Documentation
GCap Version 2.5.3.105

Documentation version : V2

Creation date : Septembre, 2022

Last update : Septembre, 2022

Contents

Index **205**

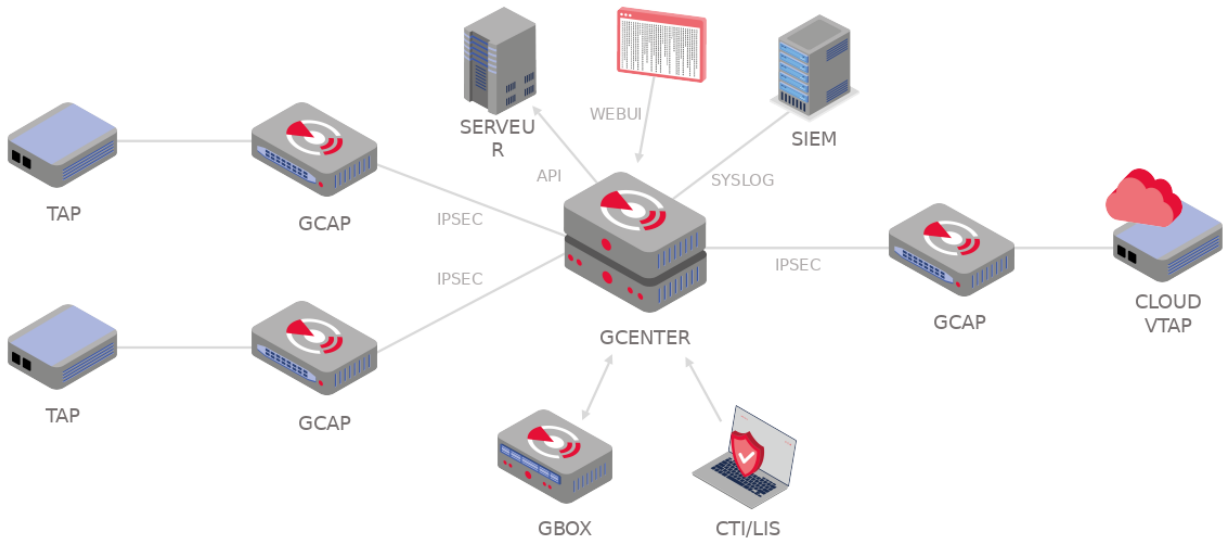
Chapter 1

Description

1.1 Introduction

La solution Trackwatch 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.

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

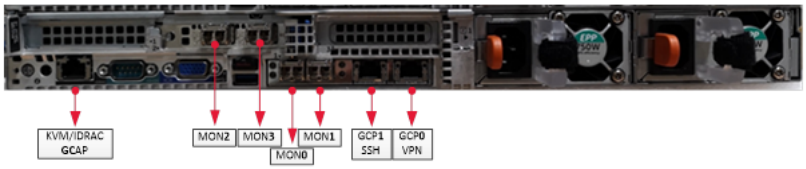
1.3.1 Différents modèles de serveurs

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 `gcp0` et `gcp1`
- des connecteurs RJ-45 et/ou fibre pour la surveillance `mon0`
- 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 déprécié, 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 `gcp0` et `gcp1`

Ces interfaces ont les fonctions suivantes :

- fonction 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...)
- fonction 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 fonctions sont portées uniquement par l'interface `gcp0`.

En **configuration double-interface** :

- la fonction 1 est portée par l'interface `gcp0`
- la fonction 2 est portée par l'interface `gcp1`.

Configuration des interfaces réseau `gcp0` et `gcp1`

Pour plus d'informations sur ces interfaces et leur configuration, se référer au paragraphe *Interfaces réseau `gcp0` et `gcp1`*.

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 de interfaces de capture est variable en fonction des spécificités de chaque modèle.

Activation des interfaces de capture et de surveillance `monx`

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

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 `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 et, pour cela, il y a 2 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 2 lien physiques appelé `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`)

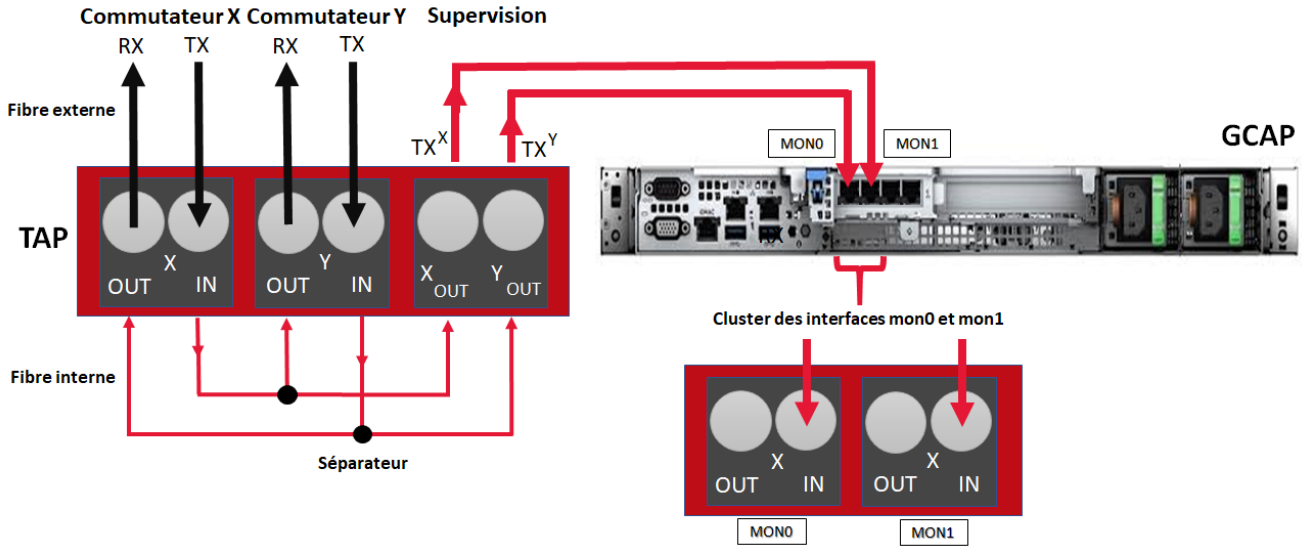
Le lien `commutateur Y` relie le commutateur et le TAP entrée **Y** et permet de dupliquer l'autre moitié du flux réseau. Le lien TX est :

- 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.



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*.

1.6 GCaps en redondance : haute disponibilité

1.6.1 Introduction

La haute disponibilité (High Availability) permet d'avoir deux GCaps en redondance, pour ne pas perdre les flux capturés en cas de panne ou d'arrêt d'un GCap.

Pour mettre en place la haute disponibilité, il faut deux GCaps sur un réseau qui communiquent avec un unique GCenter.

En cas de panne sur l'un des deux GCaps, l'autre prend le relais pour que le service continue de fonctionner pendant la réparation.

1.6.2 Fonctionnement de la haute disponibilité

1.6.2.1 Prérequis

La configuration doit être identique sur les deux GCaps, sinon les messages échangés ne seront pas considérés comme valides.

1.6.2.2 Postulat de base

Un GCap peut être soit `leader` soit `follower`.

Le GCap `leader` est le seul à pouvoir envoyer des eve logs et des fichiers au GCenter.

Le GCap `follower` stocke les eve logs et les fichiers sur son système de fichier.

Note:

La durée de rétention est de 1h pour le GCap *follower*.

Quand un GCap passe `leader`, il envoie tous les eve logs et les fichiers qu'il a stockés sur son système de fichier.

Il n'y a pas de mécanisme de préemption : si un GCap est `leader` il le restera tant que son état est `healthy`.

1.6.2.3 Election du leader

Les GCap communiquent entre eux et procèdent à l'élection du GCap `leader` et du GCap `follower`.

L'élection du GCap `leader` est celui qui a l'identifiant le plus bas : lié en partie à la date de démarrage.

Avertissement:

Si les GCaps ne parviennent pas à communiquer, alors ils deviennent tous les deux *leader*. Dans ce cas, les données sont enregistrées en double sur le système.

Note:

Ce comportement est normal car un GCap ne peut pas arrêter son fonctionnement sans la certitude qu'un autre GCap est *leader*.

1.6.2.4 Panne d'un GCap

En cas de panne du GCap `leader`, le GCap `follower` devient automatiquement le GCap `leader`.

Quand le GCap en panne redevient fonctionnel, il était et reste `follower`.

En cas de panne du GCap `follower`, le GCap `leader` reste le `leader`.

Quand le GCap en panne redevient fonctionnel, il redevient `follower`.

1.6.3 Utiliser et configurer la haute disponibilité

Pour plus d'informations, se référer au paragraphe *GCaps en redondance : haute disponibilité*.

Chapter 2

Fonctionnement

2.1 Le GCap

2.1.1 Les fonctions du GCap

Les fonctions du GCap sont :

- 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 et est localisé dans le GCap
  - les suivants sont localisés dans le GCenter. Il récupère le flux réseau envoyé par le GCap pour effectuer cette analyse :
    - le deuxième est le moteur Codebreaker,
    - le troisième est le moteur Malcore,
    - le quatrième est le moteur Retroact.
- la transmission des fichiers, codes, événements vers le GCenter,
- la communication entre GCap et GCenter (réceptions des fichiers de configuration, ruleset ...).

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 pouvoir plus d'informations, se référer au tableau *Gérer le moteur de détection*.

2.1.2.1 Filtrage du flux capturé

Une partie du flux capturé ne peut être détecté, ni reconstruit : 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:

Pour **afficher** les règles de filtrage des paquets, utiliser la commande *show advanced-configuration packet-filtering*.
Pour **spécifier** les règles de filtrage des paquets, utiliser la commande *set advanced-configuration packet-filtering*.

2.1.2.2 Règles de configuration

Note:

Pour **afficher** les règles de filtrage des paquets, utiliser la commande *show advanced-configuration local-rules*.
Pour **spécifier** les règles locales, utiliser la commande *set advanced-configuration local-rules*.

Règles de Sigflow pour la détection

Les règles pour configurer Sigflow sont définies :

- dans le GCenter et transféré depuis le GCenter (accès via la commande `show config-files rules-scirius`)
- ou localement sur le GCap (accès via la commande `{show,set} advanced-configuration local-rules`)

2.1.2.3 Règles de configuration de Sigflow pour la reconstruction de fichiers

Les règles pour configurer Sigflow sont définies :

- dans le GCenter et transféré depuis le GCenter (accès via la commande `show config-files rules-files`)
- ou localement sur le GCap (accès via la commande `{show,set} advanced-configuration local-rules`)

2.1.2.4 Règles de configuration de Sigflow pour la gestion des seuils pour la remontée d'alarmes

Les règles pour configurer Sigflow sont définies :

- dans le GCenter (accès via la commande `show config-files threshold`)
- ou localement sur le GCap (accès via la commande `{show,set} advanced-configuration local-rules`)

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 pouvoir 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 faites :

- synchroniser la date et heure du GCap sur le GCenter : voir *Présentation de la gestion de la date et heure*
- gérer les interfaces `gcp0` et `gcp1` : 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* de la CLI.

La modification de la date et heure courante se fait grâce à la commande *`set datetime* de 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 réseau gcp0 et gcp1

Les interfaces de management sont au nombre de deux. Elles se nomment respectivement gcp0 et gcp1.

Ces interfaces ont les fonctions suivantes :

- fonction 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...)
- fonction 2 : administration distante au travers du protocole SSH avec l'accès :
  - à la CLI de la sonde
  - au menu graphique d'installation/configuration (déprécié)

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 gcp0 et gcp1*.

Configuration mono-interface.

En **configuration mono-interface**, La fonction 1 et la fonction 2 sont portées uniquement par l'interface gcp0.

Pour basculer de la configuration double-interface en simple interface, se reporter à la *Procédure de basculement vers la configuration simple-interface*.

Configuration double-interface

En **configuration double-interface** :

- la fonction 1 est portée par l'interface gcp0
- la fonction 2 est portée par l'interface gcp1.

Important:

Cette configuration (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:

Il n'est pas possible d'inverser les 2 interfaces réseau.

Pour basculer de la configuration simple-interface en double-interface, se reporter à la *Procédure de basculement vers la configuration double-interface*.

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

Les interfaces de capture sur le GCap sont, par défaut, au nombre de quatre.

Ces interfaces reçoivent les flux issus des TAPs sur les interfaces indiquées:

- `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 de 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 Monvirt permettant 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.

Commandes dans la CLI

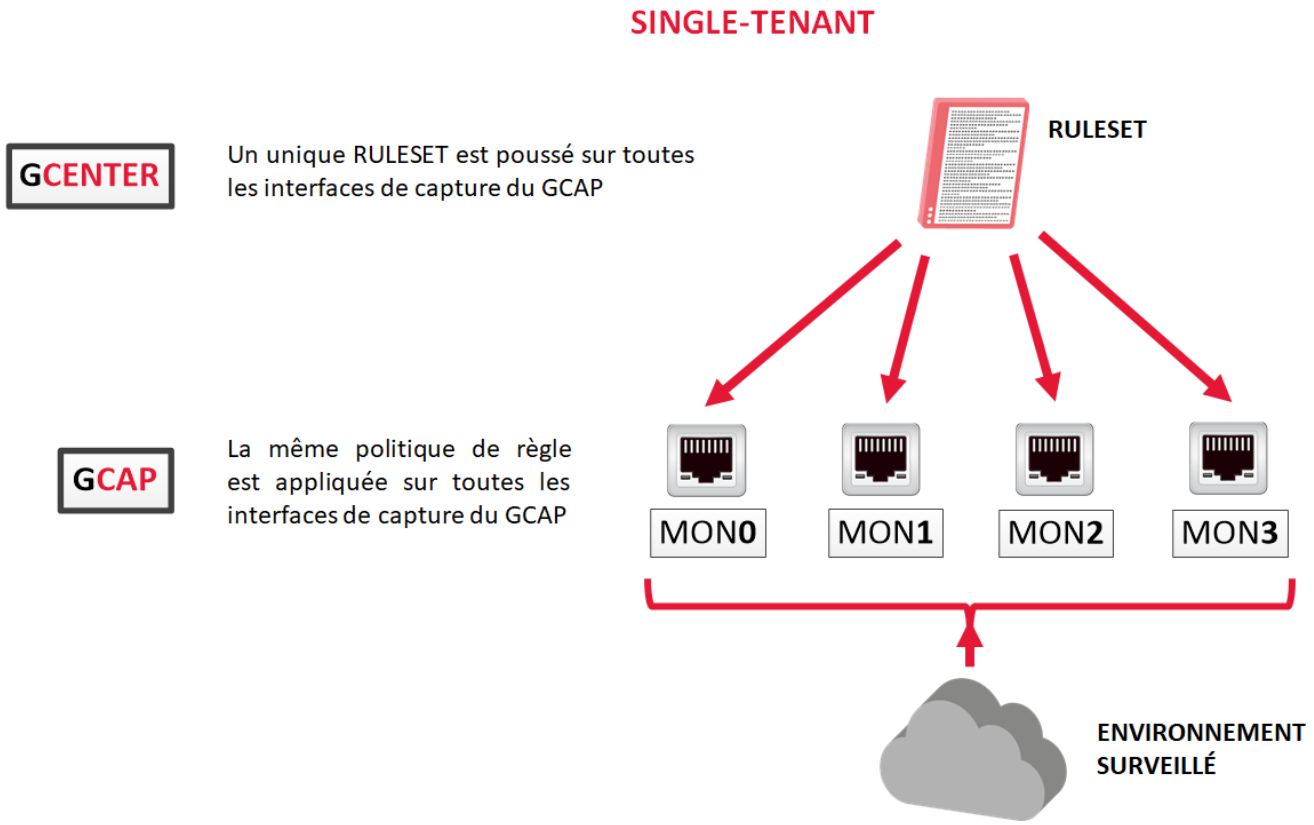
La possibilité de visualiser / créer des règles locales est faite différemment suivant la configuration. Pour avoir plus d'informations sur les règles, voir le tableau *Gérer le moteur de détection (fonctions avancées)*.

