection` du sous-groupe `show` permet d'afficher la politique du système de protection contre les attaques par force brute.

6.2.1.2.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.2.3 Commande

```
show bruteforce-protection
```

6.2.1.2.4 Exemple pour afficher la politique courante du système de protection contre les attaques par force brute

- Entrer la commande suivante.

```
(gcap-cli) show bruteforce-protection
```

- Valider.
  Le système affiche les informations suivantes.

```
Current bruteforce protection rules:
  - Max tries: 3
  - Lock duration: 120s
```

  Les comptes utilisateurs sont automatiquement verrouillés pendant une période déterminée (paramètre `Lock duration`) après plusieurs essais infructueux (paramètre `Max tries`).

6.2.1.3 bypassed-flows

Cette commande est supprimée depuis la version 2.5.3.105.

6.2.1.4 clusters

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.5 compatibility-mode

6.2.1.5.1 Introduction

La commande `compatibility-mode` du sous-groupe `show` permet d'afficher le mode de compatibilité courant pour interagir avec le GCenter.
Le mode de compatibilité va influer sur les fonctionnalités disponibles du GCap.
Plusieurs modes de compatibilité sont disponibles :

- 2.5.3.102 : GCenter 2.5.3.102
- 2.5.3.103 : GCenter 2.5.3.103

Le mode courant doit être sélectionné en fonction de la version courante du GCap et du GCenter.
Pour plus d'informations, se référer au *tableau de compatibilité*.

Note :

Le mode de compatibilité avec un GCenter en version 2.5.3.101 et inférieur est obsolète.

6.2.1.5.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.1.5.3 Commande

`show compatibility-mode`

6.2.1.5.4 Exemple pour afficher le mode de compatibilité courant

- Entrer la commande suivante.

```
(gcap-cli) show compatibility-mode
```

- Valider.
  Le système affiche le mode de compatibilité courant.

```
Current compatibility mode: 2.5.3.102
```

6.2.1.6 config-files

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.7 datetime

6.2.1.7.1 Introduction

La commande `datetime` du sous-groupe `show` permet d'afficher la date et l'heure du GCap au format `YYYY-MM-DD HH:MM:SS`.

6.2.1.7.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.7.3 Commande

`show datetime`

6.2.1.7.4 Exemple pour afficher la date et l'heure du GCap

- Entrer la commande suivante.

```
(gcap-cli) show datetime
```

- Valider.
  Le système affiche les informations courantes.

```
Current datetime is 2022-01-26 16:10:44
```

6.2.1.8 eve-stats

6.2.1.8.1 Introduction

La commande `eve-stats` du sous-groupe `show` permet d'afficher les statistiques de Sigflow (*monitoring-engine*).

6.2.1.8.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.1.8.3 Commande

```
show eve-stats
```

6.2.1.8.4 Exemple

- Entrer la commande suivante.

```
(gcap-cli) show eve-stats
```

- Valider.
  Le système affiche les informations suivantes :
- le compteur `Alerts` - Nombre d'alertes Sigflow trouvées
- les compteurs `Files` - Fichiers extraits par Sigflow
- les compteurs `Codebreaker samples` - Fichiers analysés par Codebreaker
- les compteurs `Protocols` - Listes des protocoles vus par Sigflow
- les compteurs `Detection Engine Stats` - Statistiques de Sigflow (*monitoring-engine*)

6.2.1.8.4.1 Détail du compteur `Alerts` - Nombre d'alertes Sigflow trouvées

Exemple :

```
Alerts: 0
```

6.2.1.8.4.2 Détail des compteurs `Files` - Fichiers extraits par Sigflow

- `Observed` - Nombre de fichiers observés par Sigflow.
- `Extracted` - Nombre de fichiers extraits par Sigflow.
- `Uploaded` - Données des envois sur le GCenter.
  - `Metadata` - Nombre de métadonnées envoyées sur le GCenter.
  - `File` - Nombre de fichiers envoyés sur le GCenter.

Exemple :

```
   Files:
    Observed:           6011816
    Extracted:          0
    Uploaded:
       Metadata:        0
       File:            0
```

6.2.1.8.4.3 Détail des compteurs `Codebreaker samples` - Fichiers analysés par Codebreaker

- `Extracted` - Nombre de fichiers extraits reçus par Codebreaker.
- `Uploaded` - Données sur les fichiers reçus par Codebreaker sur le GCenter.
  - `Shellcodes` - Données sur les *shellcodes*.
    - `Plain` - *Shellcodes* détectés sans encodage.
    - `Encoded` - *Shellcodes* détectés avec encodage.
  - `Powershell` - Nombre de scripts *Powershell* malicieux détectés.

Exemple :

```
Codebreaker samples:
  Extracted:          0
  Uploaded:
      Shellcodes:
          Plain:      0
          Encoded:    0
      Powershell:     0
```

Note :

Dans la version GCenter V102, ce moteur s'appelle Codebreaker
Dans la version GCenter V103, le moteur qui détecte les shellcodes est appelé **Shellcode detect engine**
Dans la version GCenter V103, le moteur qui détecte les powershells malveillants est appelé **Malicious Powershell detect engine**.

6.2.1.8.4.4 Détail des compteurs `Protocols` - Listes des protocoles vus par Sigflow

- `<protocole>` Nombre d'événements observés par Sigflow à propos du protocole (par ex. : *HTTP*, *SMB*, etc).
  Exemple :

```
  Protocols:
    DHCP:     0
    DNP3:     0
    DNS:      0
    FTP:      0
    HTTP:     6537929
    HTTP2:    0
    IKEv2:    0
    KRB5:     0
    MQTT:     0
    NETFLOW:  0
    NFS:      0
    RDP:      0
    RFB:      0
    SIP:      0
    SMB:      0
    SMTP:     0
    SNMP:     0
    SSH:      0
    TFTP:     0
    TLS:      0
    Tunnels:  0
```

6.2.1.8.4.5 Détail des compteurs `Detection Engine Stats` - Statistiques de Sigflow (*monitoring-engine*)

- `Events` - Données sur les événements observés par Sigflow
  - `Total` - Nombre total d'événements observés
  - `Stats` - Nombre de statistiques générées
- `Capture`
  - `Received` - Nombre de paquets capturés
  - `Dropped` - Nombre de paquets ignorés
- `Rules` - Données sur les règles Sigflow
  - `Loaded` - Nombre de règles chargées et validées
  - `Invalid` - Nombre de règles qui n'ont pas pu être chargées
- `TCP`
  - `SYN` - Nombre de *SYN* observés par Sigflow.
  - `SYN/ACK` - Nombre de *SYN/ACK* observés par Sigflow.

- `Sessions` - Nombre de sessions *TCP* observées par Sigflow.
- `Flow`
  - `TCP` - Nombre de sessions *TCP* observées
  - `UDP` - Nombre de sessions *UDP* observées
  - `SCTP` - Nombre de sessions *SCTP* observées
  - `ICMPv4` - Nombre de messages *ICMPv4* observés
  - `ICMPv6` - Nombre de messages *ICMPv6* observés
  - `Timeouts` - Statistiques sur les expirations des sessions *TCP*
    - `New` - Nombre de nouvelles fenêtres *TCP*
    - `Established` - Nombre de fenêtres établies
    - `Closed` - Nombre de fenêtres fermées
    - `Bypassed` - Nombre de fenêtres ignorées

Exemple :

```
Detection Engine Stats:
  Events:
    Total:     12551855
    Stats:     2110

  Capture:
    Received:  153439718
    Dropped:   60964966

  Rules:
    Loaded:    78
    Invalid:   28

  TCP:
    SYN:       10274277
    SYN/ACK:   10274629
    Sessions:  10273062

  Flows:
    TCP:       12067611
    UDP:       0
    SCTP:      0
    ICMPv4:    0
    ICMPv6:    0

  Timeouts:
      New:          0
      Established:  0
      Closed:       0
      Bypassed:     0
```

Note :

Le compteur TCP sessions comptabilise le nombre de sessions une fois l'établissement de la connexion faite (phase three-way handshake).

Le compteur Flows TCP comptabilise le nombre de sessions commencées (y compris les sessions dont l'établissement de la connexion est en cours).

6.2.1.9 gcenter-ip

6.2.1.9.1 Introduction

La commande `gcenter-ip` du sous-groupe `show` permet d'afficher l'adresse IP du GCenter avec lequel le GCap est appairé.

6.2.1.9.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :**
  - le moteur de détection doit être à l'arrêt
  - un GCenter doit être appairé

6.2.1.9.3 Commande

```
show gcenter-ip
```

6.2.1.9.4 Exemple

- Entrer la commande suivante.

```
(gcap-cli) show gcenter-ip
```

- Valider.
  Le système affiche l'adresse IP du GCenter appairé.

```
Current GCenter IP: X.X.X.X
```

  S'il n'y a pas de GCenter appairé, le message suivant est affiché :

```
Current GCenter IP: None
```

6.2.1.10 health

6.2.1.10.1 Introduction

La commande `health` du sous-groupe `show` permet d'afficher des statistiques et des informations de santé du GCap.

6.2.1.10.2 Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances :** N/A

6.2.1.10.3 Commande

```
show health
```

6.2.1.10.4 Exemple

- Entrer la commande suivante.

```
(gcap-cli) show health
```

- Valider.
  Le système affiche les informations suivantes :
- les compteurs `block` - Statistiques sur les stockages de masse
- les compteurs `cpu_stats` - Statistiques sur le processeur
- les compteurs `disks` - Statistiques d'occupation des points de montage
- les compteurs `emergency` - Informations sur l'emergency mode du GCap
- les compteurs `gcenter` - Informations sur le GCenter appairé
- les compteurs `high_availability` - Informations sur la haute disponibilité (*HA*)
- les compteurs `interfaces` - Statistiques sur les interfaces réseaux
- les compteurs `loadavg` - Statistiques sur la charge moyenne du GCap
- les compteurs `meminfo` - Statistiques sur la mémoire vive
- les compteurs `numastat` - Statistiques sur les nœud NUMA
- les compteurs `quotas`- Informations sur les quotas

- les compteurs `sofnet` - Statistiques sur les paquets reçus en fonction des cœurs de processeurs
- les compteurs `suricata` - Informations sur Sigflow (*monitoring-engine*)
- les compteurs `systemd` - Informations du système d'initialisation du système
- les compteurs `uptime` - Temps de disponibilité
- les compteurs `virtualmemory` - Information sur l'espace d'échange (*swap*)

6.2.1.10.4.1 Détails des compteurs `block` - Statistiques sur les stockages de masse

- `sdN` - Statistiques du disque N où N est une lettre de l'alphabet
  - `read_bytes` - Octets lus depuis le démarrage
  - `written_bytes` - Octets écrits depuis le démarrage

Exemple :


```
{
 "block": {
    "sda": {
        "read_bytes": 302867968,
        "written_bytes": 4837645312
    },
    "sdb": {
        "read_bytes": 3894272,
        "written_bytes": 4096
    }
}
```

6.2.1.10.4.2 Détails des compteurs `cpu_stats` - Statistiques sur le processeur

- `cpus` - Statistiques d'utilisation des CPUs
  - `cpu` - Statistiques d'utilisation globales des cœurs
  - `cpuX` - Statistique du cœur CPU X
    - `idle` - Temps écoulé à ne rien faire en millisecondes
    - `iowait` - Temps écoulé à attendre des opérations disques en millisecondes
    - `irq` - Temps écoulé sur les IRQ matériel
    - `nice` - Temps écoulé en espace utilisateur sur des processus à priorité faible en millisecondes
    - `softirq` - Temps écoulé sur les IRQ matériel en millisecondes
    - `system` - Temps écoulé en espace noyau en millisecondes
    - `user` - Temps écoulé en espace utilisateur en millisecondes
- `interrupts` - Nombre d'interruptions depuis le démarrage
- `processes_blocked` - Nombre de processus bloqués ou *death*
- `processes_running` - Nombre de processus en cours d'exécution

Exemple :


```
"cpu_stats": {
   "cpus": {
       "cpu": {
           "idle": 961816208,
           "iowait": 11419,
           "irq": 0,
           "nice": 0,
           "softirq": 397899,
           "system": 21788203,
           "user": 50806194
       },
       "cpu0": {
           "idle": 79960857,
           "iowait": 985,
           "irq": 0,
           "nice": 0,
           "softirq": 234748,
           "system": 1795880,
           "user": 4357374
       },
       "cpu1": {
           "idle": 80166571,
           "iowait": 951,
           "irq": 0,
           "nice": 0,
           "softirq": 88078,
```


(suite sur la page suivante)

(suite de la page précédente)


```
            "system": 1830370,
            "user": 4138182
        }
    },
    "interrupts": 12942835029,
    "processes_blocked": 0,
    "processes_running": 1
}
```


6.2.1.10.4.3 Détails des compteurs `disks` - Statistiques d'occupation des points de montage

- `/mountpoint/path` - Chemin du point de montage
  - `block_free` - Nombre de *blocks* disponibles
  - `block_total` - Nombre total de *blocks*
  - `inode_free` - Nombre d'inodes restants
  - `inode_total` - Nombre totale d'*inodes*

  Exemple :


```
  "disks": {
      "/": {
          "block_free": 247909,
          "block_total": 249830,
          "inode_free": 64258,
          "inode_total": 65536
      },
      "/data": {
          "block_free": 7150076,
          "block_total": 7161801,
          "inode_free": 1827417,
          "inode_total": 1827840
      },
  }
```


6.2.1.10.4.4 Détails des compteurs `emergency` - Informations sur l'emergency mode du GCap

- `emergency_active` - État actif ou inactif de l'*emergency mode*

  Exemple :


```
  "emergency": {
      "emergency_active": false
  },
```


6.2.1.10.4.5 Détails des compteurs `gcenter` - Informations sur le GCenter appairé

- `chronyc_sync` - État de la synchronisation NTP avec le GCenter
- `reachable` - GCenter joignable ou non (false)

  Exemple :


```
  "gcenter": {
      "chronyc_sync": false,
      "reachable": false
  },
```

6.2.1.10.4.6 Détails des compteurs `high_availability` - Informations sur la haute disponibilité (*HA*)

Cette fonctionnalité est obsolète.
Ces compteurs ne sont pas importants.