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

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

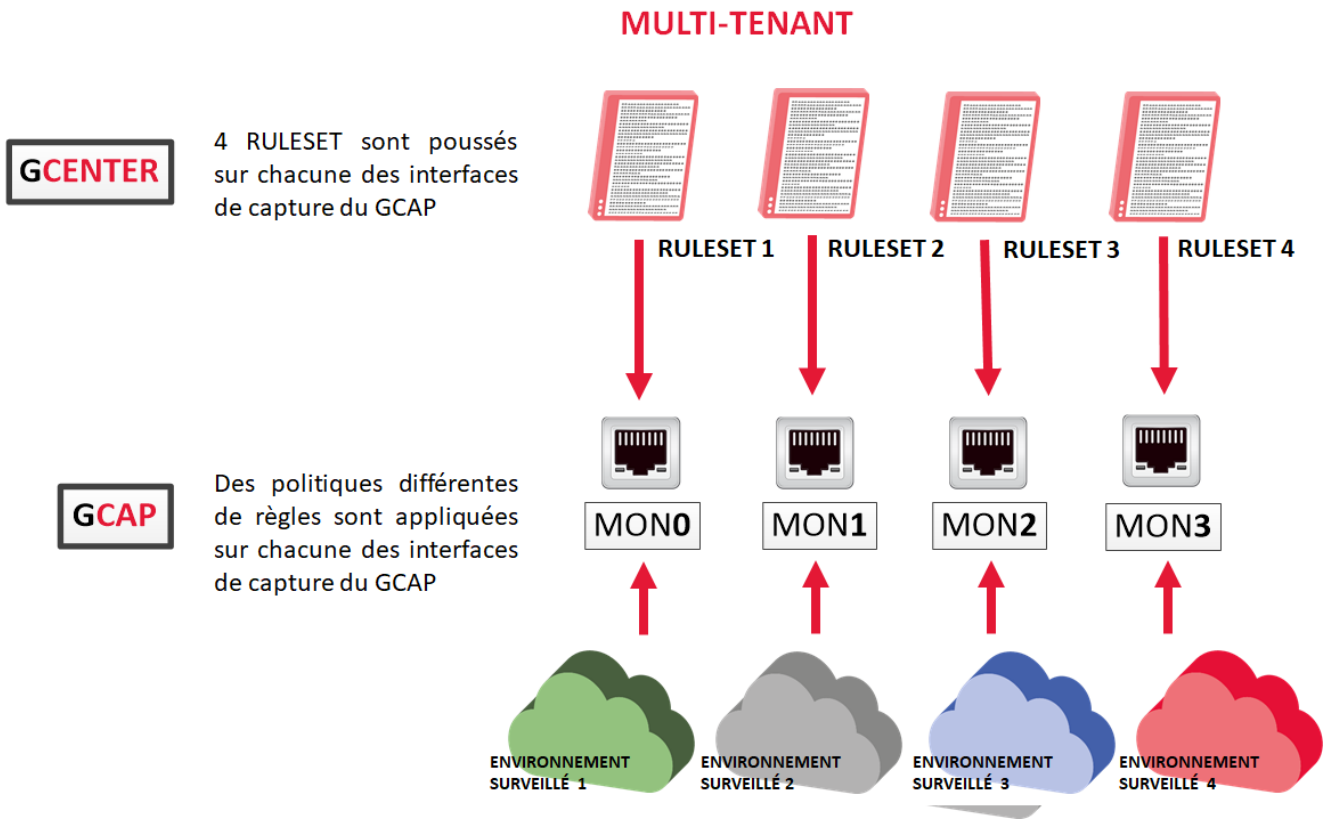
Configuration du mode single-tenant

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

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.

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 clusters*.

La configuration de l'agrégation se fait grâce à la commande *set clusters*.

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.

Une agrégation, une fois créée, doit être activée.

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.
- 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.

2.2.7 Moteur de détection Sigflow

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

- activation d'une ou plusieurs interfaces de capture sur le GCap
- appairage du GCap avec le GCenter
- activation du 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

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*.

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.

Vérification de l'état du moteur d'analyse Sigflow

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

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 et 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*).

Période de grâce

Si le nombre de règles chargées par le moteur d'analyse est important alors la durée maximale de démarrage doit être modifiée via la *CLI*.

2.2.7.5 Désactivation du moteur de détection Sigflow

Vérification de l'état du moteur de détection Sigflow

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

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 démarré.

```
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.

Affichage de la valeur courante de la MTU

Il est possible d'afficher la valeur de la MTU avec la commande *show advanced-configuration mtu*:

```
(gcap-cli) show advanced-configuration mtu

Current Monitoring Network MTU configuration:
        - mon0: 1500
        - monvirt: 1500
```

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 les fonctionnalités de Load Balancing et de Filtrage XDP ne sont pas supportées lorsque la MTU > 3000.

Modification de la valeur courante de la MTU

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

- nom de l'interface, par exemple mon0
- valeur, par exemple 1300

Note:

Pour modifier la MTU de l'interface `mon0` à 1300 :
- entrer la commande *set advanced-configuration mtu mon0 1300*
- valider

```
(gcap-cli) set advanced-configuration mtu mon0 2500
```

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

```
Updating Monitoring Network MTU configuration to:
        - mon0: 2500
```

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

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

Note:

A savoir que les protocoles sur lesquels il est possible de reconstruire dépend 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.

L'administrateur a la possibilité d'ajouter une règle locale depuis la CLI avec la commande *local-rules* si nécessaire.

Exemple de syntaxe des règles pour ces protocoles est la suivante :

```
alert ftp-data any any -> any any (msg:"[ Message regle FTP ] FTP filestore all"; filestore;␣
↪ftpdata_command:retr; sid:13371340; rev:1;)

alert smb any any -> any any (msg:"[ Message regle SMB ] SMB filestore all"; filestore;␣
↪ftpdata_command:retr; sid:13371341; rev:1;)
```

2.3 GCaps en redondance : haute disponibilité

2.3.1 Introduction et fonctionnement

Pour plus d'informations, se référer au paragraphe *GCaps en redondance : haute disponibilité*.

2.3.2 Commandes dans la CLI

La gestion de la haute disponibilité se fait à l'aide de commandes de la CLI dont la liste est donnée dans le tableau *Configurer le GCap*.

2.3.3 Procédures dans les cas d'utilisation

Pour la mise en œuvre, se référer à la *Procédure de gestion de la haute disponibilité*.

Chapter 3

Caractéristiques

3.1 Caractéristiques mécaniques des GCap

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 GCap

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

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 comprends 2 parties :

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

Chapter 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 une 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.a.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 Clés 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 :
  - consulter les journaux des alertes (`show alerts`)
  - surveiller l'utilisation du CPU (`show cpus`)
  - 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 la configuration de Sigflow ainsi que les règles transmises par le GCenter (`show config-files`)
  - afficher les statistiques du moteur de détection Sigflow (`show eve-stats`)
  - afficher les différents fichiers de logs du GCap (`show logs`)
  - afficher le mode de connexion (graphique GUI ou ligne de commande CLI) (`show setup-mode`)
- 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 le mode de connexion pour l'utilisateur courant et le niveau inférieur (graphique GUI ou ligne de commande CLI) (`set setup-mode`)
  - 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`)
- accéder aux commandes de l'ensemble `services` pour gérer les services :
  - visualiser l'état d'un ou des services (`services status`)
  - démarrer un service (`services start`)
  - arrêter un service (`services stop`)
  - afficher les périodes de conservation des fichiers du GCap (`services show`)
- 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`)
  - les agrégations des interfaces de capture et de surveillance `mon` et leurs configurations (`show clusters`)
  - le mode de compatibilité utilisé pour interagir avec le GCenter (`show compatibility-mode`)
  - la date et l'heure du GCap (`show datetime`)
  - la politique de mot de passe pour les comptes (`show password-policy`)
  - 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 :
  - le nombre de CPU dédié au moteur de détection Sigflow (`show advanced-configuration cpu-config`)
  - les règles statiques de filtrage du flux (`show advanced-configuration packet-filtering`)
  - la configuration de la haute disponibilité (`show advanced-configuration high-availability`)
  - la valeur de la MTU des interfaces de capture activées (`show advanced-configuration mtu`)
  - la configuration d'équilibrage de charge venant de l'interface de capture `monx` listée vers les CPU (`show advanced-configuration load-balancing`)
  - les règles locales de Sigflow en fonction du tenant configuré (`show advanced-configuration local-rules`)
  - le nom de remplacement des interfaces (`show advanced-configuration interface-names`)
- 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 le nombre de CPU dédié au moteur de détection Sigflow (`set advanced-configuration cpu-config`)
  - modifier la configuration de la haute disponibilité (`set advanced-configuration high-availability`)
  - définir une configuration avancée d'équilibrage de charge des flux capturés (`set advanced-configuration load-balancing`)
  - modifier les règles locales de Sigflow en fonction du tenant configuré (`set advanced-configuration local-rules`)
  - modifier la valeur de la MTU des interfaces de capture activées (`set advanced-configuration mtu`)
  - spécifier les règles statiques de filtrage du flux (`set advanced-configuration packet-filtering`)
  - détecter/nommer les interfaces du GCap (`set advanced-configuration rescan-interfaces`)

- accéder aux commandes de l'ensemble `system` pour gérer le serveur :
  - redémarrer le GCap (`system restart`)
  - éteindre le GCap (`system shutdown`)
  - arrêter un service (`system reload-drivers`)
  - recharger les pilotes des cartes réseaux (`services show`)
  - réinitialiser le verrouillage des comptes `gview`, `gviewadm` et `setup` suite à des tentatives d'authentification infructueuses (`system unlock`)

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

Table1: 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
Interface (GUI ou CLI) pour la prochaine connexion : Afficher	show setup-mode	show setup-mode	show setup-mode
Interface (GUI ou CLI) pour la prochaine connexion : modifier le mode	set setup-mode	set setup-mode	set setup-mode
Date et l'heure : afficher	show datetime	N/A	N/A
Date et l'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
Services : afficher les périodes de conservation des fichiers	services show retention-periods	services show retention-periods	N/A
Services : démarrer un service (à définir)	services start +service à définir	services start +service à définir	N/A
Services : arrêter un service (à définir)	services stop +service à définir	services stop +service à définir	N/A
Services : visualiser l'état	services status +service à définir	services status +service à définir	N/A
haute disponibilité : visualiser l'état	show advanced-configuration high-availability	N/A	N/A
haute disponibilité : configurer	set advanced-configuration high-availability	N/A	N/A
Appairage avec le GCenter	pairing	N/A	N/A

4.6.2 Gérer les comptes

Table2: 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

Table3: Gérer le moteur de détection

Fonction par niveau	setup	gviewadm	gview
Configuration de Sigflow : afficher la configuration ainsi que les règles	show config-files	show config-files	show config-files
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

4.6.3.1 Gérer le moteur de détection (fonctions avancées)

Les fonctions avancées sont :

- allocation de ressources : modification de la répartition des CPU réservés au moteur de détection
- équilibrage de charge interface capture : équilibrage de charge des flux capturés par interface de capture en utilisant des méthodes de répartition de charge (algorithme)
- filtrage du flux : spécification des règles statiques de filtrage des flux capturés par les interfaces de capture
- règles locales de Sigflow : modification local (dans le GCap) des règles de surveillance du trafic effectué par le moteur de détection Sigflow l'aide des règles de détection (fichier local_all.rules)

Table4: Gérer le moteur de détection (fonctions avancées)

Fonction par niveau	setup	gviewadm	gview
Allocation de ressources : afficher le nombre de CPU dédié	show advanced-configuration cpu-config	N/A	N/A
Allocation de ressources : modifier le nombre de CPU dédié	set advanced-configuration cpu-config	N/A	N/A
Equilibrage de charge interface de capture ```monx``` - CPU : afficher la configuration	show advanced-configuration load-balancing	N/A	N/A
Equilibrage de charge interface de capture ```monx``` - CPU : modifier la configuration	set advanced-configuration load-balancing	N/A	N/A
Filtrage du flux : afficher les règles statiques	show advanced-configuration packet-filtering	N/A	N/A
Filtrage du flux : spécifier les règles statiques	set advanced-configuration packet-filtering	N/A	N/A
Règles locales de Sigflow : afficher	show advanced-configuration local-rules	N/A	N/A
Règles locales de Sigflow : modifier	set advanced-configuration local-rules	N/A	N/A

4.6.4 Gérer le réseau

Table5: 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
Interfaces de détection : afficher le nom de remplacement des interfaces	show advanced-configuration interface-names	N/A	N/A
Interfaces de détection : détecter/nommer les interfaces	set advanced-configuration rescan-interfaces	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

Table6: Gérer le serveur

Fonction par niveau	setup	gviewadm	gview
Afficher l'aide sur les commandes	help	help	help
Lancer la GUI de configuration du GCap	gui	gui	gui
Quitter la session en cours quitter la session SSH	exit	system restart	system restart
Système : redémarrer le GCap	system restart	N/A	N/A
Système : éteindre le GCap	system shutdown	N/A	N/A
Système : rechargement des pilotes des cartes réseaux	system reload-drivers	N/A	N/A

4.6.6 Surveiller le GCAP

Table7: Surveiller le GCAP

Fonction par niveau	setup	gviewadm	gview
Surveillance : consulter les journaux des alertes	show alerts	show alerts	show alerts
Surveillance : utilisation du CPU	show cpus	show cpus	show cpus
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 différents les journaux d'événements	show logs	show logs	show logs
Surveillance : afficher des statistiques et des 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

Chapter 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 Commment se connecter au Gcap?

L'accès au GCap peut être fait :

- 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
- soit par une connexion à distance à la CLI en SSH via les interfaces réseau `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

Il n'y a pas de configuration spécifique à part la connaissance du nom et mot de passe d'accès à 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)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Cette connexion n'est pas la façon nominale 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)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Cette connexion n'est pas la façon nominale 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 `gcp0`ou `gcp1`

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

- `gcp1` (configuration double-interface) ou
- `gcp0` (configuration mono-interface)

Cette connexion est la façon nominale d'accéder au GCap.

Pour plus d'informations, voir *Procédure de connexion sur le GCap via SSH*.

5.3 Connexion à distance au GCenter

L'accès distant au GCenter se fait soit :

- soit en SSH pour configurer le GCenter.
  Pour plus d'informations, se référer à la documentation du GCenter.
- soit via un navigateur web pour pouvoir appairer le GCap.
  Pour plus d'informations, voir *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
Services: démarrer un service (à définir)	1	Visualiser l'état des services : utiliser la commande services status +service à définir
	2	Démarrer un service : utiliser la commande services start +service à définir
Services: arrêter un service (à définir)	1	Visualiser l'état des services : utiliser la commande services status +service à définir
	2	Arrêter un service : utiliser la commande services stop +service à définir
Services: visualiser l'état des services	1	Visualiser l'état des services : utiliser la commande services status +service à définir
Services: afficher les périodes de conservation des fichiers	1	Arrêter un service : utiliser la commande services show retention-periods
Haute disponibilité	1	Afficher : utiliser la commande show advanced-configuration high-availability
	2	Gestion : utiliser la procédure Gestion de la haute disponibilité de GCaps
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 gcp0 et 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
Interfaces de détection : afficher le nom de remplacement des interfaces de capture monx	1	Utiliser la commande show advanced-configuration interface-names
Authentification : détecter / nommer les interfaces de capture monx	1	Utiliser la commande set advanced-configuration rescan-interfaces
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 pour la connexion SSH gérée par l'interface gcp0	1	Utiliser la procédure Basculement vers la configuration simple-interface
Basculer vers la configuration double-interface pour la connexion SSH gérée par l'interface gcp1	1	Utiliser la procédure Basculement vers la configuration double-interface

5.4.5 Gérer le moteur de détection

Table1: Fonctions de base

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Afficher la configuration du moteur de détection ainsi que les règles	1	Utiliser la commande show config-file
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

Table2: Fonctions avancées

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Allocation de ressources : afficher le nombre de CPU dédié	1	Utiliser la commande show advanced-configuration cpu-config
Allocation de ressources : modifier le nombre de CPU dédié	1	Utiliser la commande set advanced-configuration cpu-config
Equilibrage de charge interface de capture monx - CPU : afficher la configuration	1	Utiliser la commande show advanced-configuration load-balancing
Equilibrage de charge interface de capture monx - CPU : modifier la configuration	1	Utiliser la commande set advanced-configuration load-balancing
Filtrage du flux : afficher les règles statiques	1	Utiliser la commande show advanced-configuration packet-filtering
Filtrage du flux : spécifier les règles statiques	1	Utiliser la commande set advanced-configuration packet-filtering
Règles locales de Sigflow : afficher	1	Utiliser la commande show advanced-configuration local-rules
Règles locales de Sigflow : modifier	1	Utiliser la commande set advanced-configuration local-rules
Optimiser les performances du GCap	1	Utiliser la procédure Optimiser les performances du GCap

5.4.6 Gérer le serveur

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Afficher l'aide sur les commandes	1	Utiliser la commande help
Lancer la GUI de configuration du GCap	1	Utiliser la commande gui
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
Système : rechargement des pilotes des cartes réseaux	1	Utiliser la commande system reload-drivers

5.4.7 Surveiller le GCAP

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Surveillance : consulter les journaux des alertes	1	Utiliser la commande show alerts
Surveillance : utilisation du CPU	1	Utiliser la commande show cpus
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 les différents les journaux d'événements	1	Utiliser la commande show logs
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 :
- 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 ...) : voir le tableau *Gérer les comptes*.
- Gérer les interfaces réseau `gcp0` et `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 de 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.
- Mettre à jour la base de signatures Sigflow.
- 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 affiché :

```
gcap-protor login:
```

- Entrer l'identifiant et le mot de passe correspondant.
  L'invite de commande suivant 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 visulaliser 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 nominale 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 visulaliser 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 `Lanch`).
  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 **Enter** pour afficher toutes les commandes disponibles et une courte explication.

5.5.4.4 Cas particulier

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 con

```
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 nominale 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 :

- 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 **Enter** pour afficher toutes les commandes disponibles et une courte explication.

5.5.5.4 Cas particulier

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 visulaliser 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 réseau `gcp0` et `gcp1`*).

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 affiché.

```
[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 `gcp0` et `gcp1`

5.5.9.1 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 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 set network-config domain	Procédure C
afficher ou modifier le nom du système	show network-config hostname 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 et set network-config ssh	Procédure E
afficher ou modifier la valeur MTU des interfaces	show advanced-configuration mtu set advanced-configuration mtu	Procédure F
afficher ou modifier les paramètres TCP/IP des interfaces GCPx	show network-config gcpx	Procédure G

5.5.9.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show network-config configuration*
  - *show network-config status*
  - *show network-config domain*
  - *set network-config domain*
  - *show network-config hostname*
  - *set network-config hostname*
  - *show network-config ssh*
  - *set network-config ssh*
  - *show advanced-configuration mtu*
  - *set advanced-configuration mtu*
  - *show network-config gcp0*
  - *set network-config gcp0*

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 gcpx 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 :
  - nom du système (**hostname**)
  - nom du domaine (**domain_name**)
  - détails des paramètres TCP/IP de chaque interface réseau (`gcp0` et `gcp1`)
  - activation ou non de l'interface (**enabled**)

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

{
    "hostname": "GCap",
    "domain_name": "domain.local",
    "gcp0": {
        "description": "VPN / SSH",
        "ip_address": "192.168.1.1",
        "mask": "255.255.255.0",
        "default_gateway": "192.168.1.254",
        "enabled": true,
        "mtu": 1500
    },
    "gcp1": {
        "description": "SSH",
        "ip_address": "None",
        "mask": "255.255.255.0",
        "default_gateway": "",
        "enabled": false,
```

(suite sur la page suivante)

(suite de la page précédente)

```
        "mtu": 1500
    },
```

Note:

La configuration dans l'exemple ci-dessus est en mono-interface cad `gcp0` utilisé et `gcp1` non utilisé.

Pour `gcp0` :

- le champ **description** indique que les connexions VPN et SSH sont sur cette interface
- les paramètres TCP/IP sont listés
- puisque l'interface est active, le paramètre **enabled** est **true**.

Pour `gcp1` :

- le champ **description** indique que la connexion SSH est sur cette interface
- les paramètres TCP/IP sont à **None**
- puisque l'interface n'est pas actif, le paramètre **enabled** est **false**.

5.5.9.5 Procédure B : afficher l'état des interfaces réseau `gcp0` et `gcp1` du GCap

- Entrer la commande suivante.

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

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

```
  Name          Address         Carrier      Speed           Type
  gcp0      xx:xx:xx:xx:xx:xx         UP    1000Mb/s           RJ45
  gcp1      xx:xx:xx:xx:xx:xx         UP    1000Mb/s           RJ45
```

  Pour chaque interface, les informations suivantes sont affichées :
  - `Address` : l'adresse MAC de l'interface
  - `Carrier` : état de la transmission en cours :
    - valeur `UP` : interface physique est connectée
    - valeur `DOWN` : interface physique n'est pas connectée
  - `Speed` : la vitesse de l'interface en Mb/s
  - `Type` : le type de câble/sfp branché sur le port physique

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...

00% Generating interfaces configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting gcenter-xfer-daemon service  [OK]
81% Restarting netdata service              [OK]
90% Restarting rsyslog service              [OK]
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
```

(suite sur la page suivante)

(suite de la page précédente)

```
Do you want to apply this new configuration? (y/N)
```

– Appuyer sur **y** puis valider

```
Applying configuration...

00% Generating interfaces     configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting gcenter-xfer-daemon service  [OK]
81% Restarting netdata service              [OK]
90% Restarting rsyslog service              [OK]
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 network-config ssh
```

  – Valider.
  Le système affiche l'interface SSH utilisée pour gérer le GCap.
    * Dans le cas de la configuration simple-interface, le système affiche :

```
SSH is using interface gcp0
```

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

```
SSH is using interface gcp1
```

- Pour configurer l'interface `gcp1` en SSH :
  – Entrer la commande suivante.

```
(gcap-cli) set network-config ssh gcp1
```

  – Valider.
  – Entrer la commande suivante.

```
(gcap-cli) set network-config gcp0 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 gcp1 ip-address Y.Y.Y.Y gateway Y.Y.Y.Y mask Y.Y.Y.Y␣
↪confirm
```

  - Valider.

- Pour configurer l'interface gcp0 en SSH :

Note:

L'interface `gcp1` n'est pas utilisée.

- Entrer la commande suivante.

```
(gcap-cli) set network-config ssh gcp0
```

- Valider.
- Entrer la commande suivante.

```
(gcap-cli) set network-config gcp0 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 advanced-configuration mtu
```

  - Valider.
    Le système affiche le résultat.

```
Current Network MTU configuration:
  - mon1: 1500
  - mon2: 1500
  - mon3: 1500
  - cluster0: 1500
  - gcp0: 1500
```

    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 gcp0
  - Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration mtu gcp0 2000
```

  - Valider.
    Le système affiche le résultat.

```
Updating Network MTU configuration to:
  - gcp0: 2000
```

5.5.9.10 Procédure G : afficher ou modifier les paramètres TCP/IP d'une interface gcpx

- Pour afficher la configuration de l'interface gcp0 :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config gcp0
```

  - Valider.
    Le système affiche la configuration de l'interface gcp0.
    Suivant la configuration simple interface ou double interface, les informations sont différentes.
    Les deux cas sont listés ci-après.

Configuration simple-interface
Les connexions SSH et VPN sont gérées par l'interface gcp0.
Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN / SSH):
   - IP Address: X.X.X.X
   - Mask: 255.255.255.0
   - Gateway: X.X.X.X
```

Configuration double-interface
La communication VPN est gérée par l'interface gcp0.
La connexion SSH pour la gestion du GCap est gérée par l'interface gcp1.
Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN):
   - IP Address: X.X.X.X
   - Mask: 255.255.255.0
   - Gateway: X.X.X.X
```

- Pour modifier la configuration de l'adresse de l'interface gcp0 :
  - Entrer la commande suivante.

```
(gcap-cli) set network-config gcp0 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 gcp0.

```
Setting interface gcp0 (VPN / SSH) to configuration :
   - IP Address: 10.2.19.129
   - Mask: 255.255.255.0
   - Gateway: 10.2.19.254
Do you want to apply this new configuration? (y/N)
```

  - Appuyer sur **y** puis valider.

```
Applying configuration...
00% Generating interfaces configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting gcenter-xfer-daemon service  [OK]
81% Restarting netdata service              [OK]
90% Restarting rsyslog service              [OK]
Procedure completed with success
```

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 ou modifier la valeur MTU des interfaces	show advanced-configuration mtu set advanced-configuration mtu	Procédure B
modifier la valeur MTU des interfaces	set advanced-configuration mtu	Procédure B
afficher ou administrer les interfaces de détection disponibles	show interfaces set 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

Dans cette procédure, seules les informations sur les interfaces de capture sont détaillées.

Pour les informations sur les interfaces réseau GPCx, se référer à la *Procédure de gestion des paramètres réseau des interfaces `gcp0` et `gcp1`*.

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

```
(gcap-cli) show network-config configuration
{
    ...
    },
    "mon0": {
        "description": "default",
        "enabled": true,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon1": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon2": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon3": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    }
}
```

Note:

L'interface `mon0` est active (champ **enabled** : **true**).
Les interfaces `mon1` à `mon3` sont inactives (champ **enabled** : **false**)

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 advanced-configuration mtu
```

  - Valider.

  Le système affiche le résultat.

```
Current Network MTU configuration:
        - mon1: 1500
        - mon2: 1500
        - mon3: 1500
        - cluster0: 1500
        - gcp0: 1500
```

  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 `mon1`

– Entrer la commande suivante.

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

– Valider.

Le système affiche le résultat.

```
Updating Network MTU configuration to:
        - mon1: 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.

```
Waiting 10s for interfaces to be up

Name     State      Physical Address   Status   Speed    Type
mon0     Enabled    xx:xx:xx:xx:xx:xx    UP     10Gb     10G Base-SR
mon1     Disabled   xx:xx:xx:xx:xx:xx    UP     1Gb      1G Base-SR
mon2     Disabled   xx:xx:xx:xx:xx:xx    UP     1Gb      1G Base-SR
mon3     Disabled   xx:xx:xx:xx:xx:xx    UP     1Gb      1G Base-SR
monvirt  Enabled    N/A                  UP     N/A      Virtual
```

  Les informations affichées sont :
  – **State :** l'état configuré de l'interface parmi {Enabled|Disabled}
  – **Physical Address :** l'adresse MAC de l'interface
  – **Speed :** la vitesse de l'interface
  – **Type :**
    * s'il s'agit d'une interface virtuelle : Virtual
    * s'il s'agit d'une interface physique : le type de câble/sfp branché sur le port physique
- Pour activer une interface (ici mon0 par exemple) :
  – Entrer la commande suivante.

```
(gcap-cli) set interfaces enable mon0
```

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

```
(gcap-cli) set interfaces disable mon1
```

  – 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 l'interface `gcp0`.

En configuration double-interface :

- la communication VPN est gérée par l'interface `gcp0`
- la connexion SSH pour la gestion du GCap est gérée par l'interface `gcp1`

Cette procédure décrit le basculement de la configuration double-interface vers la configuration simple-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.
En effet, en double-interface, le lien via SSH se fait sur l'interface `gcp1`.
Or après avoir lancée cette commande, ce lien sera désactivé et l'interface à utiliser sera `gcp0`.
Afin d'eviter 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

---

5.5.11.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show network-config*
  - *set network-config ssh*

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 de l'interface `gcp0` :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config gcp0
```

  - Valider.

Le système affiche la configuration de l'interface `gcp0`.
Suivant la configuration simple interface ou double interface, les informations sont différentes.
Les deux cas sont listés ci-après.

Configuration simple-interface

Les connexions SSH et VPN sont gérées par l'interface `gcp0`.

Dans ce cas, le système affiche :

```
 Interface gcp0 configuration (VPN / SSH):
  - IP Address: X.X.X.X
  - Mask: 255.255.255.0
  - Gateway: X.X.X.X
```

Le champ (VPN / SSH) indique que la configuration courante est simple-interface.

Dans ce cas, il n'y a rien à faire.

Configuration double-interface

La communication VPN est gérée par l'interface `gcp0`.

La connexion SSH pour la gestion du GCap est gérée par l'interface `gcp1`.

Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN):
        - IP Address: X.X.X.X
        - Mask: 255.255.255.0
        - Gateway: X.X.X.X
```

Le champ (VPN) indique que la configuration courante est double-interface.

L'absence du paramètre SSH sur l'interface `gcp0` indique que c'est interface `gcp1` qui gère le SSH.

conclusion : 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

- Entrer la commande *set network-config ssh gcp0* suivi des paramètres réseau de l'interface `gcp0`.
  Exemple :
  - `set network-config gcp0 ip-address 192.168.1.1 gateway 192.168.1.254 mask 255.255.255.0`

```
(gcap-cli) set network-config gcp0 ip-address 192.168.1.1 gateway 192.168.1.254 mask 255.255.
↪255.0
```

- Valider.

```
 Setting interface gcp0 (VPN / SSH) to configuration:
        - IP Address: 192.168.1.1
        - Mask: 255.255.255.0
        - Gateway: 192.168.1.254
Do you want to apply this new configuration? (y/N)
```

- Appuyer sur **y** puis valider.

```
Applying configuration...
00% Generating interfaces configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting GCenter-xfer-daemon service  [OK]
81% Restarting heartbeat service            [OK]
90% Restarting netdata service              [OK]
Procedure completed with success
```

Le système affiche la progression et affiche le message **Procedure completed with success** pour indiquer que le passage en simple-interface a été effectué.

- Recâbler les câbles réseau du GCap si besoin.

Note:

Il est nécessaire d'ajouter l'attribut 'confirm' à la fin de la commande lorsque le pairing avec le GCenter est actif.

5.5.12 Basculement vers la configuration double-interface

5.5.12.1 Introduction

En configuration mono-interface, la connexion SSH pour la gestion du GCap et la communication VPN sont gérées par l'interface `gcp0`.
En configuration double-interface :

- la communication VPN est gérée par l'interface `gcp0`
- la connexion SSH pour la gestion du GCap est gérée par l'interface `gcp1`

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.
En effet, en double-interface, le lien via SSH se fait sur l'interface `gcp1`.
Or après avoir lancée cette commande, ce lien sera désactivé et l'interface à utiliser sera `gcp0`.
Afin d'eviter 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 network-config*
  - *set network-config ssh*

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 de l'interface `gcp0`

- Entrer la commande suivante.

```
(gcap-cli) show network-config gcp0
```

- Valider.
  Le système affiche la configuration de l'interface `gcp0`.
  Suivant la configuration simple interface ou double interface, les informations sont différentes.
  Les deux cas sont listés ci-après.

Configuration double-interface

La communication VPN est gérée par l'interface `gcp0`.

La connexion SSH pour la gestion du GCap est gérée par l'interface `gcp1`.

Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN):
     - IP Address: X.X.X.X
     - Mask: 255.255.255.0
     - Gateway: X.X.X.X
```

Le champ (VPN) indique que la configuration courante est double-interface.

L'absence du paramètre SSH sur l'interface `gcp0` indique que c'est interface `gcp1` qui gère le SSH.

conclusion : la configuration courante est 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 `gcp0`.

Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN / SSH):
  - IP Address: X.X.X.X
  - Mask: 255.255.255.0
  - Gateway: X.X.X.X
```

Le champ (VPN / SSH) indique que la configuration courante est simple-interface.

Dans ce cas, il faut continuer avec la procédure suivante.

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

- Entrer la commande *`set network-config ssh gcp1`* suivi des paramètres réseau de l'interface `gcp1`.

  Note:

  Exemple
  `set network-config gcp1 ip-address 192.168.1.2 gateway 192.168.1.254 mask 255.255.255.0_`

- Valider.

```
(gcap-cli) set network-config ssh gcp1
SSH has been set to interface gcp1
Do you want to apply this new configuration? (y/N)
```

- Appuyer sur **y** puis valider.

```
Applying configuration...
00% Generating interfaces configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting GCenter-xfer-daemon service  [OK]
81% Restarting heartbeat service            [OK]
90% Restarting netdata service              [OK]
Procedure completed with success
```

  Le système affiche la progression et affiche le message **Procedure completed with success** pour indiquer que le passage en double-interface a été effectuée.
- Recâbler les câbles réseau du GCap si besoin.

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 `monx`.

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).
  Filtre XDP . 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 `mon0` et `mon1`, il faut utiliser la commande *set clusters add interfaces mon0 mon1*.

5.5.13.2 Prérequis

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

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 suivante.

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

- Valider.
  Le système affiche l'agrégation s'il en existe.
  S'il n'en existe pas, alors le message suivant est affiché :

```
No network cluster defined.
```

5.5.13.5 Procédure pour afficher les interfaces de capture disponibles et activer les 2 interfaces à agréger

- Utiliser la Procédure C de la *Procédure de gestion des paramètres des interfaces de capture monx*.
- Noter les interfaces à utiliser (par exemple `mon0` et `mon1`).

5.5.13.6 Procédure pour créer une agrégation d'interfaces

- Entrer la commande suivante.

Note:

La description d'une agrégation d'interfaces est optionnelle (partie `description test`).

```
(gcap-cli) set clusters add interfaces mon0 mon1 description `test`
```

- Valider.
  Le système affiche le résultat.

```
Creating cluster test with interfaces mon0, mon1
Successfully created cluster `test`
```

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

- Entrer la commande suivante.

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

- Valider.
  Le système affiche l'agrégation créée.

```
Name       State      Description          Interfaces
cluster0   Disabled   test                 mon0, mon1
```

L'agrégation, une fois créée avec le Name **cluster0**, doit être activée.

5.5.13.8 Procédure pour activer l'agrégation créée

- Entrer la commande suivante.

```
(gcap-cli) set clusters enable cluster0
```

- Valider.
  Le système affiche le message suivant.

```
Enabling cluster 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*

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* suivi 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 sur le GCap, opération faite plus tôt). Puis le GCap calcule le fingerprint à l'aide du FQDN du GCap et 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...
Pairing up with the GCenter (IPSec certificates exchange)...
Pairing up with the GCenter (restarting IPSec tunnel)...
Pairing 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 Name         : host.domain
Version           : 2.5.3.105-xxx
Paired on GCenter : 10.2.19.128
Tunnel status     : Up
Detection Engine  : Container down
```

  Le champ `Paired on GCenter` prend :
  - la valeur `Not paired`quand le GCap n'est pas appairé avec le GCenter
  - la valeur IP du GCenter quand le GCap est appairé avec le GCenter

5.5.15 Gestion de la haute disponibilité de GCaps

5.5.15.1 Introduction

Cette procédure décrit la haute disponibilité entre 2 GCaps.

Pour plus d'informations, se référer au paragraphe *high-availability*.