- `healthy` - État de santé de la *HA*
- `last_status` - Dernier état connu de la *HA*
- `last_transition` - Date du dernier changement d'état de la *HA* au format *ISO8601*
- `leader` - Vrai pour un GCap *leader*, faux pour un GCap *follower*
- `status` - État actif ou inactif (false) de la *HA*
  Exemple :

```
"high_availability": {
    "healthy": false,
    "last_status": -1,
    "last_transition": "0001-01-01T00:00:00Z",
    "leader": false,
    "status": false
},
```

6.2.1.10.4.7 Détails des compteurs `interfaces` - Statistiques sur les interfaces réseaux

- `bond0` - Nom de l'interface réseau
  - `rx_bytes` - Nombre d'octets reçus
  - `rx_drop` - Nombre d'octets perdus en réception
  - `rx_errs` - Nombre d'octets invalides en réception
  - `rx_packets` - Nombre total de paquets reçus depuis cette interface
  - `tx_bytes` - Nombre d'octets envoyés
  - `tx_drop` - Nombre d'octets perdus en envoi
  - `tx_errs` - Nombre d'octets invalides en envoi
  - `tx_packets` - Nombre total de paquets envoyés depuis cette interface

  Exemple :

```
"interfaces": {
    "bond0": {
        "rx_bytes": 0,
        "rx_drops": 0,
        "rx_errs": 0,
        "rx_packets": 0,
        "tx_bytes": 0,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    },
    "gcp0": {
        "rx_bytes": 138433006,
        "rx_drops": 82901,
        "rx_errs": 0,
        "rx_packets": 2143236,
        "tx_bytes": 796294,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 3635
    },
    "gcp1": {
        "rx_bytes": 137642525,
        "rx_drops": 82902,
        "rx_errs": 0,
        "rx_packets": 2135060,
        "tx_bytes": 0,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    }
},
```

6.2.1.10.4.8 Détails des compteurs `loadavg` - Statistiques sur la charge moyenne du GCap

- `active_processes` - Nombres de processus lancés
- `load_average_15_mins` - Charge moyenne sur les quinze dernières minutes
- `load_average_1_min` - Charge moyenne sur la dernière minute
- `load_average_5_mins` - Charge moyenne sur les cinq dernières minutes
- `running_processes` - Nombre de processus en cours d'exécution
  Exemple :


```
"loadavg": {
    "active_processes": 561,
    "load_average_15_mins": 0.99,
    "load_average_1_min": 0.67,
    "load_average_5_mins": 1,
    "running_processes": 2
},
```

6.2.1.10.4.9 Détails des compteurs `meminfo` - Statistiques sur la mémoire vive

- `available` - Mémoire physique totale en kilo-octets
- `buffers` - Mémoire utilisée par des opérations disques en kilo-octets
- `cached` - Mémoire utilisée par le cache en kilo-octets
- `dirty` - Mémoire utilisée par des opérations d'écritures en attente en kilo-octets
- `free` - Mémoire inutilisée en kilo-octets
- `hugepages_anonymous` - Nombre de *huge pages* transparentes anonymes utilisées
- `hugepages_free` - Nombre de *huge pages* transparentes disponibles
- `hugepages_reserved` - Nombre de *huge pages* transparentes réservées
- `hugepages_shmem` - Nombre de *huge pages* transparentes partagées
- `hugepages_surplus` - Nombre de *huge pages* transparentes en surplus
- `hugepages_total` - Nombre total de *huge pages*
- `kernel_stack` - Mémoire utilisée par les allocations de la pile du noyau en kilo-octets
- `page_tables` - Mémoire utilisée pour la gestion des pages en kilo-octets
- `s_reclaimable` - Mémoire de cache qui peut-être ré-alloué en cas de manque de mémoire en kilo-octets
- `shmem` - Mémoire utilisée par les pages partagées en kilo-octets
- `slab` - Mémoire utilisée par les structures de données du noyau en kilo-octets
- `swap_cached` - Mémoire utilisée par le cache du swap en kilo-octets
- `swap_free` - Mémoire disponible dans le swap en kilo-octets
- `swap_total` - Mémoire totale du swap en kilo-octets.
- `total` - Mémoire totale en kilo-octets
- `v_malloc_used` - Mémoire utilisée par les grandes zones de mémoire allouées par le noyau
  Pour plus d'informations, se référer à cette documentation `meminfo`.
  Exemple :


```
"meminfo": {
    "available": 13608896,
    "buffers": 380932,
    "cached": 1155824,
    "dirty": 28,
    "free": 13128080,
    "hugepages_anonymous": 423936,
    "hugepages_free": 0,
    "hugepages_reserved": 0,
    "hugepages_shmem": 0,
    "hugepages_surplus": 0,
    "hugepages_total": 0,
    "kernel_stack": 9152,
    "page_tables": 8400,
    "s_reclaimable": 43168,
    "shmem": 794564,
    "slab": 210008,
    "swap_cached": 0,
    "swap_free": 16777212,
    "swap_total": 16777212,
    "total": 15977468,
    "v_malloc_used": 66592
},
```

6.2.1.10.4.10 Détails des compteurs `numastat` - Statistiques sur les nœud NUMA

- `nodes` - Liste des nœuds NUMA
  - `nodeX` - Statistiques du nœud NUMA X
    - `interleave_hit` - Mémoire entrelacée allouée avec succès dans ce nœud
    - `local_node` - Mémoire allouée dans ce nœud alors qu'un processus fonctionnait dessus
    - `numa_foreign` - Mémoire prévu pour ce nœud, mais actuellement allouée dans un nœud différent
    - `numa_hit` - Mémoire allouée avec succès dans ce nœud comme prévu
    - `numa_miss` - Mémoire allouée dans ce nœud en dépit des préférences de processus.
      Chaque numa_miss a un numa_foreign dans un autre nœud
    - `other_node` - Mémoire allouée dans ce nœud alors qu'un processus fonctionnait dans un autre nœud

Exemple :


```
"numastat": {
    "nodes": {
        "node0": {
            "interleave_hit": 3871,
            "local_node": 4410557829,
            "numa_foreign": 0,
            "numa_hit": 4410454203,
            "numa_miss": 0,
            "other_node": 14170
        },
        "node1": {
            "interleave_hit": 3869,
            "local_node": 4224990850,
            "numa_foreign": 0,
            "numa_hit": 4224964539,
            "numa_miss": 0,
            "other_node": 21531
        }
    }
},
```


6.2.1.10.4.11 Détails des compteurs `quotas` - Statistiques sur les quotas par catégorie

- `quotas` - Liste des quotas
  - `by_gid` - Statistiques triés par groupe (identifiant gid)
  - `by_prj` - Statistiques triés par projet (identifiant prj)
  - `by_uid` - Statistiques triés par utilisateur (identifiant uid)

Dans chaque catégorie, les compteurs suivant sont affichés :

- `block_grace` - Temps de grâce pour les blocks
- `block_hard_limit` - Limite matérielle des blocks.
  Définit une limite absolue pour l'utilisation de l'espace.
  L'utilisateur ne peut pas dépasser cette limite.
  Passée cette limite, l'écriture sur ce système de fichiers lui est interdite.
- `block_soft_limit` - Limite logicielle des blocks
  Indique la quantité maximale d'espace qu'un utilisateur peut occuper sur le système de fichiers.
  Si cette limite est atteinte, l'utilisateur reçoit des messages d'avertissement quant au dépassement du quota qui lui a été attribué.
  Si son utilisation est combinée avec les délais (ou grace period), lorsque l'utilisateur continue à dépasser la limite logicielle après que se soit écoulé le délai de grâce, alors il se retrouve dans le même cas que dans l'atteinte d'une limite dure.
- `block_used` - Nombre de blocks utilisés
- `file_grace` - Temps de grâce pour les fichiers
- `file_hard_limit` - Limite matérielle des fichiers
  Définit une limite absolue pour l'utilisation de l'espace.
  L'utilisateur ne peut pas dépasser cette limite.
  Passée cette limite, l'écriture sur ce système de fichiers lui est interdite.
- `file_soft_limit` - Limite logicielle des fichiers
  Indique la quantité maximale d'espace qu'un utilisateur peut occuper sur le système de fichiers.
  Si cette limite est atteinte, l'utilisateur reçoit des messages d'avertissement quant au dépassement du quota qui lui a été attribué.
  Si son utilisation est combinée avec les délais (ou grace period), lorsque l'utilisateur continue à dépasser la limite logicielle après que se soit écoulé le délai de grâce, alors il se retrouve dans le même cas que dans l'atteinte d'une limite dure.
- `file_used` - Nombre de fichiers utilisés

Exemple :


```
"quotas": {
    "by_gid": {
        "0": {
            "block_grace": "0",
```


(suite sur la page suivante)

(suite de la page précédente)


```
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "2148952",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "177"
        },
        "10012": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "5216",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "295"
        },
        }
    },
    "by_prj": {
        "0": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "51600",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "225"
        },
        "1": {
            "block_grace": "0",
            "block_hard_limit": "7980499",
            "block_soft_limit": "7980499",
            "block_used": "2101904",
            "file_grace": "0",
            "file_hard_limit": "1000",
            "file_soft_limit": "1000",
            "file_used": "43"
        },
        }
    },
    "by_uid": {
        "0": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "2153356",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "269"
        },
        "10012": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "1032",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "258"
        },
    }
}
```


L'exemple ci après est sans limite définie : la valeur "0" indique qu'il n'y a pas de valeur définie pour les limites et les temps de grâce.


```
"10012": {
    "block_grace": "0",
    "block_hard_limit": "0",
    "block_soft_limit": "0",
```


(suite sur la page suivante)

(suite de la page précédente)


```
        "block_used": "1032",
        "file_grace": "0",
        "file_hard_limit": "0",
        "file_soft_limit": "0",
        "file_used": "258"
    },
```


6.2.1.10.4.12 Détails des compteurs `sofnet` - Statistiques sur les paquets reçus en fonction des cœurs de processeurs

- `cpus` - Statistiques d'utilisation par CPU
  - `cpuX` - Statistiques du cœur CPU X
    - `backlog_len` -
    - `dropped` - Nombre de paquets perdus
    - `flow_limit_count` - Nombre de fois où la limite de débit a été atteinte
    - `processed` - Nombre de paquets traités
    - `received_rps` - Nombre de fois où le CPU a été réveillé
    - `time_squeeze` - Nombre de fois où le thread n'a pas pu traiter tous les paquets de son backlog dans le budget imparti
  - `summed` - Statistiques d'utilisation globales des cœurs
    - `backlog_len` -
    - `dropped` - Nombre de paquets perdus
    - `flow_limit_count` - Nombre de fois où la limite de débit a été atteinte
    - `processed` - Nombre de paquets traités
    - `received_rps` - Nombre de fois où le CPU a été réveillé
    - `time_squeeze` - Nombre de fois où le thread n'a pas pu traiter tous les paquets de son backlog dans le budget imparti

Exemple :


```
  "softnet": {
      "cpus": {
          "cpu0": {
              "backlog_len": 0,
              "dropped": 0,
              "flow_limit_count": 0,
              "processed": 448550,
              "received_rps": 0,
              "time_squeeze": 2
          },
          "cpu1": {
              "backlog_len": 0,
              "dropped": 0,
              "flow_limit_count": 0,
              "processed": 36250,
              "received_rps": 0,
              "time_squeeze": 0
          }
      },
      "summed": {
          "backlog_len": 0,
          "dropped": 0,
          "flow_limit_count": 0,
          "processed": 5239450,
          "received_rps": 0,
          "time_squeeze": 27
      }
  },
```

6.2.1.10.4.13 Détails des compteurs `Sigflow` - Informations sur Sigflow (*monitoring-engine*)

`detailed_status` - Statut du container Sigflow

- `up` - État de Sigflow et du moteur de détection

detailed_status + état "up"	signification
état "Container down" + "up" false	état moteur arrêté
état "Container down" + "up" true	état impossible : appli ne peut pas tourner dans un container éteint
état "Container UP" + "up" false	état instable : appeler le support de GATEWATCHER
état "Container UP" + "up" true	état moteur démarré

Exemple :

```
    "suricata": {
        "detailed_status": "Container down",
        "up": false
    },
```

6.2.1.10.4.14 Détails des compteurs `systemd` - Informations du système d'initialisation

- `failed_services` - Liste des services échoués rapportée par `systemctl --failed`.

Exemple :

```
    "systemd": {
        "failed_services": [ "netdata.service" ]
    },
```

6.2.1.10.4.15 Détails des compteurs `uptime` - Temps de disponibilité

- `up_seconds` - Nombre de secondes écoulées depuis le démarrage.

Exemple :

```
    "uptime": {
        "up_seconds": 874179.8
    },
```

6.2.1.10.4.16 Détails des compteurs `virtualmemory` - Information sur l'espace d'échange (*swap*)

- `disk_in` : Nombre de pages sauvées sur le disque depuis le démarrage.
- `disk_out` - Nombre de pages sortantes du disque depuis le démarrage.
- `pagefaults_major` - Nombre de *page faults* par seconde.
- `pagefaults_minor` - Nombre de *page faults* par seconde pour charger une page mémoire du disque vers la RAM.
- `swap_in` - Nombre de kilo-octets que le système a échangé depuis le disque vers la RAM par seconde.
- `swap_out` - Nombre de kilo-octets que le système a échangé depuis la RAM vers le disque par seconde.
  Exemple :

```
    "virtualmemory": {
        "disk_in": 307828,
        "disk_out": 4724267,
        "pagefaults_major": 1210,
        "pagefaults_minor": 14233474300,
        "swap_in": 0,
        "swap_out": 0
    }
```

6.2.1.11 interfaces

6.2.1.11.1 Introduction

La commande `interfaces` du sous-groupe `show` permet d'afficher les interfaces réseau du GCap :

- les interfaces de management (anciennement `gcp0` et `gcp1`)
- les interfaces de détection disponibles physiques `mon0` à `monx` ou virtuelle `monvirt`

Cette commande peut prendre en paramètre le mot clé `delay` pour afficher la période de grâce accordée au démarrage des interfaces.
Les informations suivantes sont disponibles avec la commande `show interfaces` :

- **Label** : le nom de label de l'interface, **monX** pour les interfaces de capture, **tunnel** pour les connexions IPSec, **management** pour les connexions SSH ou connexions SSH et IPSec si le rôle de l'interface est **management-tunnel**, **clusterX** pour les interfaces en mode cluster.
- **Name** : le nom de système de l'interface
- **Role** : le rôle attribué à l'interface, **capture** pour les interfaces de capture, **tunnel** pour les connexions IPSec, **management** pour les connexions SSH, **management-tunnel** pour les connexions SSH et IPSec, **capture-cluster** pour les interfaces de capture en mode cluster, **inactive** pour les interfaces désactivées.
- **Capture capability** : si l'interface peut capturer du trafic
- **MTU** : le MTU de l'interface
- **Physical Address** : l'adresse MAC de l'interface
- **Speed** : la vitesse de l'interface
- **Type** : le type de câble/sfp connecté au port physique
- **Vendor ID** : l'ID du fournisseur de la carte réseau
- **Device ID** : l'ID de la carte réseau
- **PCI bus** : numéro du bus PCI utilisé par la carte réseau

---

6.2.1.11.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.11.3 Commandes

```
show interfaces{ |delay|}
```

6.2.1.11.4 Exemple pour afficher les interfaces de capture disponibles

- Entrer la commande suivante.

```
(gcap-cli) show interfaces
```

- Valider.
  Le système affiche les interfaces de capture disponibles.

```
(gcap-cli) 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
```

Note :

Toutes les interfaces existantes sont affichées, même celles qui composent une agrégation d'interfaces.