5.5.15.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show advanced-configuration high-availability status*
  - *set advanced-config high-availability*

5.5.15.3 Opérations préliminaires

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

5.5.15.4 Procédure pour afficher l'état de la haute disponibilité (redondance des GCaps)

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration high-availability status
```

- Valider.

Le système affiche l'état de la haute disponibilité avec les compteurs suivants :

- **status :** état du GCap.
  - unhealthy : le GCap n'est pas connecté au GCap voisin
  - Not configured : il n'y pas de haute disponibilité configuré sur ce système
- **paired GCap :** adresse IPv6 du GCap voisin.
- **leader :** état de l'élection parmi Leader/Follower.
- **time since last status :** temps écoulé depuis le dernier healthcheck du GCap voisin.
- **Leader since :** date à laquelle le GCap est devenu Leader.

Cas de l'absence de la haute disponibilité (redondance des GCaps)

Current high-availability status:

- status: Not configured
- paired gcap: Unknown
- leader: Follower
- time since last status: Unknown
- Follower since: Unknown

Cas de la haute disponibilité (redondance des GCaps) avec perte de connexion entre les GCaps

Current high-availability status:

- status: Operational [unhealthy]
- paired gcap: fe80::233
- leader: Leader

- time since last status: Unknown
- Leader since: 2022-01-21T15:35:09Z

5.5.15.5 Procédure pour configurer la haute disponibilité sur le premier GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability peer-ip fe80::XXX
public-ip fe80::YYY multicast-group ff02::200
peer-pubkey 2wtmY/oCaoUGreyr2CROnKAIoEgTXkSOedXlXDvUfBU=
shared-secret Xxf4fknh4KoOH2zgrI4Wyw==
```

Note:

Explication des paramètres :

- *set advanced-configuration high-availability* : commande pour configurer la haute disponibilité
- ***peer-ip fe80::XXX*** [adresse IPv6 du GCap voisin parmi:]
  - **Link-local :** si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.
  - **ULA (Unique Local Address) :** si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64.
- ***public-ip fe80::YYY*** [adresse IPv6 du GCap parmi:]
  - **Link-local :** si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.
  - **ULA (Unique Local Address) :** si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64
- *multicast-group ff02::200* : adresse IPv6 multicast pour la communication entre les GCaps. Plage FF00::/8. Ex : FF02::200.
- *peer-pubkey* 2wtmYCaoUGreyr2CROnKAIoEgTXkSOedXlXDvUfBU= : Clé publique du GCap voisin visible via la commande *show advanced-configuration high-availability pubkey*.
- *shared-secret* Xxf4fknh4KoOH2zgrI4Wyw== : secret de 16 octets encodé en base64 qui doit être identique entre les 2 GCaps.

- Valider.
  Le système affiche le résultat.

```
Updating HA configuration
High availability configuration successfully updated
```

5.5.15.6 Exemple pour configurer la haute disponibilité sur le deuxième GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability peer-ip fe80::YYY public-ip fe80::XXX␣
↪multicast-group ff02::200 peer-pubkey xehXnrigZ0IZZEvWbWri8XegNh0KaAQk8vC6mKj27Ug= shared-
↪secret Xxf4fknh4KoOH2zgrI4Wyw==
```

Le système affiche le résultat.

```
Updating HA configuration
High availability configuration successfully updated
```

5.5.15.7 Exemple pour activer la haute disponibilité sur chaque GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability enable confirm
```

Le système affiche le résultat.

```
Interfaces naming rules updated, reloading configuration
Operation successful.
High availability configuration successfully updated
```

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 défini sur le GCap et celui 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...) 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).
    Pour changer cette valeur, voir la Procédure d'assignation du nombre de CPU au moteur de détection.
  - 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 une partie 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 des compteurs par protocole, du nombre de sessions, de flux ou encore l'état des tables de hashage depuis 'Stats.log'.

5.5.16.2 Prérequis

- **Utilisateur :** setup
- **Commandes utilisées dans cette procédure :**
  - *show advanced-configuration mtu*
  - *set advanced-configuration mtu*
  - *show advanced-configuration cpu-config*
  - *set advanced-configuration cpu-config*
  - *show advanced-configuration packet-filtering*
  - *set advanced-configuration packet-filtering*
  - *show advanced-configuration load-balancing*
  - *set advanced-configuration load-balancing*

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:

Les fonctionnalités de Load Balancing et de Filtrage XDP ne sont pas supportées lorsque la MTU > 3000.

- Utiliser la commande *show advanced-configuration mtu* 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 d'assignation du nombre de CPU au moteur de détection

Astuce:

Dédier le maximum des CPU présents au moteur de détection (sans excéder 80% des CPU).
Ceci est à effectuer quand les CPU dédiés au moteur de détection sont surchargés (utiliser la commande *show cpus*).

- Utiliser la commande *show advanced-configuration cpu-config* pour afficher le nombre de CPU dédié au moteur de détection Sigflow
- Utiliser la commande *set advanced-configuration cpu-config* pour modifier le nombre de CPU dédié

5.5.16.6 Procédure de définition des règles de filtrage du flux

Astuce:

Le(s) CPU présent(s) est surchargé et une partie du flux ne peut etre analaysée, un certain nombre de pa

- pour visualiser une surcharge des CPU , utiliser la commande *show cpus*
- pour visualiser le nombre de paquets perdus (dropped) par coeur cpux, utiliser la commande *show health*, détails des compteurs sofnet - Statistiques sur les paquets reçus en fonction des cœurs de processeurs.

Une partie du flux capturé ne peut être détecté, ni reconstruit : 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.
- Utiliser la commande *set advanced-configuration packet-filtering* pour spécifier des règles statiques de filtrage des flux capturés par les interfaces de capture.

5.5.16.7 Procédure de configuration d'équilibrage de charge venant de l'interface de capture monx

Astuce:

Dans ce cas ou il y a mauvaise répartition de la charge du flux entre les CPU, 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 en utilisant des méthodes de répartition de charge (algorithme).

- Utiliser la commande *show advanced-configuration load-balancing* pour afficher la configuration d'équilibrage de charge venant de l'interface de capture monx listée vers les CPU du GCap.
- Utiliser la commande *set advanced-configuration load-balancing* pour modifier la charge des interfaces de capture.

5.5.16.8 Procédure d'optimisation des règles du moteur de détection

Astuce:

Les règles du moteur de détection peuvent être définies : - en local sur le GCap, - sur le GCenter. Ce sont sur ces 2 appliances qu'il faut les modifier pour les optimiser.
De plus, si la configuration courante est multi-tenant alors les même règles sont appliquées sur les interfaces : ceci peut ne pas être optimisé!

- Utiliser la commande `show advanced-configuration local-rules` pour afficher :
  - dans la rubrique Rules : les règles locales de Sigflow, c'est-à-dire :
    - les règles de détection
    - les règles de reconstruction de fichiers
  - dans la rubrique threshold :
    - les seuils ou limites définis par le mot clé "threshold"
    - les règles de suppression définies par le mot clé "suppress"
- Utiliser la commande *set advanced-configuration local-rules* pour modifier les règles locales de la sonde GCap.
- Optimiser les ruleset transmis depuis le GCenter. Pour cela, utiliser le GCenter.

Chapter 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
services	gérer les services du GCap
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
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.

Maintenant les commandes de l'ensemble `show` sont accessibles.

Les commandes sont aussi accessibles directement depuis l'invite **(gcap-cli)** en lançant la commande complète : par exemple `show alerts` pour la commande `alerts` 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 alerts`

```
(gcap-cli)
```

- Entrer la commande `show alerts` puis valider.

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

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

- Entrer la commande `alerts` puis valider.

6.1.8 Avoir des informations sur les commandes via l'Aide

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

Pour obtenir de l'aide concernant une commande spécifique, il est possible :

- la préfixer par `help` (exemple `help show config-files`)
- de suffixer la commande par `?` (exemple `show config-files ?`)

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'information sur la commande `exit`, se référer au paragraphe *exit*.

6.2 cli

6.2.1 show

6.2.1.1 alerts

Introduction

La commande `alerts` du sous-groupe `show` permet de surveiller les alertes émises par Sigflow.

Prérequis

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

Commande

```
show alerts
```

Exemple

- Entrer la commande suivante.

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

- Valider.

6.2.1.2 bruteforce-protection

Introduction

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

Prérequis

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

Commande

```
show bruteforce-protection
```

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
```

6.2.1.3 bypassed-flows

Introduction

Cette commande est retirée depuis la version 2.5.3.105.

6.2.1.4 clusters

Introduction

La commande `clusters` du sous-groupe `show` permet d'afficher les agrégations des interfaces de capture et de surveillance ```mon** et leurs configurations.

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*.

Note:

Cette fonctionnalité est nécessaire si le TAP qualifié présent dans l'architecture n'assure pas la fonctionnalité d'agrégation d'interfaces.

Prérequis

- **Utilisateur :** setup
- **Dépendances :** activation de deux interfaces de capture au minimum

---

Commande

```
show clusters
```

Exemple pour mettre en œuvre l'agrégation d'interfaces

Se référer à la *Procédure de gestion de l'agrégation d'interfaces de capture*.

Exemple pour afficher le cluster d'interfaces

- Entrer la commande suivante.

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

- Valider.
  Le système affiche le résultat.

```
Name       State      Description          Interfaces
cluster0   Disabled   test                 mon0, mon1
```

  Le système affiche les informations des agrégations existantes et pour chacune :
  - le nom
  - l'état
  - la description
  - les interfaces le composant

Note:

Si le message *No network cluster defined* est affiché, vérifier les prérequis avant d'entrer la commande.

6.2.1.5 compatibility-mode

Introduction

La commande `compatibility-mode` du sous-groupe `show` permet d'afficher 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 :

- 2.5.3.100 : GCenter 2.5.3.100 et inférieur
- 2.5.3.101 : GCenter 2.5.3.101
- 2.5.3.102+ : GCenter 2.5.3.102 et supérieur

Note:

Le mode de compatibilité avec un GCenter en version 2.5.3.100 est déprécié.

Prérequis

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

---

Commande

```
show compatibility-mode
```

Exemple pour afficher le mode de compatibilité configuré

- 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
```

6.2.1.6 config-files

Introduction

La commande `config-files` du sous-groupe `show` permet d'afficher :

- la configuration détaillée du moteur de détection Sigflow à l'aide de la commande `config-files suricata-config`
- les règles transmises par le GCenter au moteur Sigflow :
  - rules-scirius : les règles scirius de détection
  - rules-files : les règles de reconstruction de fichiers
  - threshold.
    Dans cette catégorie, sont définies :
    * les règles de seuils des alertes (règles de détection)
      Par exemple :
      ne plus envoyer d'alertes au delà d'une valeur (notion de limite)
      ou à l'inverse , valider des alertes à partir d'une valeur (notion de seuil)
    * les limitations des règles de détection, par exemple ne pas appliquer une règle à une adresse IP spécifique

Il est uniquement possible d'afficher les règles du tenant configuré.

Prérequis

- **Utilisateurs :** setup, gviewadm, gview
- **Dépendances :**
  - appairer le GCap et le GCenter
  - envoyer des ensembles de règles (ruleset) depuis le GCenter vers le GCap

---

Commande

`show config-files {suricata-config|rules-scirius|rules-files|threshold} [TENANT]`

La commande `show config-files` doit être suivie :

- du nom du fichier de configuration :
  - `suricata-config` pour la configuration de Sigflow
  - `rules-scirius` pour les règles scirius pour la détection utilisé par Sigflow
  - `rules-files` pour les règles de reconstruction de fichiers utilisé par Sigflow
  - `threshold` pour les règles de seuils, les limites et les règles de suppression
- du paramètre TENANT qui peut prendre les valeurs suivantes :
  - multi-tenant par int : {mon0|mon1|mon2|mon3|monvirt}
  - multi-tenant par vlan :
    - default
    - VLAN X
    - VLAN X Y

Exemple pour afficher les règles scirius pour la détection, en mode single tenant

- Entrer la commande suivante.

```
(gcap-cli) show config-files rules-scirius
```

- Valider.
  Le système affiche le résultat.

```
# Rules file for ** generated by Scirius at 2022-05-30 12:41:33.634390+00:00

 alert dns any any -> any any (msg:"[ TEST AUTO ] ALERT DNS UDP";sid:12345600;priority:2;
↪)
```

  Le fichier affiche :
  - d'abord la date de génération
  - puis, dans chaque paragraphe, une règle est définie.

  Pour plus d'information sur la syntaxe des règles, se reporter à la documentation du GCenter.

Exemple pour afficher les règles scirius pour la détection, en mode multi tenant pour l'interface `mon0`

- Entrer la commande suivante.

```
(gcap-cli) show config-files rules-scirius mon0
```

- Valider.
  Le système affiche le résultat (voir exemple ci-dessus).

  Note:

  Si le message suivant est affiché "Command *show config-files rules-scirius mon0* is not recognized", vérifier la configuration (multi tenant avec interface `mon0`).

Exemple pour afficher les règles scirius en mode multi tenant pour le vlan 10

- Entrer la commande suivante

```
(gcap-cli) show config-files rules-scirius VLAN 10
```

- Valider.
  Le système affiche le résultat (voir exemple ci-dessus).

> **Note:**
>
> Si le message suivant est affiché "Command *show config-files rules-scirius VLAN 10* is not recognized", vérifier la configuration (multi tenant avec VLAN 10).

Exemple pour afficher les seuils, les limites et les règles de suppression

- Entrer la commande suivante.

```
(gcap-cli) show config-files threshold
```

- Valider.
  Le système affiche le résultat.

```
suppress gen_id 1, sig_id 2435, track by_src, ip 10.10.10.10
threshold gen_id 1, sig_id 2435, type limit, track by_src, count 1, seconds 60)
```

  Le fichier affiche :
  - les seuils ou limites définis par le mot clé "threshold"
  - les règles de suppression définies par le mot clé "suppress"

6.2.1.7 cpus

Introduction

La commande `cpus` du sous-groupe `show` permet de lister l'ensemble des CPUs disponibles sur le GCap ainsi que leur pourcentage d'utilisation.

Prérequis

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

Commande

`show cpus`

Exemple pour afficher les CPUs et leur pourcentage d'utilisation

- Entrer la commande suivante.

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

- Valider.
  Le système affiche les informations courantes.

```
Linux 5.10.36-grsec (GCap)          19/01/22          _x86_64_        (12 CPU)

08:54:36     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice␣
↪  %idle
08:54:37     all    5.21    0.00    1.43    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  93.36
08:54:37       0    2.00    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.00
08:54:37       1    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00␣
↪ 100.00
08:54:37       2    1.01    0.00    1.01    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.98
08:54:37       3    1.01    0.00    1.01    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.98
08:54:37       4    1.01    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  98.99
08:54:37       5    0.00    0.00    1.01    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  98.99
08:54:37       6    1.01    0.00    1.01    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.98
08:54:37       7   52.00    0.00    7.00    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  41.00
08:54:37       8    1.00    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  98.00
08:54:37       9    1.01    0.00    1.01    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.98
08:54:37      10    1.01    0.00    2.02    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  96.97
08:54:37      11    1.02    0.00    1.02    0.00    0.00    0.00    0.00    0.00    0.00␣
↪  97.9
```

- Appuyer sur **CTRL** + **C** pour arrêter.
  Le système calcule les moyennes et les affiche.

6.2.1.8 datetime

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`.