6.2.1.11.5 Exemple pour afficher la période de grâce accordée au démarrage des interfaces

- Entrer la commande suivante.

```
(gcap-cli) show interfaces delay
```

- Valider.
  Le système affiche la période de grâce accordée au démarrage des interfaces.

```
NIC startup delay: 10 seconds
```

6.2.1.12 keymap

6.2.1.12.1 Introduction

La commande `keymap` du sous-groupe `show` permet d'afficher la disposition du clavier entre azerty (choix fr) et qwerty (choix en) utilisé sur les interfaces physiques (KVM, iDRAC, physique).

6.2.1.12.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.1.12.3 Commande

```
show keymap
```

6.2.1.12.4 Exemple pour afficher la langue courante du clavier

```
(gcap-cli) show keymap
```

- Valider.
  Le système affiche les informations courantes. Exemple :

```
Current keymap is fr
```

6.2.1.13 logs

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.14 monitoring-engine

6.2.1.14.1 Introduction

La commande `monitoring-engine` du sous-groupe `show` permet d'afficher les options avancées de la configuration du moteur de détection du GCap :

- la période de grâce lors du démarrage du moteur (start-timeout)
- la période de grâce lors de l'arrêt du moteur (stop-timeout)
- l'état des contrôles de vérification (sanity checks)

6.2.1.14.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.1.14.3 Commande

```
show monitoring-engine {start-timeout|stop-timeout|sanity-checks}
```

6.2.1.14.4 Exemple pour afficher la valeur par défaut du start-timeout

- Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine start-timeout
```

- Valider.
  Le système affiche la valeur courante.

```
Monitoring Engine Options:
Start timeout: 600s
```

6.2.1.14.5 Exemple pour afficher la valeur par défaut du stop-timeout

- Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine stop-timeout
```

- Valider.
  Le système affiche la valeur courante.

```
Monitoring Engine Options:
Stop timeout: 300s
```

6.2.1.14.6 Exemple pour afficher l'état du contrôles de vérification

- Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine sanity-checks
```

- Valider.
  Le système affiche la valeur courante.

```
Monitoring Engine Options:
Sanity checks enabled
```

  Le système répond que le système de contrôle est bien actif.
  Le moteur de détection ne démarre qu'après avoir vérifié qu'au moins une interface de capture `monx` a été activée et un câble est connecté.

6.2.1.15 network-config

6.2.1.15.1 Introduction

Le GCap possède :

- des interfaces de capture et de surveillance,
- des interfaces réseau pour la gestion de la sonde via SSH et pour l'appairage avec le GCenter.

Deux cas sont possibles :

- **configuration simple-interface**
  La connexion SSH pour la gestion du GCap et la communication VPN sont gérées par une interface (anciennement `gcp0`).
- **configuration double-interface**
  La communication VPN est gérée par l'interface (anciennement `gcp0`).
  La connexion SSH pour la gestion du GCap est gérée par l'autre interface (anciennement `gcp1`).

Pour plus d'informations sur les interfaces réseaux, se référer à la section *Description des entrées / sorties du GCap*.
La commande `network-config` du sous-groupe `show` permet d'afficher :

- l'état de toutes les interfaces du GCap : commande `show network-config configuration`
- l'état pour chacune des interfaces : commande `show network-config tunnel` ou `show network-config management`
- le nom du domaine : commande `show network-config domain`
- le nom d'hôte : commande `show network-config hostname`

6.2.1.15.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.15.3 Commandes

`show network-config {configuration|domain|gcp0|gcp1|hostname|ssh|status|vpn-link}`

6.2.1.15.4 Exemple pour afficher la configuration du GCap

- Entrer la commande suivante.

```
(gcap-cli) show network-config configuration
```

- Valider.
  Suivant la configuration simple interface ou double interface, les informations sont différentes.
  Les deux cas sont listés ci-après.

6.2.1.15.4.1 Configuration simple-interface


```
(gcap-cli) show network-config configuration
{
    "hostname": "GCap",
    "domain_name": "gatewatcher.com",
    "tunnel": {
        "ip_address": "192.168.1.2",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.1"
    },
    "management": {
        "ip_address": "192.168.1.2",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.1"
    },
    "enp12s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp20s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp27s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "monvirt": {
        "filtering_rules": {},
        "mtu": 1500
    }
}
```

6.2.1.15.4.2 Configuration double-interface

Dans ce cas, le système affiche les informations de configuration.


```
(gcap-cli) show network-config configuration
{
    "hostname": "GCap",
    "domain_name": "gatewatcher.com",
    "tunnel": {
        "ip_address": "192.168.1.2",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.1"
    },
    "management": {
        "ip_address": "192.168.2.2",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.2.1"
    },
    "enp12s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp20s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp27s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "monvirt": {
        "filtering_rules": {},
        "mtu": 1500
    }
}
```


6.2.1.15.5 Exemple pour afficher le domaine du GCap

- Entrer la commande suivante.

```
(gcap-cli) show network-config domain
```

- Valider.
  Le système affiche le nom du domaine.

```
Current domain name: gatewatcher.com
```

6.2.1.15.6 Exemple pour afficher la configuration de l'interface `management`

- Entrer la commande suivante.

```
(gcap-cli) show network-config management
```

- Valider.
  Le système affiche la configuration de l'interface **management**.
  Par exemple :

```
Interface tunnel configuration
        - IP Address: 192.168.1.2
        - Mask: 255.255.255.0
        - Gateway: 192.168.1.1
```

6.2.1.15.7 Exemple pour afficher la configuration de l'interface `tunnel`

- Entrer la commande suivante.

```
(gcap-cli) show network-config tunnel
```

- Valider.
  Le système affiche la configuration de l'interface `tunnel`.
  Par exemple :

```
Interface tunnel configuration
   - IP Address: 192.168.2.2
   - Mask: 255.255.255.0
   - Gateway: 192.168.2.1
```

6.2.1.15.8 Exemple pour afficher le nom d'hôte du GCap

- Entrer la commande suivante.

```
(gcap-cli) show network-config hostname
```

- Valider.
  Le système affiche l'interface le nom d'hôte du GCap.

```
Current hostname: GCap-name
```

6.2.1.16 password-policy

6.2.1.16.1 Introduction

La commande `password-policy` du sous-groupe `show` permet d'afficher la politique de mot de passe pour les comptes `setup`, `gviewadm` et `gview`.
La possibilité de modifier cette politique est donnée par la commande *`set password-policy`*.

6.2.1.16.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.1.16.3 Commande

```
show password-policy
```

6.2.1.16.4 Exemple pour afficher la politique des mots de passe par défaut

- Entrer la commande suivante.

```
(gcap-cli) show password-policy
```

- Valider.
  Le système affiche les règles à respecter pour la définition d"un mot de passe.

```
Password complexity rules:
  Minimum different characters between old and new passwords: 2
  Minimum length: 12
  Lowercase character required: yes
  Uppercase character required: yes
  Digit required: yes
  Other character class required: yes
```

Paramètre...	signification...
Minimum different characters between old and new passwords : x	Il faut au minimum x caractères différents pour qu'un mot de passe soit considéré comme différent
Minimum length	longueur minimum du mot de passe : ici 12 caractères
Lowercase character required :	yes : signifie que le mot de passe doit contenir au moins 1 minuscule
Uppercase character required :	yes : signifie que le mot de passe doit contenir au moins 1 majuscule
Digits required :	yes : signifie que le mot de passe doit contenir au moins 1 chiffre 0 à 9
Symbols required :	yes : signifie que le mot de passe doit contenir au moins 1 symbole cad ni un chiffre ni une lettre

---

6.2.1.17 passwords

6.2.1.17.1 Introduction

La commande `passwords` du sous-groupe `show` permet :

- d'afficher la liste des utilisateurs gérés par le niveau courant
  Accessible pour utilisateurs setup, gviewadm, gview
- de récupérer le token root sous forme de texte ou de QR code
  Accessible pour utilisateur setup uniquement

Note :

La fonctionnalité "récupérer le token root" doit être utilisée en concertation avec le service support de GATEWATCHER.

6.2.1.17.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.1.17.3 Commande

```
show passwords {list|text|qrcode}
```

6.2.1.17.4 Exemple pour afficher la liste des utilisateurs gérés par le niveau courant

- Entrer la commande suivante.

```
(gcap-cli) show passwords list
```

- Valider.
  Le système affiche la liste des utilisateurs gérés par le niveau courant :
  - Exemple pour le niveau gview :

    ```
    Allowed users: gview
    ```

  - Exemple pour le niveau setup :

    ```
    Allowed users: gviewadm, gview, setup
    ```

6.2.1.17.5 Exemple pour afficher le token root en texte

- Entrer la commande suivante.

```
(gcap-cli) show passwords root text
```

- Valider.
  Le système affiche le token root en texte.

```
Encrypted Root Token is: "hzDpahGYq2i8aiSXwRfmhC7W3ZtSHteyJ22J2tL5OlI1Aq+nYsgJaGi7JyXVjGKyDs1TCBZqbXiobXe9y1o"
```

6.2.1.17.6 Exemple pour afficher du token root en QR code

- Entrer la commande suivante.

```
(gcap-cli) show passwords root qrcode
```

- Valider.
  Le système affiche le token root en QR code.

```

```

6.2.1.18 protocols-selector

Cette commande est supprimée depuis la version 2.5.3.105.

6.2.1.19 session-timeout

6.2.1.19.1 Introduction

La commande `session-timeout` du sous-groupe `show` permet d'afficher le temps d'inactivité avant la déconnexion d'une session utilisateur.
Cette valeur est exprimée en minutes et la valeur par défaut est de 5 minutes.

6.2.1.19.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.19.3 Commande

```
show session-timeout
```

6.2.1.19.4 Exemple pour afficher la valeur de session-timeout

- Entrer la commande suivante.

```
(gcap-cli) show session-timeout
```

- Valider.
  Le système affiche la valeur courante de fin de session.
  Par exemple :

```
Current session timeout is 5 mins
```

6.2.1.20 setup-mode

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.21 status

6.2.1.21.1 Introduction

La commande `status` du sous-groupe `show` permet d'afficher l'état courant du GCap.

6.2.1.21.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.1.21.3 Commande

```
show status
```

6.2.1.21.4 Exemple pour afficher les informations du GCap

- Entrer la commande suivante.

```
(gcap-cli) show status
```

- Valider.
  Par exemple :

```
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
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 ...
```

Le système affiche les informations suivantes :

- **GCAP FQDN** : Fully Qualified Domain Name du GCap, ici **gcap.gatewatcher.com**.
- **Version** : version courante du logiciel : ici **2.5.4.0**.
- **Overall status** : état global courant du GCap, ici **Running**.
- **Tunnel** : état du tunnel entre GCap et GCenter, ici **up**.
- **Detection Engine** : état du container du moteur de détection, ici non démarré **Up and running**.
- **Configuration** : état de la configuration, ici **Complete**.
- **Gcap name** : nom du GCap, ici **gcap**.
- **Domain name** : nom de domaine du GCap, ici **gatewatcher.com**.
- **Tunnel interface** : adresse IP de l'interface tunnel, ici **192.168.2.2**.
- **Management interface** : adresse IP de l'interface management, ici **192.168.1.2**.
- **Gcenter version** : version du GCenter distant, ici **2.5.3.103**.
- **Gcenter IP** : adresse IP du GCenter distant, ici **192.168.2.3**.
- **Paired on Gcenter** : état de l'appairage avec le GCenter, **Yes**.
- **Monitoring interfaces** : interfaces de surveillance autorisées, ici **mon0, mon2, mon4, monvirt**.

6.2.1.22 tech-support

6.2.1.22.1 Introduction

La commande `tech-support` du sous-groupe `show` permet d'extraire les informations du GCap demandées par le support technique.

Note :

Le tech-support n'est pas chiffré et peut contenir des informations sensibles.

6.2.1.22.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.1.22.3 Commande

```
ssh -t setup@GCapX show tech-support {brief|large} > /tmp/tech-supp-brief-GCapX
```

Note :

Il faut remplacer GCapX par l'adresse IP du GCap.

6.2.1.22.3.1 Commande pour extraire un tech-support allégé

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

6.2.1.22.3.2 Commande pour extraire un tech-support standard

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

6.2.1.22.3.3 Commande pour extraire un tech-support verbeux

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

6.2.1.23 advanced-configuration

6.2.1.23.1 high availability by redundancy of 2 GCaps

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.23.2 interface-names

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.23.3 local-rules

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.23.4 memory-settings

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.23.5 MTU

Cette fonctionnalité a été supprimée depuis la version 2.5.4.0.

6.2.1.23.6 packet-filtering

6.2.1.23.6.1 Introduction

La commande `packet-filtering` du sous-groupe `show advanced-configuration` permet d'afficher les règles statiques de filtrage des paquets.

Note :

Le filtrage de paquets n'est pas supporté lorsque la MTU > 3000.

6.2.1.23.6.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :**
  - le moteur de détection doit être à l'arrêt
  - une interface de capture réseau doit être activée

6.2.1.23.6.3 Commande

`show advanced-configuration packet-filtering`

6.2.1.23.6.4 Exemple pour afficher les règles de filtrage du flux

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration packet-filtering
```

- Valider.
  Le système affiche le résultat.

```
Current XDP filters:
 - 0: iface mon1 native vlan 10
 - 1: iface mon2 native vlan 1
 - 2: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 22:22
 - 3: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 443:443
 - 4: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 465:465
 - 5: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 993:993
 - 6: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 995:995
 - 7: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 500:500
 - 8: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 4500:4500
 - 9: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto GRE
 - 10: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto ESP
 - 11: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto AH
 - 12: iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto L2TP
```

6.2.2 set

6.2.2.1 bruteforce-protection

6.2.2.1.1 Introduction

La commande `bruteforce-protection` du sous-groupe `set` permet de gérer le système de protection contre les attaques par force brute lors de la connexion d'un utilisateur.
Les comptes des utilisateurs sont automatiquement verrouillés pour une durée prédéfinie après plusieurs tentatives infructueuses.
Par défaut, cette valeur est à 3.
Pour visualiser les valeurs courantes du nombre d'essais et de la durée de verrouillage du compte, utiliser la commande *show bruteforce-protection*.

6.2.2.1.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.2.1.3 Commandes

`set bruteforce-protection {lock-duration|max-tries|restore-default}`

6.2.2.1.3.1 Commande pour définir un nombre maximum d'essais à l'authentification d'un compte (0 pour désactiver)

`set bruteforce-protection lock-duration {0|1-86400}`

6.2.2.1.3.2 Commande pour définir une durée de verrouillage du compte en secondes (0 pour désactiver)

```
set bruteforce-protection max-tries {0|1-100}
```

6.2.2.1.3.3 Commande pour restaurer la configuration par défaut

```
set bruteforce-protection restore-default
```

6.2.2.1.4 Exemple pour changer la durée de verrouillage à 360 secondes

- Entrer la commande suivante.

```
(gcap-cli) set bruteforce-protection lock-duration 360
```

- Valider.
  Le système indique que le paramètre a été modifié.

```
Updating bruteforce protection configuration
Bruteforce protection configuration updated
```

6.2.2.2 clusters

Cette commande a été supprimée depuis la version 2.5.4.0.
Pour la mise en œuvre, se référer à la *Procédure de gestion de l'agrégation d'interfaces de capture*.

6.2.2.3 compatibility-mode

6.2.2.3.1 Introduction

La commande `compatibility-mode` du sous-groupe `set` permet de modifier le mode de compatibilité utilisé pour interagir avec le GCenter.
Le mode de compatibilité va influer sur les fonctionnalités disponibles du GCap.

Plusieurs modes de compatibilité sont disponibles :

- 2.5.3.102 : GCenter 2.5.3.102
- 2.5.3.103 : GCenter 2.5.3.103

Pour un GCap	Version du GCenter	Supportée	Action ou Commande à exécuter
2.5.4.1	2.5.3.101 HF4	Non supportée	GCenter à migrer vers une version plus récente
2.5.4.1	2.5.3.102 HF3	Supportée	set compatibility-mode 2.5.3.102
2.5.4.1	2.5.3.103	Supportée	set compatibility-mode 2.5.3.103

Important :

Le tableau ci-avant est donné pour exemple. Se référer impérativement à la note de version du GCap.

Note :

Le mode de compatibilité avec la version 2.5.3.101 et inférieur est obsolète.

6.2.2.3.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.3.3 Commande

```
set compatibility-mode {2.5.3.102|2.5.3.103}
```

6.2.2.3.4 Exemple pour configurer la compatibilité entre un GCap version V2.5.4.0 avec un GCenter 2.5.3.102

- Entrer la commande suivante.

```
(gcap-cli) set compatibility-mode 2.5.3.102
```

- Valider.

6.2.2.4 datetime

6.2.2.4.1 Introduction

La commande `datetime` du sous-groupe `set` permet d'ajuster la date et l'heure du GCap.
Cela permet d'éviter des problèmes d'horloges pouvant entraîner par exemple l'impossibilité d'établir un tunnel IPSec avec le GCenter.

Note :

Il est impératif d'ajuster cette horloge pour que le GCap et le GCenter associé soient à la même heure (par exemple : pour l'horodatage des événements).

6.2.2.4.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.2.4.3 Commande

```
set datetime {YYYY-MM-DDThh:mm:ssZ}
```

6.2.2.4.4 Exemples pour modifier l'heure du GCap

- Entrer la commande suivante.

```
(gcap-cli) set datetime 2022-01-26T16:00:00Z
```

- Valider.
  Le système affiche le résultat.

```
Date successfully changed to Wed Jan 26 2022 16:00:00
```

6.2.2.5 gcenter-ip

6.2.2.5.1 Introduction

La commande `gcenter-ip` du sous-groupe `set` permet de spécifier l'adresse IP du GCenter auquel le GCap sera appairé.

Note :

Le GCap utilise cette adresse IP lors de l'appairage afin de se connecter au GCenter en SSH et récupérer la fingerprint de ce dernier.

6.2.2.5.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.5.3 Commande

`set gcenter-ip {GCenter-IP}`

6.2.2.5.4 Exemple

- Entrer la commande suivante.

```
(gcap-cli) set gcenter-ip 192.168.1.1
```

- Valider.
  Le système affiche le résultat.

```
Setting GCenter IP to 192.168.1.1
```

6.2.2.6 interfaces

6.2.2.6.1 Introduction

La commande `interfaces` du sous-groupe `set` permet d'administrer les interfaces de capture.
Les interfaces peuvent être physiques ou virtuelles.
Les interfaces virtuelles permettent de rejouer des fichiers *.pcap* directement sur le GCap.

6.2.2.6.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.6.3 Commande

Pour modifier le délai avant le démarrage des interfaces : `set interfaces delay SECOND`
Pour attribuer un rôle spécifique à une interface : `set interfaces assign-role {management|tunnel|management-tunnel|capture|capture-cluster|i`

- **Role** : Les rôles attribués à l'interface sont les suivants :
  - **capture** pour les interfaces de capture
  - **tunnel** pour les connexions IPSec
  - **management** pour les connexions SSH
  - **management-tunnel** pour les connexions SSH et IPSec
  - **capture-cluster** pour les interfaces de capture en mode cluster
  - **inactive** pour les interfaces désactivées

6.2.2.6.4 Exemple pour modifier le délai de démarrage des interfaces à 5s

- Entrer la commande suivante.

```
(gcap-cli) set interfaces delay 5
```

- Valider.

6.2.2.6.5 Exemple pour attribuer un rôle de capture à une interface spécifique

- Entrer la commande suivante.

```
(gcap-cli) set interfaces assisgn-role enp4s0 capture
```

- Valider.

Note :

Si le système affiche le message suivant, *Failed to assign role : network configuration cannot be changed now*, vérifier si le moteur de détection est allumé.

6.2.2.7 keymap

6.2.2.7.1 Introduction

La commande `keymap` du sous-groupe `set` permet de choisir la disposition du clavier entre azerty (choix fr) et qwerty (choix en) utilisé sur les interfaces physiques (KVM, iDRAC, physique).

6.2.2.7.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.2.7.3 Commande

```
set keymap {fr|en}
```

6.2.2.7.4 Exemple de clavier français

- Entrer la commande suivante.

```
(gcap-cli) set keymap fr
```

- Valider.
  Le système affiche le résultat.

```
Setting keymap to fr
```

6.2.2.7.5 Exemple de clavier anglais US

- Entrer la commande suivante.

```
(gcap-cli) set keymap en
```

- Valider.
  Le système affiche le résultat.

```
Setting keymap to en
```

6.2.2.8 monitoring-engine

6.2.2.8.1 Introduction

La commande `monitoring-engine` du sous-groupe `set` permet d'appliquer une configuration avancée pour le moteur de détection de la sonde GCap.

Note :

Si le nombre de signatures chargé par Sigflow est trop important, il faut adapter la valeur du timeout.

6.2.2.8.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection est à l'arrêt

6.2.2.8.3 Commande

Pour modifier la période de grâce lors du démarrage du moteur : `set monitoring-engine start-timeout SECOND`.
Pour modifier la période de grâce lors de l'arrêt du moteur : `set monitoring-engine stop-timeout SECOND`.
Pour activer ou désactiver la vérification des contrôles : `set monitoring-engine {disable-sanity-checks|enable-sanity-checks}`.
Si l'option `sanity-checks` est sur `enable`, le moteur de détection ne démarre qu'après avoir vérifié qu'au moins une interface de capture `monx` a été activée et qu'un câble est connecté.

6.2.2.8.4 Exemple modifier la période de grâce à 600 secondes lors du démarrage du moteur

- Pour modifier la période de grâce à 600 secondes lors du démarrage du moteur :
  - Entrer la commande suivante.

```
(gcap-cli) set monitoring-engine start-timeout 600
```

  - Valider.
- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine start-timeout
```

  - Valider.

Le système affiche la valeur courante.

```
Monitoring Engine Options:
start timeout: 600s
```

6.2.2.8.5 Exemple modifier la période de grâce lors de l'arrêt du moteur à 600 secondes

- Pour modifier la période de grâce à 600 secondes lors de l'arrêt du moteur :
  - Entrer la commande suivante.

```
(gcap-cli) set monitoring-engine stop-timeout 600
```

  - Valider.
- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine stop-timeout
```

- Valider.

Le système affiche la valeur courante.

```
Monitoring Engine Options:
Stop timeout: 600s
```

6.2.2.8.6 Exemple pour désactiver la vérification des interfaces de capture

- Pour désactiver la vérification des interfaces de capture :
  - Entrer la commande suivante.

```
(gcap-cli) set monitoring-engine disable-sanity-checks
```

  - Valider.
- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine sanity-checks
```

  - Valider.
    Le système affiche la valeur courante.

```
Monitoring Engine Options:
Sanity checks disabled
```

6.2.2.8.7 Exemple pour activer la vérification des interfaces de capture

- Pour activer la vérification des interfaces de capture :
  - Entrer la commande suivante.

```
(gcap-cli) set monitoring-engine enable-sanity-checks
```

  - Valider.
- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show monitoring-engine sanity-checks
```

  - Valider.

Le système affiche la valeur courante.

```
Monitoring Engine Options:
Sanity checks enabled
```

6.2.2.9 network-config

6.2.2.9.1 Introduction

Pour plus d'informations sur les interfaces réseau (`gcp0`/`gcp1`) et les interfaces de capture et de surveillance (`mon0` à `monx`), se référer à la commande *show network-config*.
La commande `network-config` du sous-groupe `set` permet de modifier la configuration réseau du GCap.
La commande `network-config` du sous-groupe `set` permet de configurer :

- chacune des interfaces en indiquant les paramètres réseau : commande `set network-config {gcp0|gcp1} [ip-address IP_value] [gateway GATEWAY_value] [mask MASK_value]`
- le nom de domaine : commande `set network-config domain NAME_value`
- le nom d'hôte : commande `set network-config hostname HOSTNAME_value`

6.2.2.9.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.9.3 Commande

`set network-config {management|tunnel} [ip-address IP_value] [gateway GATEWAY_value] [mask MASK_value] [confirm] [no-reload]`

`set network-config [domain-name NAME_value|hostname HOSTNAME_value] [confirm]`

Note :

L'option *no-reload* permet de ne pas recharger les services réseau.

6.2.2.9.4 Exemple pour configurer l'interface `tunnel` et l'interface `management`

- Entrer la commande suivante.

```
(gcap-cli) set network-config tunnel ip-address X.X.X.X gateway Z.Z.Z.Z mask Z.Z.Z.Z
```

- Valider.
- Entrer la commande suivante.

```
(gcap-cli) set network-config management ip-address Y.Y.Y.Y gateway Z.Z.Z.Z mask Z.Z.Z.Z confirm
```

- Valider.

6.2.2.9.5 Exemple pour modifier le GCap sur gatewatcher.com

- Pour modifier le domaine du GCap sur gatewatcher.com :
  - Entrer la commande suivante.

```
(gcap-cli) set network-config domain-name gatewatcher.com
```

  - Valider.

```
Setting hostname/domain name to:
   - Hostname: gcap-int-129-dag
   - Domain name: gatewatcher.com
Do you want to apply this new configuration? (y/N)
```

  - Appuyer sur **y** puis valider.
- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante

```
(gcap-cli) show network-config domain
```

  - Valider.
    Le système affiche le nom du domaine.

```
Current domain name: gatewatcher.com
```

6.2.2.10 password-policy

6.2.2.10.1 Introduction

La commande `password-policy` du sous-groupe `set` permet de définir une politique de mot de passe pour les comptes `setup`, `gviewadm` et `gview`. Cette politique est globale à l'ensemble des utilisateurs.

6.2.2.10.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.2.10.3 Commande

Pour définir les options de complexité du mot de passe :
`(gcap-cli) set password-policy {lowercase-optional|lowercase-required|uppercase-optional|uppercase-required|digits-optional|digit`

Pour activer ou désactiver la politique de contrôle des mots de passe :
`(gcap-cli) set password-policy {disable|enable}`

Pour restaurer la politique par défaut de contrôle des mots de passe :
`(gcap-cli) set password-policy restore-default`

Pour définir la longueur minimale du mot de passe :
`(gcap-cli) set password-policy password-length {8-100}`

Pour définir la durée de validité d'un mot de passe :
`(gcap-cli) set password-policy validity-duration {0|1-3650}`

Pour interdire des mots de passe précédemment utilisés :
`(gcap-cli) set password-policy previous-check {0|1-1000}`

6.2.2.10.4 Exemple pour enlever la contrainte sur les nombres

- Entrer la commande suivante.

```
(gcap-cli) set password-policy digits-optional
```

- Valider.
  Le système affiche le résultat.

```
Rules successfully updated
```

Note :

Pour ne pas avoir de fin de validité, mettre 0 dans le champ `` `Validity duration` ``.
Pour ne pas avoir de vérification des anciens mots de passe, mettre 0 dans le champ `` `Verify last 0 passwords` ``.

6.2.2.10.5 Exemple pour désactiver la politique par défaut de contrôle des mots de passe

- Pour désactiver la politique par défaut de contrôle des mots de passe :
  - Entrer la commande suivante.

```
(gcap-cli) set password-policy disable
```

  - Valider.
    Le système affiche le résultat.

```
Rules successfully updated
```

- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show password-policy
```

  - Valider.
    Le système affiche l'état désactivé du contrôle.