Prérequis

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

Commande

```
show datetime
```

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
```

6.2.1.9 eve-stats

Introduction

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

Prérequis

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

Commande

```
show eve-stats
```

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*)

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

Exemple:

```
...
  Alerts: 0
...
```

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
  ...
```

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
...
```

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

- `<protocole>` Nombre d'événements observés par Sigflow à propos du protocole (e.g *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
```

Détail des compteurs `Detection Engine Stats` - Statistique 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
```

(suite sur la page suivante)

(suite de la page précédente)

```
        Bypassed:      0
```

6.2.1.10 gcenter-ip

Introduction

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

Prérequis

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

Commande

```
show gcenter-ip
```

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 alors le message suivant est affiché :

```
Current GCenter IP: None
```

6.2.1.11 health

Introduction

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

Prérequis

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

Commande

`show health`

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 `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*)

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,
```


(suite sur la page suivante)

(suite de la page précédente)

```
            "written_bytes": 4096
        }
    },
    ...
```

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,
                "system": 1830370,
                "user": 4138182
            }
        },
```

(suite sur la page suivante)

(suite de la page précédente)

```
        "interrupts": 12942835029,
        "processes_blocked": 0,
        "processes_running": 1
    },
    ...
```

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
        },
    },
    ...
```

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
    },
    ...
```

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
    },
    ...
```

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

- `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
    },
...
```

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,
```

(suite sur la page suivante)

(suite de la page précédente)


```
            "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
        }
    },
...
```

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 de 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
    },
...
```

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
    },
...
```

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

- `nodes` - Liste des nodes 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
            }
        }
    },
...
```


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
        }
    },
...
```

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 + etat "up"	signification
état "Container down" + "up" false	état moteur arrêté
état "Container down" + "up" true	état impossible: appli ne peut pas tourné 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
```


(suite sur la page suivante)

(suite de la page précédente)

```
    },
...
```

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

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

Exemple :

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

Détails des compteurs `uptime` - Temps de disponibilité

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

Exemple :

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

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
    }
}
...
```

6.2.1.12 interfaces

Introduction

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

- les interfaces de management (`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` :

- **State :** l'état configuré de l'interface parmi {**Enabled**|**Disabled**}
- **Physical Address :** l'adresse mac de l'interface
- **Speed :** la vitesse de l'interface
- **Type :**
  - s'il s'agit d'une interface virtuelle : **Virtual**
  - s'il s'agit d'une interface physique : le type de câble/sfp branché sur le port physique

---

Prérequis

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

---

Commandes

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

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.

```
Waiting 10s for interfaces to be up

Name     State      Physical Address   Status   Speed    Type          Vendor ID   Device ID
↪  PCI bus
gcp0     Enabled    00:50:56:01:29:01  UP       1Gb      RJ45          0x8086      0x10d3
↪  0b:00.0
gcp1     Disabled   00:50:56:01:29:02  UP       1Gb      RJ45          0x8086      0x10d3
↪  13:00.0
mon0     Enabled    00:50:56:01:29:03  UP       1Gb      RJ45          0x8086      0x10d3
↪  1b:00.0
mon1     Disabled   00:50:56:01:29:04  UP       1Gb      RJ45          0x8086      0x10d3
↪  04:00.0
```

(suite sur la page suivante)

(suite de la page précédente)

```
mon2     Disabled   00:50:56:01:29:05  UP       1Gb      RJ45         0x8086      0x10d3
↪  0c:00.0
mon3     Disabled   00:50:56:01:29:06  UP       1Gb      RJ45         0x8086      0x10d3
↪  14:00.0
monvirt  Enabled    N/A                UP       N/A      Virtual      N/A         N/A
↪  N/A
```

Note:

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

Si les interfaces ne sont pas reconnues, le système affiche des informations non pertinentes comme l'exemple ci-dessous :

```
Waiting 10s for interfaces to be up

Name     State      Physical Address   Status   Speed    Type          Vendor ID   Device ID
↪  PCI bus
eno12399 N/A        68:05:ca:dd:fe:fa  UP       1Gb      1000BASE-SX   0x8086      0x1572
↪  31:00.0
eno12409 N/A        68:05:ca:dd:fe:fb  UP       1Gb      1000BASE-SX   0x8086      0x1572
↪  31:00.1
eno12419 N/A        68:05:ca:dd:fe:fc  UP       1Gb      1000BASE-SX   0x8086      0x1572
↪  31:00.2
eno12429 N/A        68:05:ca:dd:fe:fd  UP       1Gb      1000BASE-SX   0x8086      0x1572
↪  31:00.3
eno8303  N/A        ec:2a:72:02:3a:1c  DOWN     N/A      RJ45          0x14e4      0x165f
↪  04:00.0
eno8403  N/A        ec:2a:72:02:3a:1d  DOWN     N/A      RJ45          0x14e4      0x165f
↪  04:00.1
monvirt  Disabled   N/A                UP       N/A      Virtual       N/A         N/A
↪  N/A
```

Dans ce cas, le système n'a pas pu associer chacune des interfaces réseau avec son nom.

Note:

Les interfaces étant non assignées, l'accès via la connexion SSH sur le port *gcpx* ne fonctionne pas.
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

Pour corriger ce problème, deux actions sont possibles :

- relancer manuellement une assignation en utilisant la commande *set advanced-configuration rescan-interfaces*,
- assigner manuellement les interfaces réseau en utilisant la commande *set advanced-configuration interface-names ...*

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
```

6.2.1.13 keymap

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).

Prérequis

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

Commande

```
show keymap
```

Exemple pour afficher la langue courante du clavier

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

- Valider.

Le système affiche les informations courantes.

```
Current keymap is fr
```

6.2.1.14 logs

Introduction

La commande `logs` du sous-groupe `show` permet d'afficher les différents fichiers de logs du GCap :

Table1: Introduction

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-cron
les informations sur l'activité des utilisateurs du GCap	var-log-user
les événements de debug	var-log-debug

Une explication détaillée est donnée dans le paragraphe *Fichiers de logs*.

Prérequis

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

Commande

```
show logs {detection-engine-logs|var-log-kernel|var-log-messages|var-log-auth|var-log-cron|var-log-daemo
```

Exemple pour afficher les événements du moteur de détection

Pour cette commande, le moteur de détection doit avoir été démarré.

- Entrer la commande suivante.

```
(gcap-cli) show logs detection-engine-logs
```

- Valider.

Le système affiche les événements du moteur de détection.

Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-detection-engine-logs*.

Exemple pour afficher les événements liés au noyau

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-kernel
```

- Valider.

Le système affiche les événements liés au noyau.
Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-kernel*.

Exemple pour afficher l'agrégation de différents journaux

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-messages
```

- Valider.

Le système affiche les informations de connexion.
Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-messages*.

Exemple pour afficher les informations d'authentification du GCap

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-auth
```

- Valider.

Le système affiche les informations de connexion.
Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-auth*.

Exemple pour afficher les informations de lancement des tâches planifiées

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-cron
```

- Valider.

Le système affiche les informations de lancement des tâches planifiées.

Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-cron*.

Exemple pour afficher les informations sur l'activité des différentes applications utilisées

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-daemon
```

- Valider.

Le système affiche les informations sur l'activité des différentes applications utilisées.

Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-daemon*.

Exemple pour afficher les informations sur l'activité des utilisateurs du GCap

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-user
```

- Valider.

Le système affiche les informations informations sur l'activité des utilisateurs du GCap.

Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-user*.

Exemple pour afficher les logs de debug

- Entrer la commande suivante.

```
(gcap-cli) show logs var-log-debug
```

- Valider.

Le système affiche les informations sur l'activité des utilisateurs du GCap.
Une explication détaillée est donnée dans le paragraphe *Fichiers de logs-var-log-debug*.

6.2.1.15 monitoring-engine

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)

Prérequis

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

---

Commande

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

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
```

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
```

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.

6.2.1.16 network-config

Introduction

Le GCap possède :

- interfaces de capture et de surveillance (`mon0` à `monx`),
- interfaces réseau (`gcp0`/`gcp1`) 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 l'interface␣
↪```gcp0```.
```

- **configuration double-interface**.

```
La communication VPN est gérée par l'interface ```gcp0```.

La connexion SSH pour la gestion du GCap est gérée par l'interface ```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 toutes les interfaces du GCap : commande `show network-config configuration`
- l'état pour uniquement les interfaces réseau : commande `show network-config status`
  - l'état pour chacune des interfaces : commande `show network-config gcp0` ou `show network-config gcp1`
  - l'état pour l'ensemble des interfaces réseau : commande `show network-config status`
- le nom du domaine : commande `show network-config domain`
- le nom d'hôte : commande `show network-config hostname`
- l'interface utilisée pour gérer la sonde en SSH : commande `show network-config ssh`
- la vitesse du lien VPN entre GCap et GCenter : commande `show network-config vpn-link speed`

Prérequis

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

---

Commandes

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

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.

Configuration simple-interface

Dans ce cas, le système affiche les informations de configuration réseau y compris de `gcp1` (non utilisée).

```
(gcap-cli) show network-config configuration
{
    "hostname": "GCap",
    "domain_name": "gatewatcher.com",
    "gcp0": {
        "description": "VPN / SSH",
        "ip_address": "X.X.X.X",
        "mask": "255.255.255.0",
        "default_gateway": "X.X.X.X",
        "enabled": true,
        "mtu": 1500
    },
    "gcp1": {
        "description": "SSH",
        "ip_address": "None",
        "mask": "255.255.255.0",
        "default_gateway": "",
        "enabled": false,
        "mtu": 1500
    },
    "mon0": {
        "description": "default",
        "enabled": true,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon1": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon2": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon3": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    }
}
```

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",
    "gcp0": {
        "description": "VPN",
        "ip_address": "X.X.X.X",
        "mask": "255.255.255.0",
        "default_gateway": "X.X.X.X",
        "enabled": true,
        "mtu": 1500
    },
    "gcp1": {
        "description": "SSH",
        "ip_address": ""X.X.X.X"",
        "mask": "255.255.255.0",
        "default_gateway": "255.255.255.0",
        "enabled": true,
        "mtu": 1500
    },
    "mon0": {
        "description": "default",
        "enabled": true,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon1": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon2": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    },
    "mon3": {
        "description": "default",
        "enabled": false,
        "filtering_rules": {},
        "mtu": 1500
    }
}
```

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
```

Exemple pour afficher la configuration de l'interface `gcp0`

- Entrer la commande suivante.

```
(gcap-cli) show network-config gcp0
```

- Valider.

Le système affiche la configuration de l'interface `gcp0`.

Suivant la configuration simple interface ou double interface, les informations sont différentes.

Les deux cas sont listés ci-après.

Configuration simple-interface : interface `gcp0`

Les connexions SSH et VPN sont gérées par l'interface `gcp0`.

Dans ce cas, le système affiche :

```
Interface ```gcp0``` configuration (VPN / SSH):
        - IP Address: X.X.X.X
        - Mask: 255.255.255.0
        - Gateway: X.X.X.X
```

Configuration double-interface : interface `gcp0`

La communication VPN est gérée par l'interface `gcp0`.

La connexion SSH pour la gestion du GCap est gérée par l'interface `gcp1`.

Dans ce cas, le système affiche :

```
Interface gcp0 configuration (VPN):
        - IP Address: X.X.X.X
        - Mask: 255.255.255.0
        - Gateway: X.X.X.X
```

Exemple pour afficher la configuration de l'interface gcp1

- Entrer la commande suivante.

```
(gcap-cli) show network-config gcp1
```

- Valider.

Le système affiche la configuration de l'interface gcp1.

Suivant la configuration simple interface ou double interface, les informations sont différentes.

Les deux cas sont listés ci-après.

Configuration simple-interface : interface gcp1

Dans ce cas, le système affiche les informations de gcp1 non utilisée :

```
Interface gcp1 configuration (SSH):
        - IP Address: None
        - Mask: 255.255.255.0
```

Configuration double-interface : interface gcp1

Dans ce cas, le système affiche les informations de gcp1 qui est utilisée :

```
Interface gcp1 configuration (SSH):
        - IP Address: X.X.X.X
        - Mask: 255.255.255.0
        - Gateway: X.X.X.X
```

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
```

Exemple pour afficher l'interface utilisée pour gérer la sonde en SSH

- Entrer la commande suivante.

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

- Valider.

Le système affiche l'interface SSH utilisée pour gérer le GCap.

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

```
SSH is using interface gcp0
```

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

```
SSH is using interface gcp1
```

Exemple pour afficher l'état des interfaces réseau `gcp0` et `gcp1` du GCap

- Entrer la commande suivante.

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

- Valider.

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

```
   Name          Address         Carrier      Speed           Type
   gcp0     xx:xx:xx:xx:xx:xx         UP    1000Mb/s          RJ45
   gcp1     xx:xx:xx:xx:xx:xx         UP    1000Mb/s          RJ45
```

Pour chaque interface, les informations suivantes sont affichées :

```
- ```Address``` : l'adresse mac de l'interface
- ```Carrier``` :
- valeur ```UP``` si l'interface physique est connectée
- valeur ```DOWN``` autrement
- ```Speed``` : la vitesse de l'interface en Mb/s
- ```Type``` : le type de câble/sfp branché sur le port physique
```

Exemple pour afficher la vitesse du lien VPN entre GCap et GCenter

- Entrer la commande suivante.

```
(gcap-cli) show network-config vpn-link speed
```

- Valider.

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

```
  Current VPN link speed: Fast
```

Le système affiche la valeur courante : ici `Fast`.

6.2.1.17 password-policy

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`*.

Prérequis

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

Commande

```
show password-policy
```

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 interfaces de détection disponibles.

```
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

6.2.1.18 passwords

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.

Prérequis

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

Commande

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

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
```

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"
```

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.

6.2.1.19 protocols-selector

Introduction

Cette commande est retirée depuis la version 2.5.3.105.

6.2.1.20 session-timeout

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.

Prérequis

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

Commande

```
show session-timeout
```

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.

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

6.2.1.21 setup-mode

Introduction

La commande `setup-mode` du sous-groupe `show` permet d'afficher :

- le niveau courant,
- l'interface de chaque profil utilisateur accessible :
  - interface graphique ou mode GUI
  - interface en ligne de commande ou mode CLI

Le mode par défaut est le mode CLI.

Le mode GUI est déprécié.

La possibilité de modifier ces choix est donnée par la commande *set setup-mode*.

Prérequis

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

Commande

```
show setup-mode
```

Exemple pour afficher le mode des profils utilisateurs

- Entrer la commande suivante.

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

- Valider.

```
Current default setup modes:
        - gview: cli mode
        - gviewadm: cli mode
        - setup: cli mode
```

Ceci signifie que :

- l'utilisateur courant est setup (niveau le plus haut affiché)
- lors du prochain accès, chaque utilisateur va se connecter en mode CLI

6.2.1.22 status

Introduction

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

Prérequis

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

Commande

```
show status
```

Exemple pour afficher les informations du GCap

- Entrer la commande suivante.

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

- Valider.

```
status

GCap Name          : GCap
Version            : 2.5.3.105
Paired on GCenter  : Not paired
Tunnel status      : Down
Detection Engine   : Container down

© Copyright GATEWATCHER 2021
```

Le système affiche les informations suivantes :

- **GCAP name** : nom du GCap (ici GCap)
- **Version** : version courante du logiciel : ici 2.5.3.105
- **Tunnel status** : état du tunnel entre GCap et GCenter (ici non appairé **Not paired**)
- **Detection Engine** : état du container du moteur de détection (ici non démarré **Container down**)

6.2.1.23 tech-support

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.

Prérequis

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

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.

Commande pour extraire un tech-support allégé

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

Commande pour extraire un tech-support standard

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

Commande pour extraire un tech-support verbeux

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

6.2.1.24 advanced-configuration

cpu-config

Introduction

La commande `cpu-config` du sous-groupe `show advanced-configuration` permet d'afficher le nombre de CPU dédié au moteur de détection Sigflow.

Prérequis

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

---

Commande

```
show advanced-configuration cpu-config
```

Exemple pour afficher les CPUs attribués à Sigflow

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration cpu-config
```

- Valider.

Le système affiche le nombre de CPU dédié au moteur de détection Sigflow.

```
Current CPU profile is 1/2
```

Dans cet exemple, il y a 1 CPU dédié sur 2 présents.

haute disponibilité par mise en redondance de 2 GCaps

Introduction

La commande `status` du sous-groupe `show advanced-configuration high-availability` permet d'afficher l'état du GCap.

La commande `configuration` du sous-groupe `show advanced-configuration high-availability` permet d'afficher la configuration de la haute disponibilité du GCap.

La commande `pubkey` du sous-groupe `show advanced-configuration high-availability` permet d'afficher la clé publique utilisée par la haute disponibilité.

Fonctionnement : Se référer au paragraphe *Fonctionnement de la haute disponibilité*.

Type de configuration réseau :

- **liaison avec 1 interface :** `mon0` est remplacée par `ha0`, on peut donc utiliser les interfaces de capture à partir de `mon1`
- **liaison avec 2 interfaces :** `mon0` et `mon1` sont remplacées par `ha0` et `ha1`, on peut donc utiliser les interfaces de capture à partir de `mon2`

Un GCap `leader` devient `follower` dans les conditions suivantes :

- Perte de la liaison avec le GCenter pendant 1 min
- Perte du moteur de détection pendant 5 min

Prérequis

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

---

Commande

```
show advanced-configuration high-availability {status|configuration|pubkey}
```

Exemple pour afficher l'état de la haute disponibilité (redondance des GCaps)

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration high-availability status
```

- Valider.

Le système affiche le résultat sur le GCap connecté.

```
Current high-availability status:
    - status: Operational [unhealthy]
    - paired GCap: fe80::233
    - leader: Leader
    - time since last status: Unknown
    - Leader since: 2022-01-21T15:35:09Z
```

Les compteurs affichés sont :

- **status :** état du GCap :
  - Operational : ok
  - unhealthy : si le GCap n'est pas connecté au GCap voisin.
- **paired GCap :** adresse IPv6 du GCap voisin.
- **leader :** état de l'élection parmi :
  - Leader
  - Follower.
- **time since last status :** temps écoulé depuis le dernier healthcheck du GCap voisin.
- **Leader since :** date à laquelle le GCap est devenu Leader.

Exemple pour afficher la clé publique utilisé par la haute disponibilité

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration high-availability pubkey
```

- Valider.

Le système affiche la clé publique.

```
Wireguard public key: 'FypsdignOR6aRP9j5pJkTcAJoi4eE/gTV9McCpBYjAk='
```

Exemple pour afficher la configuration de la haute disponibilité du GCap

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration high-availability configuration
```

- Valider.

Le système affiche le résultat.