```
No active password policy
```

6.2.2.11 passwords

6.2.2.11.1 Introduction

La commande `passwords` du sous-groupe `set` permet de modifier le mot de passe des utilisateurs setup, gviewadm, gview.

Utilisateur	peut modifier le mot de passe		
	setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

Les mots de passe doivent correspondre à des règles prédéfinies.

Pour plus d'informations sur ces règles, utiliser la commande *show password-policy*.

Important :

Vérifier la configuration du clavier avant de modifier le mot de passe (commande *show keymap*).

6.2.2.11.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.2.11.3 Commande

```
set passwords {setup|gviewadm|gview}
```

6.2.2.11.4 Exemple pour modifier le mot de passe de l'utilisateur actuel (ici setup)

- Entrer la commande suivante.

```
(gcap-cli) set passwords setup
```

- Valider.

```
(current) LDAP Password:
```

- Saisir le mot de passe LDAP puis valider.
  Le système demande le nouveau mot de passe du compte (ici setup).

```
New password:
```

- Saisir le nouveau mot de passe puis valider.
  Le système demande de ressaisir le nouveau mot de passe.

```
Retype new password:
```

- Ressaisir le nouveau mot de passe puis valider.
  Le système informe que le mot de passe a été changé.

```
passwd: password updated successfully
Password changed for user setup
```

6.2.2.11.5 Exemple pour modifier le mot de passe d'un autre utilisateur

- Entrer la commande suivante.

```
(gcap-cli) set passwords gviewadm
```

- Valider.

```
Password complexity rules:
   Minimum different characters between old and new passwords: 2
   Minimum length: 12
   Lowercase character required: yes
   Uppercase character required: yes
   Digit required: yes
   Other character class required: yes
New password:

```

- Saisir le nouveau mot de passe du compte (ici gviewadm) puis valider.
  Le système demande de ressaisir le nouveau mot de passe.

```
Retype new password:
```

- Ressaisir le nouveau mot de passe puis valider.
  Le système informe que le mot de passe a été changé.

```
passwd: password updated successfully
Password changed for user gviewadm
```

6.2.2.12 protocols-selector

Cette commande est supprimée depuis la version 2.5.3.105.

6.2.2.13 session-timeout

6.2.2.13.1 Introduction

La commande `session-timeout` du sous-groupe `set` permet de configurer le temps d'inactivité avant la déconnexion d'une session utilisateur.

Ci-dessous les options de configuration :

- la valeur par défaut est de `5min`
- la valeur `0` permet de désactiver la déconnexion automatique
- la valeur maximale est de `1440min`

La modification de cette configuration est possible à tout moment et n'a aucun impact sur le fonctionnement global du GCap.

6.2.2.13.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.2.13.3 Commande

```
set session-timeout MINUTES
```

6.2.2.13.4 Exemple pour changer la valeur par défaut de la déconnexion automatique via l'utilisateur setup

- Pour changer la valeur par défaut de la déconnexion automatique via l'utilisateur setup :
  - Entrer la commande suivante.

```
(gcap-cli) set session-timeout 1200
```

  - Valider.
    Le système affiche le résultat.

```
Setting session timeout to 1200 mins
Session timeout successfully changed.
```

- Pour vérifier la modification de la valeur :
  - Entrer la commande suivante.

```
(gcap-cli) show session-timeout
```

  - Valider.
    Le système affiche la valeur courante de fin de session.

```
Current session timeout is 1200 mins
```

6.2.2.14 setup-mode

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.2.15 ssh-keys

6.2.2.15.1 Introduction

La commande `ssh-keys` du sous-groupe `set` permet d'ajouter ou de modifier les clés SSH.
Suivant le compte, il est possible de changer uniquement le niveau courant et le niveau inférieur.
L'ajout ou la modification peut se faire soit en ligne de commande soit via l'éditeur de texte Nano.
La modification des clés SSH écrase les anciennes clés. Il faut spécifier les anciennes suivies des nouvelles dans la commande.

Utilisateur	peut modifier le mot de passe		
	setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

Le GCap permet d'avoir jusqu'à 50 utilisateurs différents avec des tailles de clé différentes :

- RSA 2048 ou 4096
- ssh-ed25519
- ecdsa-sha2-nistp256.

6.2.2.15.2 Prérequis

- **Utilisateur :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.2.15.3 Commande

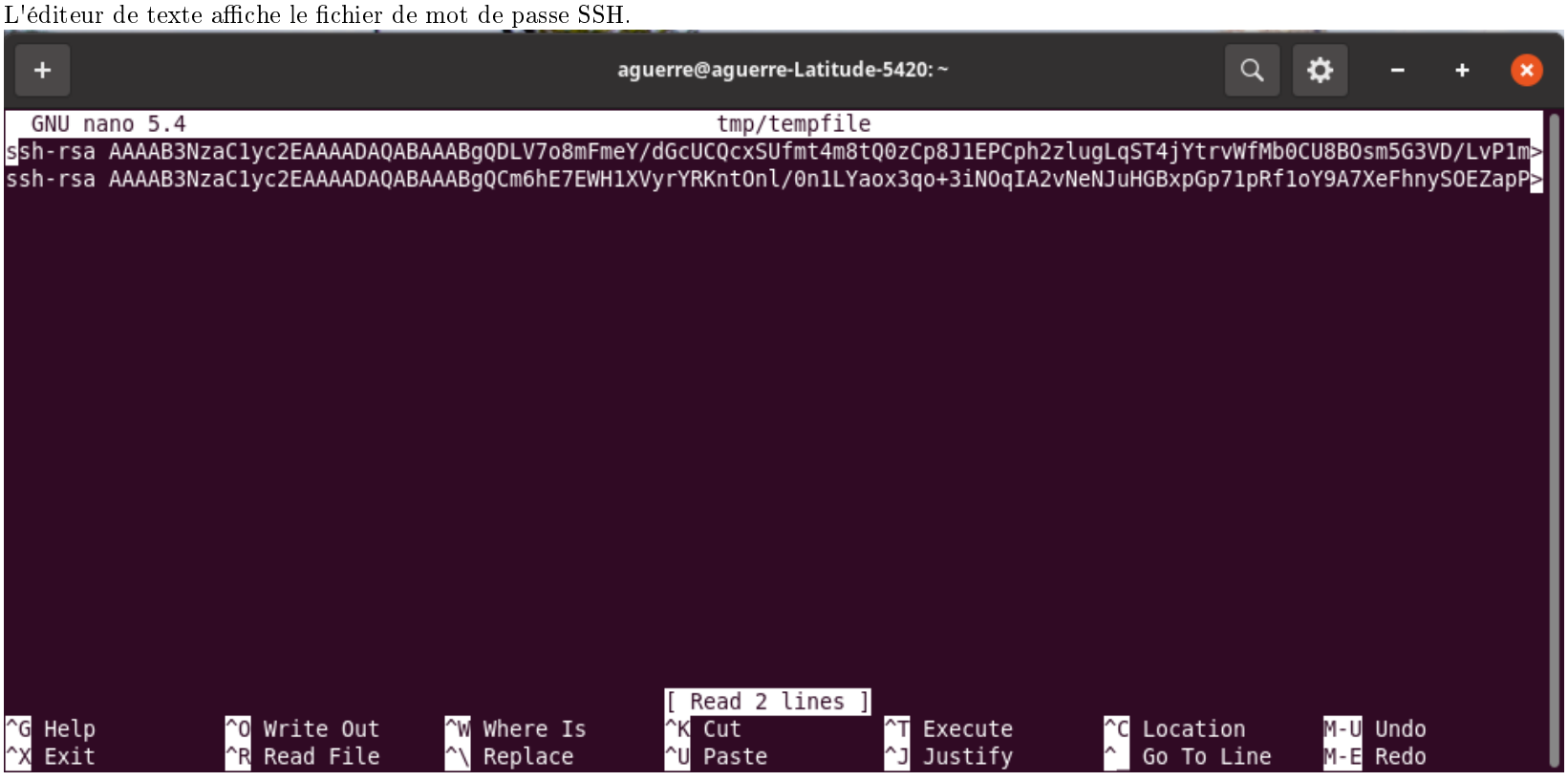
```
set ssh-keys {setup|gviewadm|gview} "ssh-rsa ...\nssh-rsa
```

6.2.2.15.4 Exemple pour utiliser l'éditeur de texte

- Entrer la commande suivante.

```
(gcap-cli) set ssh-keys gview
```

- Valider.
  L'éditeur de texte affiche le fichier de mot de passe SSH.



  Chaque ligne du fichier est une clé SSH et commence par ssh-rsa.
- Pour supprimer une clé, supprimer la ligne.
  Pour changer une clé, modifier une ligne.
  Pour ajouter une clé, ajouter une ligne en commençant par ssh-rsa.
- Pour sortir, appuyer sur **CTRL** + **X**.
- Enregistrer les modifications si besoin.

6.2.2.15.5 Exemple pour ajouter une clé SSH à l'utilisateur setup depuis une connexion avec l'utilisateur setup

- Entrer la commande suivante.

```
(gcap-cli) set ssh-keys setup "ssh-rsa ..."
```

- Valider.

6.2.2.16 advanced-configuration

6.2.2.16.1 high-availability

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.2.16.2 interface-names

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.2.16.3 local-rules

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.2.16.4 mtu (Maximum Transfert Unit)

6.2.2.16.4.1 Introduction

La commande `mtu` du sous-groupe `set advanced-configuration` permet de modifier la valeur en octets de la MTU des interfaces réseau activées (`mon0`, `mon1`, ... `monx`, `gcp0`, `gcp1`, clusters).
Cette valeur doit se trouver entre `1280` et `9000` octets.

> **Note :**
>
> Les fonctionnalités de filtrage XDP ne sont pas supportées lorsque la MTU > 3000.

6.2.2.16.4.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.16.4.3 Commande

```
set advanced-configuration mtu {interface-name}
```

6.2.2.16.4.4 Exemple pour modifier la valeur de la MTU de l'interface `ensp04`

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration mtu mon1 1500
```

- Valider.
  Le système affiche le résultat.

```
Updating Network MTU configuration to:
      - mon1: 1500
```

6.2.2.16.5 packet-filtering

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.2.16.6 rescan-interfaces

6.2.2.16.6.1 Introduction

La commande `rescan-interfaces` du sous-groupe `set advanced-configuration` permet de :

- scanner les interfaces réseau
- synchroniser les interfaces réseau détectées avec les noms prédéfinies dans le système

Cette commande sert notamment lorsque les interfaces sont mal nommées ou quand elles sont dans le désordre : ceci peut arriver dans certains cas de matériels anciens ou mal reconnus.

6.2.2.16.6.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.2.16.6.3 Commande

```
set advanced-configuration rescan-interfaces [no-reboot]
```

6.2.2.16.6.4 Exemple pour scanner les interfaces du GCap sans redémarrer

Note :

Les interfaces étant potentiellement non assignées, les accès via la connexion SSH peut ne pas fonctionner.
Donc seuls les accés physiques ou via l'accès la console de gestion (iDrac) sont possibles.

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration rescan-interfaces no-reboot
```

- Valider.

```
Operation successful.
```

6.2.3 services

6.2.3.1 Commandes services

Ces commandes ont été supprimées depuis la version 2.5.4.0.

6.2.3.2 show

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.3.3 start

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.3.4 status

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.3.5 stop

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.4 system

6.2.4.1 delete-data

6.2.4.1.1 Introduction

La commande `delete-data` du sous-groupe `system` permet de supprimer toutes les données générées par le moteur de détection stockées dans le système de fichiers.

6.2.4.1.2 Prérequis

- **User :** setup
- **Dépendances :**

6.2.4.1.3 Commande

`system delete-data`

6.2.4.1.4 Example of deleting data

- Entrer la commande suivante.

```
(gcap-cli) system delete-data confirm
```

- Valider.
  toutes les données seront effacées et le GCap redémarrera.
  La connexion en SSH va être interrompue.

6.2.4.2 reload-drivers

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.4.3 restart

6.2.4.3.1 Introduction

La commande `restart` du sous-groupe `system` permet de redémarrer le GCap.
Si avant le démarrage, le moteur de détection est activé (état **UP**), il le sera après le démarrage.
Si avant le démarrage, le GCap est appairé avec le GCenter, il le sera après le démarrage.

6.2.4.3.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** aucune

6.2.4.3.3 Commande

`system restart`

6.2.4.3.4 Exemple pour redémarrer un GCap

- Entrer la commande suivante.

```
(gcap-cli) system restart
```

- Valider.
  La connexion en SSH va être interrompue.

6.2.4.4 shutdown

6.2.4.4.1 Introduction

La commande `shutdown` du sous-groupe `system` permet d'éteindre le GCap.

Important :

Une fois éteint, le GCap devra être remis sous tension via l'accès distant par l'iDRAC.

6.2.4.4.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** le moteur de détection doit être à l'arrêt

---

6.2.4.4.3 Commande

```
system shutdown
```

6.2.4.4.4 Exemple pour éteindre un GCap

- Entrer la commande suivante.

```
(gcap-cli) system shutdown
```

- Valider.

6.2.4.5 unlock

6.2.4.5.1 Introduction

La commande `unlock` du sous-groupe `system` permet de réinitialiser le verrouillage des comptes `gview`, `gviewadm` et `setup` suite à des tentatives d'authentification infructueuses.

6.2.4.5.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :** N/A

6.2.4.5.3 Commande

`system unlock {setup|gview|gviewadm}`

6.2.4.5.4 Exemple pour déverrouiller le compte setup

- Entrer la commande suivante.

```
(gcap-cli) system unlock setup
```

- Valider.
  Le système affiche le résultat.

```
User setup successfully unlocked
```

6.2.4.6 upgrade

6.2.4.6.1 Introduction

La commande `upgrade` du sous-groupe `system` permet de faire passer la sonde à une version supérieure.

6.2.4.6.2 Prérequis

- **User :** setup
- **Dépendances :**
- le moteur de détection doit être à l'arrêt

6.2.4.6.3 Commande

`system upgrade`

6.2.4.6.4 Exemple de mise à niveau d'un GCap

- Entrer la commande suivante pour lister les packages disponibles sur le GCenter.

```
(gcap-cli) system upgrade list
```

- Valider.
- Entrer la commande suivante pour mettre à niveau la sonde.