```
Current high-availability configuration [enabled]:
    - bonding enabled: disabled
    - public ip: fe80::149/128
    - multicast group: ff02::200
    - peer public IP: fe80::233
    - peer public key: 2wtmY/oCaoUGreyr2CROnKAIoEgTXkSOedXlXDvUfBU=
    - shared secret: Xxf4fknh4KoOH2zgrI4Wyw==
```

- **bonding enabled :**
  - enabled : si l'agrégation est activée
  - disabled : autrement.
- **public ip :** Adresse IPv6 du GCap parmi :
  - **Link-local :** Si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.

  - **ULA (Unique Local Address) :** Si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** Si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64.
- **multicast group :** Adresse IPv6 multicast pour la communication entre les GCaps. Plage FF00::/8. Ex : FF02::200.
- **peer public IP :** Adresse IPv6 du GCap voisin parmi :
  - **Link-local :** Si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.
  - **ULA (Unique Local Address) :** Si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** Si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64.
- **peer public key :** Clé publique du GCap voisin via la commande `show advanced-configuration high-availability pubkey`.
- **shared secret :** Secret de 16 octets encodé en base 64 qui doit être identique entre les 2 GCaps.

interface-names

Introduction

La commande `interface-names` du sous-groupe `advanced-configuration` permet d'afficher le nom des interfaces.

Prérequis

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

---

Commande

```
show advanced-configuration interface-names
```

Exemple pour afficher les noms des interfaces

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration interface-names
```

- Valider.

Le système affiche le nom des interfaces.

load-balancing

Introduction

La commande `load-balancing` du sous groupe `show advanced-configuration` permet d'afficher la configuration d'équilibrage de charge venant de l'interface de capture `monx` listée vers les CPU du GCap.

Note:

La fonctionnalité est compatible avec certains modèles de GCap (voir datasheet des modèles).

Prérequis

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

---

Commande

```
show advanced-configuration load-balancing
```

Exemple pour afficher la configuration du load balancing

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration load-balancing
```

- Valider.

```
Showing current load balancing configuration

Interface mon2:
  - Load balancing method: XDP
  - Load balancing algorithm: 5-tuple
  - Seed: 1
```

local-rules

Introduction

La commande `local-rules` du sous-groupe `show advanced-configuration` permet d'afficher :

- dans la rubrique `Rules` : les règles locales de Sigflow, c'est-à-dire :
  - les règles de détection et
  - les règles de reconstruction de fichiers
- dans la rubrique `threshold` :
  - les seuils ou limites définis par le mot clé "threshold"
  - les règles de suppression définies par le mot clé "suppress"

Il est possible d'afficher uniquement les règles du tenant configuré.

Si la sonde est configurée en mode single tenant alors seul le fichier local_all.rules pourra être affiché.

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

Prérequis

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

---

Commande

```
show advanced-configuration local-rules {TENANT|list}
```

Le paramètre TENANT peut prendre les valeurs suivantes :

- single-tenant : all
- multi-tenant par int : {mon0|mon1|mon2|mon3|monvirt}
- multi-tenant par vlan :
  - default
  - VLAN X
  - VLAN X Y

Exemple pour lister les fichiers de règles consultables

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration local-rules list
```

- Valider.

Le système affiche le résultat.

```
Available rule files:
    - mon0
    - monvirt
```

Exemple pour lister les fichiers de règles consultables afficher les règles en mode single tenant

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration local-rules all
```

- Valider.

Le système affiche le résultat.

```
Rules:
alert dns any any -> any any (msg:"[ TEST AUTO ] ALERT DNS UDP";sid:12345600;priority:2;)

Thresholds
```

Le résultat est affiché en deux catégories :

- **rules** : dans cette catégorie, sont listées les règles définies localement
- **Thresholds** : dans cette catégorie, sont listés les seuils et limites définies localement

---

Exemple pour afficher les règles en mode multi tenant pour l'interface mon0

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration local-rules mon0
```

- Valider.

Le système affiche le résultat.

```
Displaying rules for mon0

Rules:
alert dns any any -> any any (msg:"[ TEST AUTO ] ALERT DNS UDP";sid:12345600;priority:2;)

Thresholds
```

Exemple pour afficher les règles en mode multi tenant pour le vlan 10

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration local-rules VLAN 10
```

- Valider.

Le système affiche le résultat.

```
Displaying rules for vlan 10

Rules:
alert dns any any -> any any (msg:"[ TEST AUTO ] ALERT DNS UDP";sid:12345600;priority:2;)

Thresholds
```

MTU

Introduction

La commande `mtu` du sous-groupe `show advanced-configuration` permet d'afficher la valeur en octets de la MTU de toutes les interfaces réseau activées.

Prérequis

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

---

Commande

```
show advanced-configuration mtu
```

Exemple pour afficher la valeur de la MTU

- Entrer la commande suivante.

```
(gcap-cli) show advanced-configuration mtu
```

- Valider.

Le système affiche le résultat.

```
Current Network MTU configuration:
        - mon1: 1500
        - mon2: 1500
        - mon3: 1500
        - cluster0: 1500
        - gcp0: 1500
```

Les valeurs sont affichées pour toutes les interfaces réseau actives.

packet-filtering

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.

Prérequis

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

Commande

```
show advanced-configuration packet-filtering
```

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

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*.

Prérequis

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

Commandes

```
set bruteforce-protection {lock-duration|eve-compress|eve-upload|file-extraction|file-upload|filter-file
```

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}
```

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

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

Commande pour restaurer la configuration par défaut

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

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

Introduction

La commande `clusters` du sous-groupe `set` permet de configurer l'agrégation sur les interfaces de capture du GCap.

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*.

Cette commande permet de définir les interfaces qui sont raccordées au même TAP afin d'avoir une interprétation correct du flux.

Note:

Cette fonctionnalité est nécessaire si le TAP qualifié présent dans l'architecture n'assure pas la fonctionnalité d'agrégation d'interfaces.
Le cluster hérite automatiquement de la MTU de l'interface ayant la plus haute MTU dans le groupement.

L'agrégation a des *Impacts sur les autres fonctionnalités*.

Prérequis

- **Utilisateur :** setup
- **Dépendances :** activation de deux interfaces de capture au minimum

---

Commandes

Commande pour ajouter une agrégation d'interfaces

```
(gcap-cli) set clusters add interfaces {mon0|mon1|mon2|mon3} {mon0|mon1|mon2|mon3} description
DESCRIPTION
```

Commande pour activer ou désactiver une agrégation d'interfaces

```
(gcap-cli) set clusters {enable|disable} NAME
```

Le champ `NAME` est visualisable par la commande `show clusters`.

Commande pour supprimer une agrégation d'interfaces

```
(gcap-cli) set clusters delete NAME
```

Exemple pour créer une agrégation des interfaces `mon0` et `mon1` avec la description `test`

- Entrer la commande suivante.

```
(gcap-cli) set clusters add interfaces mon0 mon1 description `test`
```

- Valider.

Le système affiche le résultat.

```
Creating cluster test with interfaces mon0, mon1
Successfully created cluster `test`
```

6.2.2.3 compatibility-mode

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 :

- 2.5.3.100: GCenter 2.5.3.100 et inférieur
- 2.5.3.101: GCenter 2.5.3.101
- 2.5.3.102+: GCenter 2.5.3.102 et supérieur

Note:

Le mode de compatibilité avec la version 2.5.3.100 et inférieur est déprécié.

Prérequis

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

---

Commande

```
set compatibility-mode {2.5.3.100|2.5.3.101|2.5.3.102+}
```

Exemple pour configurer la compatibilité avec un GCenter 2.5.3.101

- Entrer la commande suivante.

```
(gcap-cli) set compatibility-mode 2.5.3.101
```

- Valider.

6.2.2.4 datetime

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 (exemple : pour l'horodatage des événements).

Prérequis

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

Commande

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

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

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.

Prérequis

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

---

Commande

```
set gcenter-ip {GCenter-IP}
```

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

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.

Important:

Les interfaces composant une agrégation d'interfaces ("cluster"), ne peuvent être ni activées ni désactivées.

Prérequis

- **Utilisateur :** setup
- **Dépendances :**
  - le moteur de détection doit être à l'arrêt
  - pour activer une interface, elle doit être dans l'état désactivé
  - pour désactiver une interface, elle doit être dans l'état activé

Commande

Pour modifier le délai avant le démarrage des interfaces :
`set interfaces delay SECOND`

Pour activer ou désactiver des interfaces : `set interfaces {enable|disable} {mon0|mon1|mon2|mon3|monvirt}`

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

- Entrer la commande suivante.

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

- Valider.

Exemple pour activer l'interface de capture `mon0`

- Entrer la commande suivante.

```
(gcap-cli) set interfaces enable mon0
```

- Valider.

Note:

Si le système affiche le message suivant, *Command set interfaces enable monx is not recognized* est affiché, vérifier si l'interface monx constitue une agrégation à l'aide de la commande *show clusters*.

Exemple pour désactiver l'interface de capture `mon1`

- Entrer la commande suivante.

```
(gcap-cli) set interfaces disable mon1
```

- Valider.

Note:

Si le système affiche le message suivant, *Command set interfaces disable monx is not recognized* est affiché, vérifier si l'interface monx constitue une agrégation à l'aide de la commande *show clusters*.

6.2.2.7 keymap

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).

Prérequis

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

Commande

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

Exemple de clavier français

- Entrer la commande suivante.

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

- Valider.

Le système affiche le résultat.

```
Setting keymap to fr
```

Exemple de clavier anglais

- 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

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.

Prérequis

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

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.

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
```

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
```

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
```

Exemple pour activer la vérification des interfaces de capture

- Pour désactiver 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

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 du domaine : commande `set network-config domain NAME_value`
- le nom d'hôte : commande `set network-config hostname HOSTNAME_value`
- l'interface utilisée pour gérer la sonde en SSH : commande `set network-config ssh {gcp0|gcp1}`
- la vitesse du lien VPN entre GCap et GCenter : commande `set network-config vpn-link speed {slow|fast}`
  - Le paramètre slow définit un lien inférieur à 100Mbit/s.
  - Le paramètre fast définit un lien supérieur à 100Mbit/s.

Prérequis

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

---

Commande

`set network-config {gcp0|gcp1} [ip-address IP_value] [gateway GATEWAY_value] [mask MASK_value] [confirm] [no-reload]`

`set network-config ssh {gcp0|gcp1} [confirm] [no-reload]`

`set network-config [domain-name NAME_value|hostname HOSTNAME_value] [confirm]` `set network-config vpn-link speed {slow|fast}`

Note:

L'option *no-reload* permet de ne pas recharger les services réseau.

Exemple pour configurer l'interface `gcp0` pour l'appairage et l'interface `gcp1` pour la gestion

- Entrer la commande suivante.

```
(gcap-cli) set network-config ssh gcp1
```

- Valider.
- Entrer la commande suivante.

```
(gcap-cli) set network-config gcp0 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 gcp1 ip-address Y.Y.Y.Y gateway Z.Z.Z.Z mask Z.Z.Z.Z confirm
```

- Valider.

Exemple pour configurer l'interface `gcp0` pour l'appairage et pour la gestion

Note:

L'interface `gcp1` n'est pas utilisée.

- Entrer la commande suivante.

```
(gcap-cli) set network-config ssh gcp0
```

- Valider.
- Entrer la commande suivante.

```
(gcap-cli) set network-config gcp0 ip-address X.X.X.X gateway X.X.X.X mask X.X.X.X confirm
```

- Valider.

Exemple pour modifier le domaine du GCap en gatewatcher.com

- Pour modifier le domaine du GCap en 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.

```
Applying configuration...

00% Generating interfaces configuration     [OK]
09% Generating network configuration        [OK]
18% Generating sshd configuration           [OK]
27% Reconfiguring network                   [OK]
36% Reconfiguring firewall                  [OK]
45% Notifying new network addresses         [OK]
54% Restarting sshd service                 [OK]
63% Restarting rsyslog service              [OK]
72% Restarting gcenter-xfer-daemon service  [OK]
81% Restarting netdata service              [OK]
90% Restarting rsyslog service              [OK]
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
```

Exemple pour modifier la vitesse du lien VPN entre GCap et GCenter (par exemple passer de fast à slow)

- Pour visualiser la vitesse courante :
  - Entrer la commande suivante.

```
(gcap-cli) show network-config vpn-link speed
```

  - Valider.

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

```
Current VPN link speed: Fast
```

Le système affiche la valeur courante : ici `Fast`.

- Pour modifier la vitesse courante (de fast vers slow) :
  - Entrer la commande suivante.

```
(gcap-cli) set network-config vpn-link speed slow
```

  - Valider.

Le système affiche le résultat de la modification de la configuration.

```
New VPN link qualifiers configured successfully
```

6.2.2.10 password-policy

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.

Prérequis

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

Commande

Pour définir les options de complexité du mot de passe :

```
(gcap-cli) set password-policy {lowercase-optional|lowercase-required|uppercase-optional|uppercase-requi
```

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}
```

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.` ``

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

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 modifer le mot de passe (commande *show keymap*).

Prérequis

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

Commande

```
set passwords {setup|gviewadm|gview}
```

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
```

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

Introduction

Cette commande est retirée depuis la version 2.5.3.105.

6.2.2.13 session-timeout

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.

Prérequis

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

Commande

```
set session-timeout MINUTES
```

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

Introduction

La commande `setup-mode` du sous-groupe `set` permet de choisir, pour chaque profil utilisateur, :

- soit l'interface graphique (mode GUI)
- soit l'interface en ligne de commande (mode CLI)

Le mode CLI est activé par défaut sur l'ensemble des profils utilisateurs (setup, gview, gviewadm).

La modification de cette configuration est possible à tout moment et n'a aucun impact sur le fonctionnement global du GCap.

Note:

Le mode GUI est déprécié et sera retiré dans une future version.

La possibilité d'afficher la configuration courante est donnée par la commande *show setup-mode*.

Prérequis

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

Commande

```
set setup-mode {setup|gview|gviewadm} {gui|cli}
```

Exemple pour changer le mode par défaut du profil utilisateur setup vers le mode CLI

- Entrer la commande suivante.

```
(gcap-cli) set setup-mode setup cli
```

- Valider.
Le système affiche change le mode par défaut pour le mode CLI.

```
Setting setup to mode cli
Default setup mode successfully updated. Changes will be effective on next login
```

Comme indiqué, le changement se fera à la prochaine connexion.

Note:

Si le message suivant est affiché :

```
User setup is already set to mode cli
Default setup mode successfully updated.
Changes will be effective on next login
```

cela signifie que le mode courant est en mode CLI mais, par sécurité, il est appliqué de nouveau.

6.2.2.15 ssh-keys

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 :

- RSA 2048 ou 4096
- ssh-ed25519
- ecdsa-sha2-nistp256.

Prérequis

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

Commande

```
set ssh-keys {setup|gviewadm|gview} "ssh-rsa ...\nssh-rsa
```

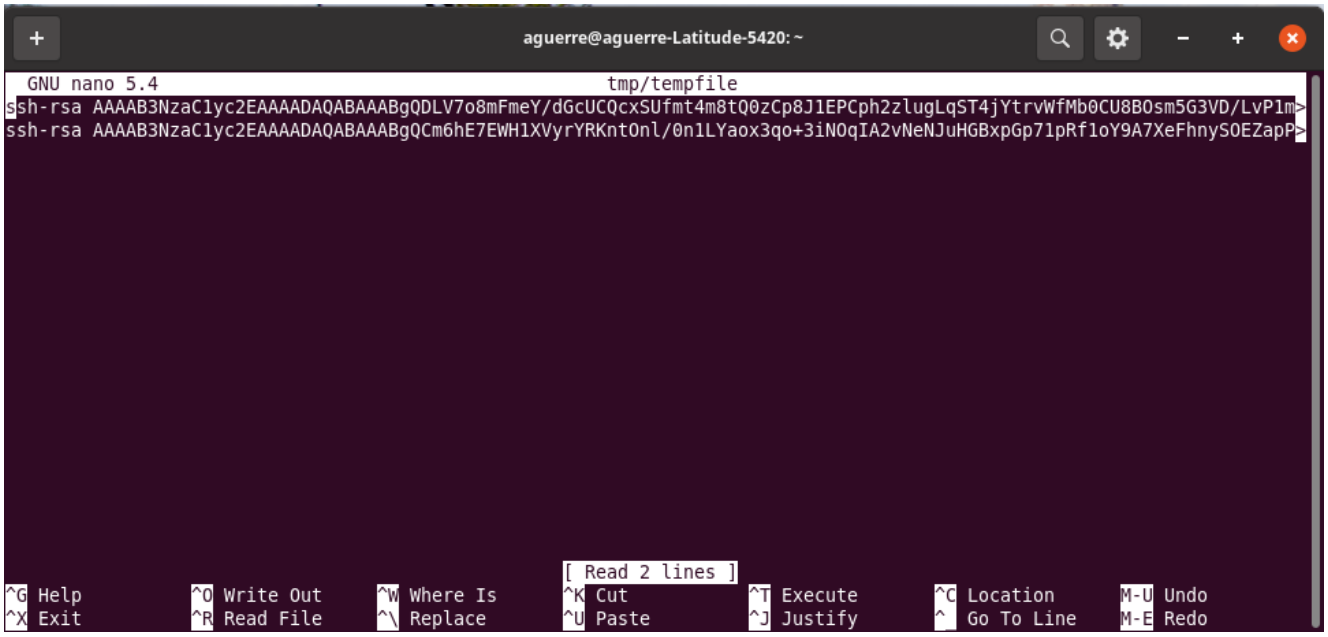
Exemple pour utiliser l'éditeur de texte

- 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 commencant par ssh-rsa.
- Pour sortir, appuyer sur **CTRL** + **X**.
- Enregistrer les modifications si besoin.

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

cpu-config

Introduction

La commande `cpu-config` du sous-groupe `advanced-configuration` permet de modifier le nombre de CPU dédié au moteur de détection Sigflow.

Cette attribution de CPU peut se faire en sélectionnant :

- la répartition des CPU pour Sigflow p/r au total des CPU présents : paramètre (`1/2`, `2/3`, `3/4`, `4/5`)
- les numéros des CPU réservés pour Sigflow

Important:

Ne pas excéder 80% des CPU pour Sigflow.

Prérequis

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

---

Commande

```
set advanced-configuration cpu-config {1/2|2/3|3/4|4/5|custom} [CPU_LIST]
```

Exemple pour attribuer la moitié des CPUs à Sigflow

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration cpu-config 1
```

- Valider
  Le système affiche l'action demandée.

```
Updating CPU profile from 3/4 to 1/2
```

Exemple pour attribuer une liste de CPUs à Sigflow

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration custom 1,2,3,4,5
```

- Valider.