```
(gcap-cli) system upgrade apply '[package_name]' confirm
```

- Valider.
  À la fin de l'opération, la sonde va redémarrer
  La connexion en SSH va être interrompue.

6.2.5 monitoring-engine

6.2.5.1 Introduction

Le moteur de détection de la sonde GCap capture le trafic réseau et fait l'analyse afin de générer les événements de sécurité (alertes et métadonnées).
La commande `monitoring-engine` permet :

- de démarrer le moteur de détection
- d'arrêter le moteur de détection
- de visualiser l'état du moteur de détection

Note :

Pour cette commande, il existe des options avancées (voir la section *set monitoring-engine*).
Une fois le moteur de capture activé, certaines commandes de configuration du GCap ne sont plus accessibles.
Cette information est indiquée par le champ "Dépendances" dans le descriptif de chacune des commandes.
Il faut désactiver le moteur de capture pour les rendre à nouveau accessibles.
Si la configuration du GCap est modifiée via le GCenter, le moteur de détection est rechargé automatiquement.
Si l'appliance GCap est redémarrée, il n'y a aucun impact sur l'état du moteur de détection.

6.2.5.2 Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances** :
  - Ajouter l'IP du GCenter (`set gcenter-ip`).
  - Appairer le GCap et le GCenter.
  - Choisir la version de compatibilité GCenter.
  - Activer au moins une interface de capture.

Note :

Si l'option `sanity-checks` est sur `enable`, le moteur de détection ne démarre qu'après avoir vérifié qu'au moins une interface de capture `monx` a été activée et qu'un câble est connecté.

6.2.5.3 Commande

`monitoring-engine {status|start|stop}`

6.2.5.4 Exemple pour afficher l'état du moteur de détection

- Entrer la commande suivante.

```
(gcap-cli) monitoring-engine status
```

- Valider. Le système affiche l'état du moteur :

```
Detection engine is down
```

Signification :
- Detection engine `down` : signifie que l'état du moteur est inactif
- Detection engine `up` : signifie que l'état du moteur est actif

---

6.2.5.5 Exemple pour démarrer le moteur de détection

Le système affiche l'invite de commande suivant :

```
Monitoring DOWN gcap-name (gcap-cli)
```

L'invite de commande indique l'état du moteur de détection : ici il est arrêté.

- Entrer la commande suivante.

```
(gcap-cli) monitoring-engine start
```

- Valider.
- Vérifier l'état du moteur de détection :
  Le système affiche l'invite de commande suivant :

```
[Monitoring UP] gcap-name (gcap-cli)
```

L'invite de commande indique l'état du moteur de détection : ici il est démarré.

6.2.5.6 Exemple pour arrêter le moteur de détection

Le système affiche l'invite de commande suivant :

```
[Monitoring UP] gcap-name (gcap-cli)
```

L'invite de commande indique l'état du moteur de détection : ici il est démarré.

- Entrer la commande suivante.

  ```
  (gcap-cli) monitoring-engine stop
  ```

- Valider.
- Vérifier l'état du moteur de détection :

  ```
  Monitoring DOWN gcap-name (gcap-cli)
  ```

  L'invite de commande indique l'état du moteur de détection : ici il est arrêté.

6.2.6 pairing

6.2.6.1 Introduction

La commande `pairing` permet de configurer l'appairage IPsec avec le GCenter.

6.2.6.2 Prérequis

- **Utilisateur :** setup
- **Dépendances :**
  - le moteur de détection doit être à l'arrêt
  - les interfaces réseaux doivent être correctement configurées
  - l'adresse IP du GCenter doit être renseignée via la commande `set gcenter-ip`
  - la compatibilité du GCenter doit être renseignée via la commande `set compatibility-mode`

6.2.6.3 Commande

`pairing {fingerprint FINGERPRINT otp OTP|reload-tunnel}`

6.2.6.4 Exemple pour appairer un GCap version 2.5.4.0 avec un GCenter

- récupérer le FQDN (hostname + domain) du GCap via la commande `show status`.

```
(gcap-cli) show status
```

- se rendre sur l'interface WEB du GCenter pour ajouter le nom complet FQDN (Fully Qualified Domain Name) de la sonde.
  Pour plus d'informations, se référer à la documentation du GCenter.
- renseigner l'empreinte SSH du GCenter dans la commande `pairing`.
- renseigner l'OTP généré dans la commande `pairing`.

```
(gcap-cli) pairing fingerprint XXX otp XXX
```

- valider l'appairage avec la commande `show status`.

```
(gcap-cli) show status
```

Pour plus d'informations sur cette procédure, se référer à la *Procédure d'appairage entre un GCap et un GCenter*.

6.2.7 unpair

6.2.7.1 Introduction

La commande `unpair`permet de supprimer une configuration liée à l'appairage (configuration IPSec).

6.2.7.2 Prérequis

- **User :** setup

6.2.7.3 Commande

`unpair`

6.2.7.4 Exemple de désappariement

- Entrer la commande suivante

```
(gcap-cli) unpair
```

- Valider.
  Le système affiche **Operation successful**.
  Pour plus d'informations sur l'appairage, se référer à la *Procédure d'appairage entre un GCap et un GCenter*.

6.2.8 replay

6.2.8.1 Introduction

Un fichier avec l'extension pcap est un fichier dans lequel le trafic réseau brut a été capturé.
La commande `replay` permet :

- de lister les fichiers pcap disponibles
- demander au moteur de détection d'analyser ce trafic réseau pour reconstruire les paquets contenus dans ce flux
- de le rejouer avec possibilité de modifier la vitesse par rapport à celle de la capture initiale

Ci-dessous les options de configuration :

- **Lister les fichiers pcap disponibles**
  - `list`
- **Choisir le nom du fichier pcap**
  - `pcap`
- **Choisir la vitesse de rejeu**
  - `speed`
- **Choisir un rejeu en boucle**
  - `forever`

Note :

L'ajout de pcap n'est possible qu'avec les versions compatibles du logiciel du GCenter.
L'ajout de pcap est uniquement possible en ligne de commande avec le compte *root*, sinon se rapprocher du service support de Gatewatcher.

6.2.8.2 Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances :**
  - le moteur de détection est démarré (`UP`)
  - l'interface `monvirt` est activée
  - au moins un fichier pcap doit être présent dans le répertoire pcap

---

6.2.8.3 Commande

`replay pcap name.pcap {speed FACTOR} {forever}`

`replay list`

Commandes disponibles :

- `forever` : signifie de rejouer le fichier pcap jusqu'à appui sur **CTRL + C**
- `speed x` : x est un nombre qui spécifie la vitesse du rejeu du fichier pcap (X fois la vitesse nominale)

6.2.8.4 Exemple pour afficher la liste des fichiers pcap disponibles

- Entrer la commande suivante.

```
[Monitoring UP] GCap-lab (gcap-cli) replay list
```

- Valider.

```
Available pcaps are:

test-dga-v1.pcap
test-malcore-v1.pcap
test-powershell-v1.pcap
test-shellcode-v1.pcap
test-sigflow-v1.pcap
```

La liste des fichiers pcap présents est affichée.
Les fichiers listés ci-avant ont été installés lors d'une nouvelle installation ou lors d'une mise à jour si aucun autre fichier pcap n'est présent sur le GCap.
Chacun de ces fichiers permet de tester un moteur différent.

Note :

Pour le fichier test-sigflow-v1.pcap, il est possible de rejouer ce fichier pcap mais :

- si l'une des 2 signatures suivantes est présente dans le ruleset appliqué au Gcap alors les alertes au niveau du Gcenter sont visibles :
  - sid :2020716 => ET POLICY Possible External IP Lookup ipinfo.io
  - sid :2013028 ==> ET POLICY curl User-Agent Outbound
- si aucune de ces signatures n'est présente dans le ruleset alors il n'y a pas d'alerte au niveau du GCenter donc on ne saura pas si le moteur sigflow fonctionne correctement

---

6.2.8.5 Exemple pour rejouer un fichier pcap avec la vitesse de capture

- Entrer la commande suivante.

```
(gcap-cli) replay pcap name.pcap speed 4
```

- Valider.

```
Test start: 2022-05-13 14:49:31.287043 ...
Actual: 38024 packets (43981183 bytes) sent in 5.00 seconds
Rated: 8795627.9 Bps, 70.36 Mbps, 7604.27 pps
Actual: 58291 packets (66785902 bytes) sent in 10.00 seconds
Rated: 6678332.4 Bps, 53.42 Mbps, 5828.87 pps
Actual: 83666 packets (95744520 bytes) sent in 15.02 seconds
Rated: 6374049.4 Bps, 50.99 Mbps, 5569.93 pps
Actual: 110051 packets (125880214 bytes) sent in 20.02 seconds
Rated: 6285776.9 Bps, 50.28 Mbps, 5495.35 pps
Actual: 147566 packets (169410025 bytes) sent in 25.02 seconds
Rated: 6769298.3 Bps, 54.15 Mbps, 5896.45 pps
Actual: 169247 packets (193816539 bytes) sent in 30.03 seconds
Rated: 6453918.8 Bps, 51.63 Mbps, 5635.77 pps
Actual: 195575 packets (223882527 bytes) sent in 35.06 seconds
Rated: 6385197.7 Bps, 51.08 Mbps, 5577.85 pps
Actual: 221886 packets (253884171 bytes) sent in 40.09 seconds
Rated: 6331801.8 Bps, 50.65 Mbps, 5533.77 pps
Actual: 260874 packets (298969988 bytes) sent in 45.11 seconds
Rated: 6627011.6 Bps, 53.01 Mbps, 5782.57 pps
Actual: 280646 packets (321206175 bytes) sent in 50.19 seconds
```

(suite sur la page suivante)

(suite de la page précédente)

```
Rated: 6399274.4 Bps, 51.19 Mbps, 5591.20 pps
Test complete: 2022-05-13 14:50:24.974433
Actual: 300745 packets (344377408 bytes) sent in 53.68 seconds
Rated: 6414493.3 Bps, 51.31 Mbps, 5601.78 pps
Flows: 3774 flows, 70.29 fps, 296049 flow packets, 4696 non-flow
Statistics for network device: injectiface
    Successful packets:        300745
    Failed packets:            0
    Truncated packets:         0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN):  0
```

Le système affiche toutes les cinq secondes environ les compteurs :

- débit en Bps
- débit en Mbps
- débit en pps (paquets)

puis les compteurs finaux.

6.2.9 help

Pour obtenir de l'aide concernant les commandes disponibles, il est possible de :

- la préfixer par `help` (exemple `help show config-files`)
- suffixer la commande par `?` (exemple `show config-files ?`)

L'aide permet d'afficher les commandes disponibles et un descriptif de celle-ci dans le contexte courant.

6.2.9.1 Utilisation de ?

La commande `?` peut être utilisée :

- seule : dans ce cas, il a la même fonction que la commande `help`
- après la commande pour laquelle l'aide doit être affichée : suffixation

---

6.2.9.1.1 Prérequis pour ?

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.9.1.2 Commande ?

- `(gcap-cli) ?` pour afficher la liste des commandes accessibles
- `(gcap-cli) show status ?` pour afficher l'aide de la commande `status` de l'ensemble `show`

6.2.9.1.3 Utilisation de ? de suffixation

Pour lister les fichiers de configurations accessibles via la CLI :

- utiliser la commande `show network` suivi de `?`

```
(gcap-cli) show network ?
```

- Valider.
  Le système affiche les informations suivantes :

```
(gcap-clInspect configurations
==================================

Available commands:
   - configuration: Show current network configuration in JSON format
   - tunnel: Show current configuration for tunnel interface
   - management: Show current configuration for management interface
   - hostname: Show current configuration for hostname
   - domain: Show current configuration for domain
```

6.2.9.2 Utilisation de `help`

La commande `help` peut être utilisée :

- seule : dans ce cas, le système affiche les commandes accessibles dans le niveau actuel
- avant la commande pour laquelle l'aide doit être affichée : préfixation
- après la commande pour laquelle l'aide doit être affichée mais il faut saisir `--help` ou `-h`

6.2.9.2.1 Prérequis pour `help`

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.9.2.2 Commande `help`

- `(gcap-cli) help` pour afficher la liste des commandes accessibles
- `(gcap-cli) show status --help` pour afficher l'aide de la commande `status` de l'ensemble `show`
- `(gcap-cli) help show status` pour afficher l'aide de la commande `status` de l'ensemble `show`

6.2.9.2.3 Utilisation de `help` seul

- Entrer la commande suivante.

```
(gcap-cli) help
```

- Valider.
  Le système affiche les informations suivantes :

```
CLI entrypoint
==============

Available commands:
 - show: Show system configuration
 - set: Modify system configuration
 - services: Manage service
 - system: Handle system operations
 - monitoring-engine: Handle Monitoring Engine
 - help: Display command help message
 - colour: Handle colour support for current CLI session
 - exit: Exit configuration tool
```

6.2.9.2.4 Exemple de préfixation : afficher les commandes disponibles dans le contexte monitoring-engine depuis la racine de gcap-cli

- Entrer la commande suivante.

```
(gcap-cli) help monitoring-engine
```

- Valider.
  Le système affiche les informations suivantes :
  cas 1

```
   Available commands:
       - start: Start the Monitoring Engine
       - status: View current Monitoring Engine status
```

  Dans ce cas, le moteur peut être démarré

ou

cas 2

```
Available commands:
   - status: View current Monitoring Engine status
```

Dans ce cas, les prérequis pour démarrer le moteur ne sont pas réunis.

6.2.9.2.5 Exemple de suffixation : afficher les informations d'une commande

- Entrer la commande suivante.

```
(gcap-cli system) shutdown --help
```

- Valider.
  Le système affiche les informations suivantes :

```
Shutdown GCap
```

6.2.10 colour

6.2.10.1 Introduction

La commande `colour` permet d'activer ou désactiver les couleurs dans les sorties de l'instance en cours de gcap-cli.

6.2.10.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.10.3 Commande

`colour {disable|enable}`

6.2.10.4 Exemple pour afficher des statuts des services avec de la couleur

- Entrer la commande suivante.

```
(gcap-cli) colour enable
```

- Valider.
  Le système affiche ensuite les informations avec de la couleur.

```
    <pre>
    <span style="color:green;">[Monitoring UP]</span> <span style="color:red;">GCap</span><span style="color:blue;">␣
↪(gcap-cli)</span> service status
    <span style="color:green;">up</span> - Service eve-generation
    <span style="color:green;">up</span> - Service eve-upload
    <span style="color:green;">up</span> - Service file-extraction
    <span style="color:green;">up</span> - Service file-upload
    <span style="color:red;">down</span> - Service filter-fileinfo
    <span style="color:red;">down</span> - Service eve-compress

    <span style="color:green;">[Monitoring UP]</span> <span style="color:red;">GCap</span><span style="color:blue;">␣
↪(gcap-cli)</span> colour disable
    </pre>
```

6.2.10.5 Exemple pour afficher des états des services sans la couleur

- Entrer la commande suivante.

```
(gcap-cli) colour disable
```

- Valider.
  Le système affiche ensuite les informations sans la couleur voir (exemple ci-après).

```
<pre>
[Monitoring UP] GCap (gcap-cli) service status

up - Service eve-generation
up - Service eve-upload
up - Service file-extraction
up - Service file-upload
down - Service filter-fileinfo
down - Service eve-compress
</pre>
```

6.2.11 gui (deprecated)

Cette commande a été supprimée depuis la version 2.5.4.0.

6.2.12 exit

6.2.12.1 Introduction

La commande `exit` permet :

- de revenir à la racine (gcap cli) si le prompt est ailleurs dans l'arborescence
- de quitter la session SSH si le prompt est déjà à la racine (gcap-cli)

Le raccourci **CTRL** + **D** permet d'appeler la commande `exit`.

6.2.12.2 Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :** N/A

6.2.12.3 Commande

```
exit
```

6.2.12.4 Exemple pour sortir du contexte "set protocols-selector logging"

- Entrer la commande suivante.

```
(gcap-cli set protocols-selector logging) exit
```

- Valider.
  Le prompt a changé et montre le contexte racine :

```
(gcap-cli)
```

6.2.12.5 Exemple pour sortir de la CLI

- Entrer la commande suivante.

```
(gcap-cli) exit
```

- Valider.

Chapitre 7

Métriques

7.1 Liste des métriques comparaison version 2.5.3.105 vs 2.5.3.104

La version 2.5.3.105 utilise de nouveaux compteurs et en renomme d'autres.
Les tableaux ci après comparent les compteurs des versions 2.5.3.105 vs 2.5.3.104.

7.1.1 Métriques internes version 2.5.3.105 vs 2.5.3.104

Nom sur version V105	Nom sur version V104	Ecart entre les versions
netdata.runtime_proc_net_dev		compteur rajouté avec la V105
netdata.runtime_xdp_filter	netdata.runtime_xdp_filter_local	compteur renommé avec la V105
netdata.runtime_disk_usage	netdata.runtime_disk_usage_local	compteur renommé avec la V105
netdata.runtime_proc_meminfo		compteur rajouté avec la V105
netdata.runtime_proc_loadavg		compteur rajouté avec la V105
netdata.runtime_proc_uptime		compteur rajouté avec la V105
netdata.runtime_proc_vmstat		compteur rajouté avec la V105
netdata.runtime_proc_stat		compteur rajouté avec la V105
netdata.runtime_high_availability		compteur rajouté avec la V105
netdata.runtime_sys_block		compteur rajouté avec la V105
netdata.runtime_proc_net_softnet_stat		compteur rajouté avec la V105
netdata.runtime_suricata	netdata.runtime_suricata_local	compteur renommé avec la V105
netdata.runtime_codebreaker	netdata.runtime_codebreaker_local	compteur renommé avec la V105
netdata.web_thread[1-6]_cpu		compteur renommé avec la V105
netdata.plugin_diskspace_dt		compteur renommé avec la V105
netdata.plugin_diskspace		compteur renommé avec la V105
	netdata.plugin_proc_cpu	compteur renommé avec la V105
	netdata.plugin_proc_modules	compteur renommé avec la V105

7.1.2 Informations systèmes version 2.5.3.105 vs 2.5.3.104

Nom sur version V105	Nom sur version V104	Ecart entre les versions
disk_space.<partition>		compteur rajouté avec la V105
disk_inodes.<partition>		compteur rajouté avec la V105
disk_usage.mountpoint.<mount>		compteur rajouté avec la V105
sys_block.blocks.\<disque>		compteur rajouté avec la V105
proc_stat.processes	system.processes	compteur renommé avec la V105
proc_stat.interrupts	system.intr	compteur renommé avec la V105
proc_stat.cpu.cpu(0-n)	system.cpu.cpu(0-n)	compteur renommé avec la V105
proc_vmstat.swapio	system.swapio	compteur renommé avec la V105
proc_vmstat.pgpio	system.pgpgio	compteur renommé avec la V105
proc_vmstat.pagefaults	mem.pgfaults	compteur renommé avec la V105
proc_uptime.uptime	system.uptime	compteur renommé avec la V105
proc_loadavg.Load_average	system.load	compteur renommé avec la V105
proc_loadavg.Active_processes	system.active_processes	compteur renommé avec la V105
proc_meminfo.RAM	system.ram	compteur renommé avec la V105
proc_meminfo.available	mem.available	compteur renommé avec la V105
proc_meminfo.swap	system.swap	compteur renommé avec la V105
proc_meminfo.kernel	mem.kernel	compteur renommé avec la V105
proc_meminfo.hugepages	mem.transparent_hugepages	compteur renommé avec la V105
	system.io	compteur supprimé avec la V105
	system.net	compteur supprimé avec la V105

7.1.3 Informations réseau version 2.5.3.105 vs 2.5.3.104

Nom sur version V105	Nom sur version V104	Ecart entre les versions
proc_net_dev.net_drops.<iface>	proc_net_dev_local.net_drops.<iface>	compteur renommé avec la V105
proc_net_dev.net_drops.<iface>	proc_net_dev_local.net_errors.<iface>	compteur renommé avec la V105
proc_net_dev.net_pkts.<iface>	proc_net_dev_local.net_pkts.<iface>	compteur renommé avec la V105
proc_net_dev.net.<iface>	proc_net_dev_local.net.<iface>	compteur renommé avec la V105
proc_net_softnet_stat.cpu[0-n].sched		compteur rajouté avec la V105
proc_net_softnet_stat.cpu[0-n].packets		compteur rajouté avec la V105
proc_net_softnet_stat.summed.sched		compteur rajouté avec la V105
proc_net_softnet_stat.summed.packets		compteur rajouté avec la V105

7.1.4 Informations appliance et détection version 2.5.3.105 vs 2.5.3.104

Nom sur version V105	Nom sur version V104	Ecart entre les versions
high_availability.ha_status		compteur rajouté avec la V105
high_availability.leader_status		compteur rajouté avec la V105
high_availability.last_status		compteur rajouté avec la V105
high_availability.health_status		compteur renommé avec la V105
xdp_filter.dropped_bytes		compteur rajouté avec la V105
xdp_filter.dropped_packets		compteur rajouté avec la V105
xdp_filter.bypassed_half_flows		compteur rajouté avec la V105
codebreaker.shellcode_samples	codebreaker_local.shellcode_samples	compteur renommé avec la V105

7.2 Liste des métriques disponibles à partir de la version 2.5.3.105

7.2.1 Métriques internes

Nom	Dimensions Unité	Commentaires
netdata.runtime_proc_net_dev	run time ms	Temps d'exécution du script de collecte d'information sur les interfaces
netdata.runtime_xdp_filter	run time ms	Temps d'exécution du script de collecte d'information sur les filtres XDP
netdata.runtime_disk_usage	run time ms	Temps d'exécution du script de collecte d'information sur l'utilisation des disques
netdata.runtime_proc_meminfo	run time ms	Temps d'exécution du script de collecte d'information sur l'utilisation de la mémoire
netdata.runtime_proc_loadavg	run time ms	Temps d'exécution du script de collecte d'information sur la charge du GCap
netdata.runtime_proc_uptime	run time ms	Temps d'exécution du script de collecte d'information sur l'uptime
netdata.runtime_proc_vmstat	run time ms	Temps d'exécution du script de collecte d'information sur la mémoire virtuelle
netdata.runtime_proc_stat	run time ms	Temps d'exécution du script de collecte d'information sur le détail d'utilisation CPU
netdata.runtime_high_availability	run time ms	Temps d'exécution du script de collecte d'information sur la haute disponibilité
netdata.runtime_sys_block	run time ms	Temps d'exécution du script de collecte d'information sur les I/O disques
netdata.runtime_proc_net_softnet_stat	run time ms	Temps d'exécution du script de collecte d'information sur la stack réseau
netdata.runtime_suricata	run time ms	Temps d'exécution du script de collecte d'information sur Sigflow
netdata.runtime_codebreaker	run time ms	Temps d'exécution du script de collecte d'information sur Codebreaker
netdata.web_thread[1-6]_cpu	user system ms/s	Temps d'utilisation CPU des threads netdata
netdata.plugin_diskspace_dt	duration ms/run	Temps d'exécution du script de collecte d'information sur l'espace disque
netdata.plugin_diskspace	user system ms/s	Temps d'utilisation CPU du plugin de collecte d'information sur l'espace disque

7.2.2 Détails des compteurs de Sigflow

7.2.2.1 Détail du compteur Alerts - Nombre d'alertes Sigflow trouvées

Nom	Dimensions	Commentaires
suricata.alert	Alerts.value	Nombre d'alertes Sigflow trouvées

7.2.2.2 Détail des compteurs Codebreaker samples - Fichiers analysés par Codebreaker

Nom	Dimensions	Commentaires
codebreaker.shellcode_samples	plain encoded	Shellcodes détectés sans encodage / Shellcodes détectés avec encodage
codebreaker.powershell_samples	Powershell.value	Nombre de scripts Powershell malicieux détectés

7.2.2.3 Détail des compteurs Protocols - Listes des protocoles vus par Sigflow

Les compteurs suivants affichent le nombre d'événements observés par Sigflow à propos de chaque protocole.

Nom	Dimensions	Unité	Commentaires
suricata.dhcp	DHCP.value	nombre	protocole DHCP
suricata.dnp3	DNP3.value	nombre	protocole DNP3
suricata.dns	DNS.value	nombre	protocole DNS
suricata.ftp	FTP.value	nombre	protocole FTP
suricata.http	HTTP.value	nombre	protocole HTTP
suricata.http2	HTTP2.value	nombre	protocole HTTP2
suricata.ikev2	IKEv2.value	nombre	protocole IKEv2
suricata.krb5	krb5.value	nombre	protocole KRB5
suricata.mqtt	MQTT.value	nombre	protocole MQTT
suricata.netflow	NETFLOW.value	nombre	protocole NETFLOW
suricata.nfs	NFS.value	nombre	protocole NFS
suricata.rdp	RDP.value	nombre	protocole RDP
suricata.rfb	RFB.value	nombre	protocole RFB
suricata.sip	SIP.value	nombre	protocole SIP
suricata.smb	SMB.value	nombre	protocole SMB
suricata.smtp	SMTP.value	nombre	protocole SMTP
suricata.snmp	SNMP.value	nombre	protocole SNMP
suricata.ssh	SSH.value	nombre	protocole SSH
suricata.tftp	TFTP.value	nombre	protocole TFTP
suricata.tls	TLS.value	nombre	protocole TLS
suricata.tunnel	tunnel.value	nombre	protocole tunnel

7.2.2.4 Détail des compteurs Detection Engine Stats - Statistique de Sigflow (monitoring-engine)

Nom	Dimensions	Commentaires
suricata.Status	alive.value	Etat du container Sigflow et du moteur de detection (boolean)
suricata.total	total.value	Nombre total d'événements observés
suricata.fileinfo	• extracted • sent • duplicated	• Nombre de fichiers extraits • Nombre de fichiers envoyés • Nombre de fichiers dupliqués
suricata.received_packets	• ReceivedPackets.value • DroppedPackets.value	• Nombre de paquets capturés • Nombre de paquets ignorés
suricata.rules	• RulesLoaded.value • RulesFailed.value	• Nombre de règles chargées et validées • Nombre de règles qui n'ont pas pu être chargées
suricata.tcp_sessions	TcpSessions.value	Nombre de sessions TCP observées par Sigflow
suricata.tcp_pkt_on_wrong_thread	TcpPktOnWrongThread.value	Misrouted packets par Sigflow
suricata.flows	• FlowTCP.value • FlowUDP.value	• Nombre de sessions TCP observées • Nombre de sessions UDP observées

7.2.3 Détails des compteurs de statistiques et des informations de santé du GCap.

7.2.3.1 Détails des compteurs de quotas

Nom	Dimensions	Commentaires
quotas.uid.block	• block.used • block.soft_limit • block.hard_limit	• Nombre de blocks utilisés • Limite logicielle • Limite matérielle
quotas.uid.file	• file.used • file.soft_limit • file.hard_limit	• Nombre de fichiers utilisés • Limite logicielle • Limite matérielle
quotas.uid.grace	• grace.block • grace.file	• Temps de grâce pour les blocks • Temps de grâce pour les fichiers

---

7.2.3.2 Détails des compteurs cpu_stats - Statistiques sur le processeur

Nom	Dimensions	Unité	Commentaires
proc_stat.interrupts	• interrupts	• intr/s	• Nombre d'interruptions par seconde
proc_stat.processes	• running • blocked	• processes	• Etat des processus
proc_stat.cpu.cpu[0-n]	• softirq • irq • user • system • nice • iowait • idle	• pourcentage	• Pourcentage d'utilisation du CPU

7.2.3.3 Informations systèmes

Nom	Dimensions	Unité	Commentaires
sys_block.blocks.<disque>	read written	bytes	I/O sur le disque <**disque**>
proc_uptime.uptime	uptime.uptime	seconds	System uptime
disk_inodes.<partition>	avail used reserved for root	inodes	Utilisation des inodes de la partition <partition>
xdp_filter.dropped_bytes	dropped_bytes	bytes	Volume droppé par XDP
xdp_filter.dropped_packets	dropped_packets	pkts	Paquets droppés par XDP
xdp_filter.bypassed_half_flows	bypassed_half_flows	half flows	Nombre de demi-flux droppé par XDP

7.2.3.4 Détails des Compteurs high_availability - Informations sur la haute disponibilité (HA)

Nom	Dimensions	Unité	Commentaires
high_availability.ha_status	ha.status	boolean	HA activée (1) ou non (0) (1) ou non (0)
high_availability.leader_status	ha.health_status	boolean	Etat du nœud (0 : slave ou non configuré / 1 : leader)
high_availability.health_status	ha.health_status	boolean	Capacité du nœud à devenir leader (0 : non ou non configuré / 1 : OK)
high_availability.last_received_status	ha.last_status	seconds	Durée depuis le changement d'état

---

7.2.3.5 Détails des compteurs interfaces - Statistiques sur les interfaces réseaux

Nom	Dimensions	Unité	Commentaires
proc_net_dev.net.**<iface>**	• received • sent	bytes	Trafic sur l'interface <**iface**>
proc_net_dev.net_drops.**<iface>**	• rx drops • tx drops	pkts	Nombre de paquets perdus sur l'interface <**iface**>
proc_net_dev.net_errors.**<iface>**	• rx errors • tx errors	pkts	Nombre de paquets en erreur sur l'interface <**iface**>
proc_net_dev.net_pkts.**<iface>**	• received • sent	pkts	Nombre de paquets sur l'interface <**iface**>

7.2.3.6 Détails des compteurs loadavg - Statistiques sur la charge moyenne du GCap

Nom	Dimensions	Commentaires
proc_loadavg.Load_average	• load.load1 • load.load5 • load.load15	• Charge moyenne de la dernière minute • Charge moyenne sur les cinq dernières minutes • Charge moyenne sur les quinze dernières minutes
proc_loadavg.Active_processes	active_processes.active	Nombre de processus actifs

---

7.2.3.7 Détails des compteurs meminfo - Statistiques sur la mémoire vive

Nom	Dimensions	Commentaires
suricata.memuse	• MemUseTCP.value • MemUseTCPReassembly • MemUseFlow.value • MemUseHTTP.value • MemUseFTP.value	• TCP memory • TCP reassembly memory • Flows memory • HTTP memory • FTP memory
suricata.memcap	• MemCapTCPSession.value • MemCapTCPSegment.value • MemCapFlow.value • MemCapHTTP.value • MemCapFTP.value	• TCP session allocation failures • TCP segment allocation failures • Flow allocation failures • HTTP allocation failures • FTP allocation failures
proc_meminfo.ram	• free • used • cached • bufferse	• Mémoire inutilisée en kilo-octets • Mémoire utilisée • Mémoire utilisée par le cache • Mémoire utilisée par des opérations
proc_meminfo.available	available	Mémoire physique totale en kilo-octets
proc_meminfo.swap	• swap_free • swap_used • swap_cached	• fichier d'échange (swap) disponible • fichier échange (swap) utilisée • fichier d'échange (swap) servant au cache
proc_meminfo.kernel	• kernel.slab • kernel.kernel_stack • kernel.page_tables • kernel.v_malloc_used	• Mémoire utilisée par les structures de données du noyau • Mémoire utilisée par les allocations de la pile du noyau • Mémoire utilisée pour la gestion des pages • Mémoire utilisée par les grandes zones de mémoire allouées par le noyau
proc_meminfo.hugepages	• hugepages_free • hugepages_used • hugepages.surplus • hugepages.reserved	• Nombre de huge pages transparentes disponibles • Nombre de huge pages transparentes utilisées • Nombre de huge pages transparentes en surplus • Nombre de huge pages transparentes réservées

7.2.3.8 Détails des compteurs numastat - Statistiques sur les nœuds NUMA

Nom	Dimensions	Unité	Commentaires
numa_stat	numa_hit	MiB	Mémoire allouée avec succès dans ce nœud comme prévu
	numa_stat	MiB	• Mémoire allouée dans ce nœud en dépit des préférences de processus • Chaque numa_miss a un numa_foreign dans un autre nœud
	numa_foreign	MiB	Mémoire prévu pour ce nœud, mais actuellement allouée dans un nœud différent
	other_node	MiB	Mémoire allouée dans ce nœud alors qu'un processus fonctionnait dans un autre nœud
	interleave_hit	MiB	Mémoire entrelacée allouée avec succès dans ce nœud
	local_node	MiB	Mémoire allouée dans ce nœud alors qu'un processus fonctionnait dessus

7.2.3.9 Détails des compteurs softnet - Statistiques sur les paquets reçus en fonction des cœurs de processeurs

Nom	Dimensions	Unité	Commentaires
proc_net_softnet_stat.cpu[0-n].packets	• Processed • Dropped • Flow limit count • Process queue lengths	pkts	Paquets traités sur le cpu concerné
proc_net_softnet_stat.cpu[0-n].sched	• Received RPS (IPI schedules) • Time squeeze	events	événements de la stack réseau sur le cpu concerné
proc_net_softnet_stat.summed.packets	• Processed • Dropped • Flow limit count • Input/Process queue lengths	pkts	Paquets traités par la pile réseau

7.2.3.10 Détails des compteurs virtualmemory - Information sur l'espace d'échange (swap)

Nom	Dimensions	Unité	Commentaires
proc_vmstat.swapio	• in • out	pkts	I/O swap
proc_vmstat.pagefaults	• minor • major	faults/s	Memory Page Faults /s

7.3 Récupération des métriques

Les métriques du GCap sont mises à disposition au travers de l'instance Netdata hébergée sur le GCenter.
Afin de connaître les différentes méthodes d'accès, se reporter à la section *Supervision* de la documentation du GCenter.
Les métriques sont collectées à intervalle régulier :

- toutes les 10 secondes pour les métriques liées au système
- toutes les minutes pour les métriques liées à la détection

Chapitre 8

Annexes

8.1 Fichiers d'événements

Il est possible de consulter les fichiers d'événements.

Pour afficher...	nom du fichier...
les événements du moteur de détection	detection-engine-logs
les événements liés au noyau	var-log-kernel
l'agrégation de différents journaux	var-log-messages
les informations d'authentification du GCap	var-log-auth
les informations de lancement des tâches planifiées	var-log-cron
les informations sur l'activité des différentes applications utilisées	var-log-daemon
les informations sur l'activité des utilisateurs du GCap	var-log-user
les événements de debug	var-log-debug

8.1.1 Événements du moteur de détection : detection-engine-logs

Ce journal contient les événements du moteur de détection. Ils permettent d'obtenir plus des informations sur l'état ou les erreurs du moteur de détection.
Quelques exemples de lignes utiles :

- fin du démarrage