```
cpu-config custom 1,2,3,4,5
Building custom profile 1,2,3,4,5
```

- Redémarrer le GCap, sans quoi, le comportement pourra s'avérer aléatoire.

high-availability

Introduction

La commande `high-availability` du sous-groupe `advanced-configuration` permet de configurer la haute disponibilité entre 2 GCap (fonction ajoutée à partir de la version 2.5.3.105).

Fonctionnement :

Se référer au paragraphe *Fonctionnement de la haute disponibilité*.

Type de configuration réseau :

- **liaison avec 1 interface :** `mon0` est remplacée par `ha0`
  Les interfaces de capture disponibles sont donc `mon1`, `mon2`, etc
- **liaison avec 2 interfaces :** `mon0` et `mon1` sont remplacées par `ha0` et `ha1`.
  Les interfaces de capture disponibles sont donc `mon2`, `mon3`, etc.

Un GCap `leader` devient `follower` dans les conditions suivantes :

- perte de la liaison avec le GCenter pendant 1 min
- perte du moteur de détection pendant 5 minutes

Prérequis

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

---

Commande

```
set advanced-config high-availability [public-ip IPV6/MASK] [gateway GATEWAY|null]
[peer-ip IPV6] [multicast-group IPV6] [shared-secret SECRET] [peer-pubkey KEY]
[bonding-enabled|bonding-disabled]
```

```
set advanced-config high-availability [enable|disable] [confirm]
```

Explication des paramètres :

- **bonding-enabled :** activer l'agrégation des cartes `mon0` + `mon1`.
- **bonding-disabled :** désactiver l'agrégation des cartes `mon0` + `mon1`.
- **enable :** activer la haute disponibilité.
- **disable :** désactiver la haute disponibilité.
- **gateway :** adresse IPv6 de la passerelle dans le cas où les GCap ne sont pas dans le même sous-réseau.

- **multicast-group :** adresse IPv6 multicast pour la communication entre les GCaps. Plage FF00::/8. Ex : FF02::200.
- **peer-ip :** adresse IPv6 du GCap voisin parmi:
  - **Link-local :** si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.
  - **ULA (Unique Local Address) :** si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64.
- **peer-pubkey :** Clé publique du GCap voisin via la commande `show advanced-configuration high-availability pubkey`.
- **public-ip :** adresse IPv6 du GCap parmi:
  - **Link-local :** si les GCap sont dans le même sous-réseau. Plage FE80::/10. Ex : FE80::100/64.
  - **ULA (Unique Local Address) :** si les GCap sont dans des sous-réseaux différents. Plage FD00::/7. Ex : FD00::100/64.
  - **Global Unicast :** si les GCap doivent communiquer via internet. Plage 2001::/3. Ex : 2001::1/64.
- **shared-secret :** secret de 16 octets encodé en base64 qui doit être identique entre les 2 GCaps.

Exemple pour configurer la haute disponibilité sur le premier GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability peer-ip fe80::XXX public-ip␣
↪fe80::YYY multicast-group ff02::200 peer-pubkey 2wtmY/
↪oCaoUGreyr2CROnKAIoEgTXkSOedXlXDvUfBU= shared-secret Xxf4fknh4KoOH2zgrI4Wyw==
```

Le système affiche le résultat.

```
Updating HA configuration
High availability configuration successfully updated
```

Exemple pour configurer la haute disponibilité sur le deuxième GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability peer-ip fe80::YYY public-ip␣
↪fe80::XXX multicast-group ff02::200 peer-pubkey␣
↪xehXnrigZOIZZEvWbWri8XegNhOKaAQk8vC6mKj27Ug= shared-secret Xxf4fknh4KoOH2zgrI4Wyw==
```

Le système affiche le résultat.

```
Updating HA configuration
High availability configuration successfully updated
```

Exemple pour activer la haute disponibilité sur chaque GCap

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration high-availability enable confirm
```

Le système affiche le résultat.

```
Interfaces naming rules updated, reloading configuration
Operation successful.
High availability configuration successfully updated
```

Exemple pour générer un secret partagé avec le script Python suivant

```
import base64
import secrets

shared_secret = base64.b64encode(secrets.token_bytes(16))
```

interface-names

Introduction

La commande `interface-names` du sous-groupe `set advanced-configuration` permet d'effectuer :

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

Prérequis

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

---

Commandes

`set advanced-configuration interface-names {{<PCI-ID> <name>...}|reset}`

Exemple pour assigner manuellement les interfaces du GCap

- Pour vérifier la nécessité de faire l'assignation des interfaces
  - Entrer la commande suivante.

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

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

```
Waiting 10s for interfaces to be up

Name    State    Physical Address  Status Speed Type    Vendor ID Device ID PCI bus
gcp0    Enabled  00:50:56:01:29:01 UP     1Gb   RJ45    0x8086    0x10d3    0b:00.0
gcp1    Disabled 00:50:56:01:29:02 UP     1Gb   RJ45    0x8086    0x10d3    13:00.0
mon0    Enabled  00:50:56:01:29:03 UP     1Gb   RJ45    0x8086    0x10d3    1b:00.0
mon1    Disabled 00:50:56:01:29:04 UP     1Gb   RJ45    0x8086    0x10d3    04:00.0
mon2    Disabled 00:50:56:01:29:05 UP     1Gb   RJ45    0x8086    0x10d3    0c:00.0
mon3    Disabled 00:50:56:01:29:06 UP     1Gb   RJ45    0x8086    0x10d3    14:00.0
monvirt Enabled  N/A               UP     N/A   Virtual N/A       N/A       N/A
```

    Dans ce cas, les noms des interfaces sont corrects. L'assignation existante a bien été faite.
    Exemple d'un cas de défaut :

```
Name     State     Physical Address   Status Speed  Type         Vendor ID Device ID␣
↪PCI bus
eno12399 N/A       68:05:ca:dd:fe:fa  UP     1Gb    1000BASE-SX  0x8086    0x1572   ␣
↪31:00.0
eno12409 N/A       68:05:ca:dd:fe:fb  UP     1Gb    1000BASE-SX  0x8086    0x1572   ␣
↪31:00.1
eno12419 N/A       68:05:ca:dd:fe:fc  UP     1Gb    1000BASE-SX  0x8086    0x1572   ␣
↪31:00.2
eno12429 N/A       68:05:ca:dd:fe:fd  UP     1Gb    1000BASE-SX  0x8086    0x1572   ␣
↪31:00.3
eno8303  N/A       ec:2a:72:02:3a:1c  DOWN   N/A    RJ45         0x14e4    0x165f   ␣
↪04:00.0
eno8403  N/A       ec:2a:72:02:3a:1d  DOWN   N/A    RJ45         0x14e4    0x165f   ␣
↪04:00.1
monvirt  Disabled  N/A                UP     N/A    Virtual      N/A       N/A      ␣
↪N/A
```

Note:

Les interfaces étant non assignées, l'accès via la connexion SSH sur le port *gcpx* ne fonctionne pas. Donc seuls, sont possibles :

- les accés physiques ou
- via l'accès web sur la console de gestion (iDRAC) ou
- via la connexion SSH sur le port iDRAC

Dans ce cas, le système n'a pas pu associer chacune des interfaces réseau avec son nom.

- Pour corriger ce problème, effectuer la procédure suivante.

Astuce:

Pour effectuer l'assignation, il faut utiliser le ID *PCI Bus*.

Pour l'ensemble des interfaces, il y a 3 parties :
- un ensemble de 4 interfaces correspondant aux interfaces de capture `mon0` à `monx`
- un ensemble de 2 interfaces correspondant aux interfaces de gestion `gcp0` à `gcp1`
- la ligne `monvirt` qui n'est pas à affecter

donc l'affectation à effectuer est la suivante en triant par :
- vendor ID
- device ID
- adresse physique (PCI bus)

Dans cet exemple, ceci donne :

Nom détecté (Name)	Vendor ID	Device ID	PCI bus	NOM à assigner
eno12399	0x8086	0x1572	31:00.0	`mon0`
eno12409	0x8086	0x1572	31:00.1	`mon1`
eno12419	0x8086	0x1572	31:00.2	`mon2`
eno12429	0x8086	0x1572	31:00.3	`mon3`
eno8303	0x8086	0x165f	04:00.0	`gcp0`
eno8403	0x8086	0x165f	04:00.1	`gcp1`
monvirt	N/A	N/A	N/A	pas d'assignation

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration interface-names 0x165f 31:00.0 mon0 31:00.1 mon1␣
↪31:00.2 mon2 31:00.3 mon3 04:00.0 gcp0 04:00.1 gcp1
```

- Valider.

Exemple pour réinitialiser l'assignation courante et revenir à une assignation automatique

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration interface-names reset
```

- Valider.
  Le système affiche le message suivant :

```
Network interfaces will be refreshed and corresponding configuration applied
Rebooting in 10 seconds...
You can still abort by pressing CTRL+C.
```

load-balancing

Introduction

The `load-balancing` command of the `set advanced-configuration` subgroup enables an advanced load balancing configuration of the captured flows per capture interface using load balancing methods (algorithm).

Below are the configuration options:

- the `kernel-native (RPS)` method is configured by default on all capture interfaces
- the `custom (XDP)` method enables advanced configuration:
  - Algorithm `3-tuple`: enables choosing an algorithm with three tuples (VLAN ID + IP Addresses + IP Protocol) for load balancing captured flows
  - algorithm `5-tuple`: enables choosing an algorithm with five tuples (VLAN ID + IP Addresses + IP Protocol + L4 Ports if applicable) for load balancing the captured flows

– keyword `seed`: enables defining a seed to better distribute the identical traffic

Note:

The functionality is compatible with some GCap models (see model datasheet).

Prerequisites

- **User:** setup
- **Dependencies:** the detection engine must be switched off

---

Command with kernel-native method

```
set advanced-configuration load-balancing method kernel-native
```

Command with custom method (XDP)

```
set advanced-configuration load-balancing method custom algorithm {3-tuple|5-tuple} seed
INTEGER
```

Help

Help on the set advanced-configuration load-balancing command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing  ?
```

- Validate.
  The system displays:

```
Update current load balancing configuration
===========================================

Available commands:
  - mon2: Update load balancing configuration for interface mon2
  - confirm: Accept the risks and confirm running the procedure
```

Help on the set advanced-configuration load-balancing mon2 command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing mon2 ?
```

- Validate.
  The system displays:

```
Update load balancing configuration for interface mon2
======================================================

Available commands:
  - method: Set load balancing method for interface
  - algorithm: Set load balancing algorithm for interface (custom mode only)
  - seed: Set load balancing seed for interface (custom mode only)
  - confirm: Accept the risks and confirm running the procedure
```

Help on the set advanced-configuration load-balancing mon2 method command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing  mon2 method ?
```

- Validate.
  The system displays:

```
Set load balancing method for interface
=======================================

Available commands:
  - kernel-native: Set load balancing to kernel native method (RPS)
  - custom: Set load balancing to custom (XDP)
```

Help on the set advanced-configuration load-balancing mon2 custom command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing  mon2 method custom ?
```

- Validate.
  The system displays:

```
Set load balancing to custom (XDP)
==================================

Available commands:
   - mon2: Update load balancing configuration for interface mon2
   - algorithm: Set load balancing algorithm for interface (custom mode only)
   - seed: Set load balancing seed for interface (custom mode only)
   - confirm: Accept the risks and confirm running the procedure
```

Help on the set advanced-configuration load-balancing mon2 method custom algorithm command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing  mon2 method custom algorithm ?
```

- Validate.
  The system displays:

```
Set load balancing algorithm for interface (custom mode only)
=============================================================

Available commands:
  - 3-tuple: Set load balancing algorithm to 3-tuple
  - 5-tuple: Set load balancing algorithm to 5-tuple
```

Help on the set advanced-configuration load-balancing mon2 method custom algorithm 5-tuple seed command

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing  mon2 method custom algorithm 5-
↪tuple seed ?
```

- Validate.
  The system displays:

```


Set load balancing seed for interface (custom mode only)
========================================================

Available commands:
  - <seed>: Set the load balancing seed (positive integer)
```

Example of applying the custom XDP method with a 5-tuple algorithm for the mon2 interface

- Enter the following command.

```
(gcap-cli) set advanced-configuration load-balancing mon2 method custom algorithm 5-tuple
```

- Validate.

```
This feature is experimental and possibly unstable.
Traffic may become corrupted and detection might fail.
Here be dragons.
Please type 'CONFIRM' in uppercase to continue
```

- Enter `CONFIRM`.

```
Updating load balancing methods
Updating method for interface mon2
Done.

Updating load balancing parameters
Updating parameters for interface mon2
```

local-rules

Introduction

La commande `local-rules` du sous-groupe `set advanced-configuration` permet de modifier les règles locales de la sonde GCap.

Ces règles peuvent être globales ou par interface.

Ces modifications sont fait localement dans le GCap donc non visibles volontairement au niveau du GCenter.

Détail sur les Règles

Les règles modifiées localement sont :

- dans le fichier `Rules:`, les règles locales de Sigflow, c'est-à-dire :
  - les règles de détection et
  - les règles de reconstruction de fichiers
- dans le fichier `threshold:`:
  - les seuils ou limites définis par le mot clé "threshold"
  - les règles de suppression définies par le mot clé "suppress"

Cas d'utilisation

Il y a plusieurs cas d'utilisation :

- rendre des signatures confidentielles sans que les opérateurs du GCenter puissent les voir (notion de 'besoin d'en connaître')
- faire une modification des signatures locales des sondes dans des cas complexes
- lorsque le GCenter est confié à un tiers et que ce dernier ne peut manier des marqueurs ou des signatures d'un certain niveau.

Note:

En multi tenant, il est possible de modifier uniquement les règles pour une seule interface de capture (tenant configuré) : il y a un fichier par interface.
En mode single tenant, les modifications s'appliquent à toutes les interfaces à la fois : il y a un fichier unique pour toutes les interfaces.

Prérequis

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

---

Commande

`set advanced-configuration local-rules TENANT`

Le paramètre TENANT peut prendre les valeurs suivantes :

- single-tenant : all
- multi-tenant par int : {mon0|mon1|mon2|mon3|monvirt}
- multi-tenant par vlan :
  - default
  - VLAN X
  - VLAN X Y

Processus général

A l'exécution de la commande `set advanced-configuration local-rules ...`, deux fichiers de règles s'ouvrent successivement à travers l'éditeur de texte Nano.

Le processus de modification des fichiers est le suivant :

- Nano ouvre automatiquement le premier fichier.
  Il permet de modifier les règles de la catégorie `Rules:`, c'est-à-dire :
  - les règles de détection
  - les règles de reconstruction
- Modifier le contenu de ce fichier

  Note:

  Une fois dans l'interface, un copié/collé des règles de détection peut être fait.
  Il n'y a pas de limitation dans le nombre de signatures pour les interfaces mais elles ne doivent pas avoir le même identifiant SID que les autres règles déjà présentes.

- Fermer (**CTRL** + **X**) après sauvegarde
- Nano ouvre automatiquement le deuxième fichier.
  Il permet de modifier les règles de la catégorie `threshold:`, c'est-à-dire :
  - les seuils ou limites définis par le mot clé "threshold"
  - les règles de suppression définies par le mot clé "suppress"

  Note:

  Il est possible d'ajouter d'autres types de règles afin de limiter ou supprimer certaines alertes.
  Il existe :
  - les **Suppress Rules** qui suppriment une alerte en fonction de l'adresse IP source ou destination,
  - mais aussi les **Threshold Rules** qui limitent le nombre d'alertes à afficher en fonction d'un ou plusieurs réseaux.