```
[97] <Info> -- All AFP capture threads are running.
```

- fin de rechargement de règles

```
 [76] <Info> -- cleaning up signature grouping structure... complete
 [76] <Notice> -- rule reload complete
```

- erreur de chargement de règles

```
[76] <Error> -- [ERRCODE: SC_ERR_UNKNOWN_PROTOCOL(124)] - protocol "dnp3" cannot be used in a signature.  Either␣
↪detection for this protocol is not yet supported OR detection has been disabled for protocol through the yaml option␣
↪app-layer.protocols.dnp3.detection-enabled
 [76] <Error> -- [ERRCODE: SC_ERR_INVALID_SIGNATURE(39)] - error parsing signature "alert dnp3 $EXTERNAL_NET any ->
↪$INTERNAL_NET any (msg: "Failing rule"; sid:2000001; rev:1;) from file /etc/suricata/rules/local_all.rules at line 1  ␣
↪
```

8.1.2 Événements liés au noyau : var-log-kernel

Ce journal contient les informations des événements liés au noyau.
Quelques exemples d'informations utiles :

- changement d'état d'un lien

```
2022-02-03T12:48:39.578422+00:00 GCap.domain.tld kernel: [ 9149.189652] i40e 0000:17:00.0 mon0: NIC Link is Down
2022-02-03T12:48:40.457410+00:00 GCap.domain.tld kernel: [ 9150.068228] i40e 0000:17:00.0 mon0: NIC Link is Up, 10 Gbps␣
↪Full Duplex, Flow Control: None
```

8.1.3 Informations d'authentification du GCap : var-log-auth

Ce journal contient les informations d'authentification du GCap.
Quelques exemples de lignes utiles :

- erreur d'authentification SSH

```
2022-02-03T14:10:17.680152+00:00 GCap.domain.tld sshd: root [pam]#000[338683]: level=error msg="failed to check␣
↪credentials for \"root\": \"invalid password: password mismatch\""
2022-02-03T14:10:26.682897+00:00 GCap.domain.tld sshd[338675]: error: PAM: Authentication failure for root from 1.2.3.4
2022-02-03T14:10:26.785321+00:00 GCap.domain.tld sshd[338675]: Connection closed by authenticating user root 1.2.3.4␣
↪port 3592 [preauth]
```

- les événements IPSec

```
2022-02-03T13:38:10.770453+00:00 GCap.domain.tld charon: 06[IKE] reauthenticating IKE_SA GCenter[4]                 ␣
↪                                        2022-02-03T13:38:10.771116+00:00 GCap.domain.tld charon: 06[IKE] deleting␣
↪IKE_SA GCenter[4] between 10.2.19.152[C=FR, O=GATEWATCHER, CN=lenovo-se350-int-sla.gatewat
cher.com]...2.3.4.5[CN=GCenter.domain.tld.com]
2022-02-03T13:38:13.085957+00:00 GCap.domain.tld charon: 16[IKE] IKE_SA deleted
2022-02-03T13:38:13.141553+00:00 GCap.domain.tld charon: 16[IKE] initiating IKE_SA GCenter[5] to 2.3.4.5           ␣
↪                                    2022-02-03T13:38:13.364748+00:00 GCap.domain.tld charon: 07[IKE] establishing␣
↪CHILD_SA GCenter{18} reqid 2
2022-02-03T13:38:14.827308+00:00 GCap.domain.tld charon: 12[IKE] IKE_SA GCenter[5] established between 10.2.19.152[C=FR,␣
↪O=GATEWATCHER, CN=GCap.domain.tld]...2.3.4.5[CN=GCenter.domain.tld.com]
```

8.1.4 Informations sur l'activité des différentes applications utilisées : var-log-daemon

Ce journal contient les informations sur l'activité des différentes applications utilisées.
Quelques exemples de lignes utiles :

- synchronisation de configuration avec le GCenter

```
2022-02-03T16:25:35.583926+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO] Successfully rsynced GCap.domain.
↪tld-rules/suricata_configuration.json:
2022-02-03T16:25:35.840272+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO] Successfully rsynced GCap.domain.
↪tld-rules-static/v2.0/codebreaker_shellcode.rules:
2022-02-03T16:25:35.840643+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO] Codebreaker file /data/containers/
↪suricata/etc/suricata/rules/codebreaker_shellcode.rules was identical
2022-02-03T16:25:35.975630+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO] Successfully rsynced GCap.domain.
↪tld-rules-static/v2.0/codebreaker_powershell.rules:
2022-02-03T16:25:35.975771+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO] Codebreaker file /data/containers/
↪suricata/etc/suricata/rules/codebreaker_powershell.rules was identical
```

8.1.5 Informations sur l'activité des utilisateurs : var-log-user

Ce journal contient les informations sur l'activité des utilisateurs du GCap.
Quelques exemples de lignes utiles :

- démarrage du moteur de détection

```
2022-02-03T14:18:26.428461+00:00 GCap.domain.tld root: [GCap_suricata_tools.suricata-INFO] Detection Engine successfully␣
↪started!
```

- les actions effectuées via la commande `gcap-cli`

```
2022-02-03T16:47:50.636706+00:00 GCap.domain.tld GCap-setup (root) [main main.py handle_shell 656] : [GCap_cli.main-
↪NOTICE] Starting CLI
2022-02-03T16:47:50.636768+00:00 GCap.domain.tld GCap-setup (root) [main main.py handle_shell 676] : [GCap_cli.main-
↪INFO] Acquiring lock                              2022-02-03T16:47:50.636832+00:00 GCap.domain.tld GCap-setup (root)␣
↪[main main.py handle_shell 686] : [GCap_cli.main-INFO] Running single CLI command
2022-02-03T16:47:50.784347+00:00 GCap.domain.tld GCap-setup (root) [main main.py default 530] : [GCap_cli.main-NOTICE]␣
↪[user root] Running CLI command 'show logs var-log-kernel'                                                          ␣
↪                                                                                                                 2022-02-
↪03T16:47:50.784889+00:00 GCap.domain.tld GCap-setup (root) [inspect inspect.py run 332] : [GCap_setup.inspect-NOTICE]␣
↪Starting inspect procedure
2022-02-03T16:47:50.784930+00:00 GCap.domain.tld GCap-setup (root) [inspect inspect.py run 339] : [GCap_setup.inspect-
↪NOTICE] Selecting inspection action: `View kernel logs (/var/log/kern.logs)`
2022-02-03T16:47:51.714026+00:00 GCap.domain.tld GCap-setup (root) [inspect inspect.py run 336] : [GCap_setup.inspect-
↪NOTICE] Stopping inspect procedure
2022-02-03T16:47:51.718373+00:00 GCap.domain.tld GCap-setup (root) [main main.py handle_shell 710] : [GCap_cli.main-
↪NOTICE] [user root] Stopping CLI
```

8.1.6 Événements de debug : var-log-debug

Ce journal contient les événements de debug.
Cette entrée est principalement utilisée par le support lors de dépannage avancé.

8.1.7 Agrégation de différents journaux : var-log-messages

Ce journal contient l'agrégation de différents journaux cités ci-dessus.

8.1.8 Informations de lancement des tâches planifiées : var-log-cron

Ce journal contient les informations de lancement des tâches planifiées.

Chapitre 9

Glossaire

CLI
: La CLI (Command Line Interface) est le moyen utilisé pour administrer et configurer le GCap. Il s'agit de l'ensemble des commandes en mode texte.

FQDN
: Le FQDN (Fully Qualified Domain Name) correspond au nom hôte.domaine.

GCap
: Le GCap est la sonde de détection de la solution Trackwatch. Elle récupère le flux réseau du TAP et reconstitue les fichiers qu'elle envoie au GCenter.

GCenter
: Le GCenter est le composant qui administre le GCap et effectue l'analyse des fichiers envoyés par le GCap.

gview
: Nom du compte destiné à un opérateur

gviewadm
: Nom du compte destiné à un responsable

MTU
: La MTU (Maximum Transfert Unit) est la taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation) sur une interface réseau.

OTP
: L'OTP (One Time Password) est un mot de passe à usage unique défini sur le Gcenter.

RAID1
: Le RAID 1 consiste en l'utilisation de n disques redondants. Chaque disque de la grappe contenant à tout moment exactement les mêmes données, d'où l'utilisation du mot « miroir » (mirroring).

RAID5
: Le RAID 5 fait appel à plusieurs disques durs (3 minimum) regroupés en grappe pour constituer une seule unité logique. Les données sont dupliquées en double et réparties sur 2 disques différents.

setup
: Nom du compte destiné à un administrateur système

SIGFLOW
: Le moteur de détection (appelé aussi Sigflow) est chargé de la reconstitution des fichiers et aussi l'un des moteurs pour la détection d'intrusions.

TAP
: Le TAP (Test Access Point) est un dispositif passif qui permet de dupliquer un flux réseau.

```
PDF documentation
```

Index