Exemple pour modifier les règles en mode single tenant

Important:

Les modifications faites en mode single tenant seront appliquées à toutes les interfaces de capture.

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration local-rules all
```

- Valider.
  L'éditeur de texte s'ouvre avec le fichier permettant de modifier les règles de la catégorie `Rules:`.
  Voir le paragraphe Processus général ci avant.

Exemple pour modifier les règles en mode multi tenant pour l'interface `mon0`

Important:

Les modifications faites en mode multi tenant pour l'interface `` `mon0` `` ne seront appliquées qu'à cette interface. Il est donc possible d'avoir des règles de détection et des seuils par interface de capture.

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration local-rules mon0
```

- Valider.
  L'éditeur de texte s'ouvre avec le fichier permettant de modifier les règles de la catégorie `Rules:`.
  Voir le paragraphe Processus général ci avant.

Exemple pour modifier les règles en mode multi tenant pour le vlan 10

Important:

Les modifications faites en mode multi tenant pour le vlan 10 ne seront appliquées qu'à ce vlan.

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration local-rules VLAN 10
```

- Valider.
  L'éditeur de texte s'ouvre avec le fichier permettant de modifier les règles de la catégorie `Rules:`.
  Voir le paragraphe Processus général ci avant.

Exemple pour modifier les règles en mode multi tenant pour le vlan par défaut

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration local-rules default
```

- Valider.

L'éditeur de texte s'ouvre avec le fichier permettant de modifier les règles de la catégorie `Rules:`.

Voir le paragraphe Processus général ci avant.

mtu (Maximum Transfert Unit)

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 Load Balancing et de filtrage XDP ne sont pas supportées lorsque la MTU > 3000.

Prérequis

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

---

Commande

`set advanced-configuration mtu {mon0|mon1|mon2|mon3|monvirt}`

Exemple pour modifier la valeur de la MTU de l'interface `mon1`

- 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
```

packet-filtering

Introduction

La commande `packet-filtering` du sous-groupe `set advanced-configuration` permet de spécifier des règles statiques de filtrage des flux capturés par les interfaces de capture.

Cela permet notamment d'exclure les flux :

- qui ne sont pas analysables
- qui pourraient saturer les ressources de l'appliance (CPUs...)

Ci-dessous les options de configuration :

- **création de règle de filtrage**
  Pour créer une règle de filtrage, il faut suivre les étapes suivantes :
  - définir le vlan natif
    La commande `set advanced-configuration packet-filtering interface mon1 change-native-vlan` permet de spécifier le numéro de VLAN non-tagué 802.1q ou 802.1ad (VLAN imbriqués) aux trames qui n'ont pas de VLAN.
  - définir l'interface de capture `interface`
  - définir le vlan `vlan`
    La syntaxe pour le support de 802.1AD (Q-in-Q) est X:Y:
    * X est "l'outer TAG". "L'outer TAG" peut être tagué tel 0x88A8,802.1AD
    * Y est "l'inner TAG". "L'inner TAG" peut être tagué tel 0x9100, 0x9200, 0x8100 (Cisco)
  - spécifier le flux (`prefix`, `port-range`, `protocol`, `ciphered-protocols`)
  - le mot clé `confirm` permet de forcer la confirmation de la commande
- **supprimer une règle de filtrage**
  Pour supprimer une règle de filtrage, il faut suivre les étapes suivantes :
  - définir l'id de la règle en utilisant la commande : `show advanced-config packet-filtering`.
  - supprimer une seule règle avec l'ID de la règle : `set advanced-configuration packet-filtering delete ID`.
  - supprimer un groupe de règles avec la syntaxe `begin-end` : `set advanced-configuration packet-filtering delete ID_BEGIN-ID_END`.

Note:

La fonctionnalité de packet-filtering n'est pas supportée lorsque la MTU $>$ 3000.

Prérequis

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

---

Commande

Pour définir le vlan natif :
`set advanced-configuration packet-filtering interface {mon0|mon1|mon2|mon3} change-native-vlan VLAN_ID confirm`

`set advanced-configuration packet-filtering interface {mon0|mon1|mon2|mon3} drop vlan VLAN_ID prefix PREFIX_NETWORK port-range {BEGIN:END} confirm`

Pour ajouter à l'interface de capture `monx` une règle de filtrage des flux chiffrés du vlan ID :
`set advanced-configuration packet-filtering interface {mon0|mon1|mon2|mon3} drop ciphered-protocols vlan VLAN_ID confirm`

Pour supprimer une seule règle avec l'ID de la règle :
`set advanced-configuration packet-filtering delete ID`

Pour supprimer un groupe de règles avec la syntaxe : `set advanced-configuration packet-filtering delete {BEGIN-END}`

Exemple pour ajouter à l'interface de capture `mon1` une règle de filtrage des flux chiffrés du vlan 110

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration packet-filtering interface mon1 drop ciphered-
↪protocols vlan 110 confirm
```

- Valider.
  Le système affiche le résultat.

```
Adding rules:
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto ESP
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto AH
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto L2TP
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto GRE
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 22:22
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 443:443
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 465:465
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 500:500
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 993:993
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 995:995
 - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 4500:4500
```

Exemple pour définir le vlan natif

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration packet-filtering interface mon1 change-native-vlan␣
↪10
```

- Valider.
  Le système affiche le résultat.

```
The following rules will be created:
   - iface mon1 native vlan 10

Do you want to continue? [y/N]
```

- Entrer **y**

Exemple pour supprimer une règle de filtrage

- 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
```

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration packet-filtering delete 4 confirm
```

- Valider.

```
Deleting the following rules:
  - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto TCP range 465:465
```

- Entrer la commande suivante.

```
(gcap-cli) set advanced-configuration packet-filtering delete 6-9 confirm
```

- Valider.

```
Deleting the following rules:
  - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 500:500
  - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto UDP range 4500:4500
  - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto GRE
  - iface mon1 drop vlan 110 prefix 0.0.0.0/0 proto ESP
```

rescan-interfaces

Introduction

La commande `rescan-interfaces` du sous-groupe `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.

Prérequis

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

---

Commande

```
set advanced-configuration rescan-interfaces [no-reboot]
```

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 Introduction

Les 'eve-log' du GCap sont les journaux d'analyse du service de détection d'anomalies réseau. Ces événements sont horodatés et ordonnés en fonction du moment de la capture.

La liste des services surveillés est la suivante :

Service	Fonction
local-alerts	• Les alertes sont envoyées d'office au GCenter pour traitement de celles-ci avec des outils appropriés. • Le service local-alerts permet de stocker localement les alertes. • Ce service, monopolisant des ressources (CPU + espace disque), ne doit être activé que pour effectuer du diagnostic avancé en collaboration avec le service support de Gatewatcher. • Ne pas oublier d'arrêter ce service après usage. Ce service n'est pas démarré nativement.
eve-generation	• Génération des eve logs et stockage des événements sur le GCap. • L'arrêt de ce service arrête la capture de fichiers
eve-compress	• Compression des eve logs sur le GCap permet la compression des eve logs mais utilise puissance des CPU • En cas de connectivité intermittente, ou tout autre problème prévenant l'envoi des journaux au GCenter, il est conseillé d'activer cette fonction afin de maximiser la durée de conservation des journaux sur le GCap.
eve-upload	• Envoi des eve logs vers le GCenter. • L'arrêt de ce service n'a pas d'influence sur l'extraction des fichiers
file-extraction	• Extraction des fichiers par la sonde GCap
file-upload	• Envoi des fichiers extraits vers le GCenter
filter-fileinfo	• Filtrage des fileinfos (`event_type: fileinfo` dans elasticsearch) • Supprime ou conserve automatiquement les évènements de type `fileinfo` à propos de fichiers qui ne seraient pas conservées pour analyse par le GCenter • Le but est de réduire le rapport signal/bruit et limiter la quantité de journaux envoyés au GCenter • Ce sont des réplicas (`fileinfo.stored: false` dans elasticsearch)

Chacun de ces services peut être :

- démarré : se référer à la commande *start*
- arrêté : se référer à la commande *stop*

Pour visualiser l'état courant des services, se référer à la commande *status*.

6.2.3.2 show

Introduction

La commande `show retention-periods` du sous-groupe `services` permet d'afficher les périodes de conservation des fichiers du GCap.

A la fin de cette période de conservation, les fichiers sont supprimés du GCap.

Ces valeurs sont configurables depuis la section `GCap variables` sur le GCenter.

Liste des périodes de conservation :

- `unsent` files : les fichiers reconstruits non transmis au GCenter.

  La valeur par défaut est 1296000s soit 15j.

- `sent` files : les fichiers reconstruits transmis au GCenter.

  La valeur par défaut est 86400s soit 24h.

- `eve` files : les eve logs.

  La valeur par défaut est 1296000s soit 15j.

Prérequis

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

Commande

`services show retention-periods`

Exemple pour afficher la valeur des périodes de conservation

- Entrer la commande suivante.

```
(gcap-cli) services show retention-periods
```

- valider.
  Le système affiche les valeurs courantes.

```
Current file retention periods:
 - unsent files: 1296000
 - sent files: 86400
 - eve files: 1296000
```

Note:

Les périodes sont exprimées en secondes.

6.2.3.3 start

Introduction

Pour visualiser la liste des services ainsi que leur interêt et les eventuelles restrictions, se référer à la partie *Introduction*.

La commande `start` du sous-groupe `services` permet de démarrer un service du GCap mais cela dépend de l'état courant de ces services (voir commande *services status*).

Par défaut, les services suivants sont démarrés :

- le service eve-generation

- le service eve-upload
- le service file-extraction
- le service file-upload

Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances :** le service doit être arrêté pour pouvoir le démarrer

---

Commande

Suivant le complément à la commande `services start`, il est possible d'effectuer différentes opérations.

```
services start {eve-generation|eve-upload|file-extraction|file-upload|filter-fileinfo|local-alerts|eve-c
}
```

Pour démarrer...	compléter la commande `services start` avec...	prerequis
la génération des eve logs	`eve-generation`	Aucun
l'envoi des eve logs au GCenter	`eve-upload`	Il faut activer eve-generation
l'extraction des fichiers par le GCap	`file-extraction`	Aucun
l'envoi des fichiers extraits vers le GCenter	`file-upload`	Il faut activer file-extraction
le filtrage des fileinfos	`filter-fileinfo`	**Il faut activer :** 1. eve-generation 2. eve-upload 3. file-extraction 4. file-upload
l'affichage des alertes	`local-alerts`	Aucun
la compression des eve logs sur le GCap	`eve-compress`	Il faut activer eve-generation

---

Exemple pour démarrer le filtrage des fileinfos (accessible à partir du compte gviewadm)

- Entrer la commande suivante.

```
(gcap-cli) services start filter-fileinfo
```

- Valider.
  Le système indique que le service **filter-fileinfo** démarre.

```
Starting services filter-fileinfo
```

Exemple pour démarrer la la compression des eve logs sur le GCap

- Entrer la commande suivante.

```
(gcap-cli) services start eve-compress
```

- Valider.
  Le système indique que le service **eve-compress** démarre.

```
Starting services eve-compress
```

Exemple pour démarrer les alertes locales

- Entrer la commande suivante.

```
(gcap-cli) services start local-alerts
```

- Valider.
  Le système indique que le service **local-alerts** démarre.

```
Starting services local-alerts
```

Exemple pour démarrer la génération des eve logs au GCenter

- Entrer la commande suivante.

```
(gcap-cli) services start eve-generation
```

- Valider.
  Le système indique que le service eve-generation démarre.

```
Starting service eve-generation
```

Exemple pour démarrer l'envoi des eve logs au GCenter

- Si le service eve-generation n'est pas actif alors le démarrer, voir la procédure ci-avant.
- Si le service eve-generation est actif alors continuer la procédure..
  - Entrer la commande suivante.

```
(gcap-cli) services start eve-upload
```

  - Valider.

Le système indique que le service eve-upload démarre.

```
```
Starting service eve-upload
```
```

Exemple pour démarrer l'extraction des fichiers

- Entrer la commande suivante.

```
(gcap-cli) services start file-extraction
```

- Valider.
  Le système indique que le service file-extraction démarre.

```
Starting service file-extraction
```

Exemple pour démarrer l'envoi des fichiers extraits au GCenter

- Si le service file-extraction n'est pas actif alors le démarrer, voir la procédure ci-avant.
- Si le service file-extraction est actif alors continuer la procédure..
  - Entrer la commande suivante.

    ```
    (gcap-cli) services start file-upload
    ```

  - Valider.
    Le système indique que le service `file-upload` démarre.

    ```
    Starting service file-upload
    ```

6.2.3.4 status

Introduction

Pour visualiser la liste des services, se référer à la partie *Introduction*.

La commande `status` du sous-groupe `services` permet d'afficher l'état de chacun des services du GCap :

- état `up` : état actif
- état `down` : état inactif .

Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances :** aucune

Commande

```
services status {eve-generation|eve-compress|eve-upload|file-extraction|file-upload|filter-fileinfo|loca
```

Exemple pour afficher l'état de tous les services

- Entrer la commande suivante.

```
(gcap-cli) services status
```

- Valider.

```
up - Service eve-generation
up - Service eve-upload
up - Service file-extraction
up - Service file-upload
down - Service filter-fileinfo
down - Service local-alerts
down - Service eve-compress
```

Exemple pour afficher l'état du service file-upload

- Entrer la commande suivante.

```
(gcap-cli) services status file-upload
```

- Valider.

```
up - Service file-upload
```

6.2.3.5 stop

Introduction

Pour visualiser la liste des services, se référer à la partie *Introduction*.

La commande `stop` du sous-groupe `services` permet d'arrêter un service du GCap mais cela dépend de l'état courant de ces services (voir commande *services status*).

Par défaut, les services suivants sont démarrés :

- le service eve-generation
- le service eve-upload
- le service file-extraction
- le service file-upload

Prérequis

- **Utilisateurs :** setup, gviewadm
- **Dépendances :** le service doit être démarré pour pouvoir l'arrêter

---

Commande

```
services stop {eve-generation|eve-upload|file-extraction|file-upload|filter-fileinfo|local-alerts|eve-co
}
```

Suivant le complément à la commande `services stop`, il est possible d'effectuer différentes opérations.

Pour arrêter...	compléter la commande services stop avec...	prerequis
• la génération des eve logs • conséquence: arrêt de la capture de fichiers	`eve-generation`	Aucun
• l'envoi des eve logs au GCenter • aucune influence sur la génération des logs	`eve-upload`	Aucun
• l'extraction des fichiers par le GCap	`file-extraction`	Aucun
• l'envoi des fichiers extraits vers le GCenter • aucune influence sur l'extraction des fichiers	`file-upload`	Aucun
• le filtrage des fileinfos	`filter-fileinfo`	Aucun
• l'affichage des alertes	`local-alerts`	Aucun
• la compression des eve logs sur le GCap	`eve-compress`	Aucun

Exemple pour arrêter la génération des eve logs au GCenter

- Entrer la commande suivante.

```
(gcap-cli) services stop eve-generation
```

- Valider. Le système indique que le service **eve-generation** s'arrête.

```
Stopping service eve-generation
```

Exemple pour arrêter l'envoi des eve logs au GCenter

- Entrer la commande suivante.

```
(gcap-cli) services stop eve-upload
```

- Valider. Le système indique que le service **eve-upload** s'arrête.

```
Stopping service eve-upload
```

Exemple pour arrêter l'extraction des fichiers

- Entrer la commande suivante.

```
(gcap-cli) services stop file-extraction
```

- Valider.
  Le système indique que le service **file-extraction** s'arrête.

```
Stopping service file-extraction
```

Exemple pour arrêter l'envoi des fichiers extraits au GCenter

- Entrer la commande suivante.

```
(gcap-cli) services stop file-upload
```

- Valider.
  Le système indique que le service **file-upload** s'arrête.

```
Stopping service file-upload
```

Exemple pour arrêter le filtrage des fileinfos

- Entrer la commande suivante.

```
(gcap-cli) services stop filter-fileinfo
```

- Valider.
  Le système indique que le service **filter-fileinfo** s'arrête.

```
Stopping services filter-fileinfo
```

Exemple pour arrêter les alertes locales

- Entrer la commande suivante.

```
(gcap-cli) services stop local-alerts
```

- Valider.
  Le système indique que le service **local-alerts** s'arrête.

```
Stopping services local-alerts
```

Exemple pour arrêter la compression des eve logs sur le GCap

- Entrer la commande suivante.

```
(gcap-cli) services stop eve-compress
```

- Valider.
  Le système indique que le service **eve-compress** s'arrête.

```
Stopping services eve-compress
```

6.2.4 system

6.2.4.1 reload-drivers

Introduction

La commande `reload-drivers` du sous-groupe `system` permet de recharger les pilotes des cartes réseaux et de remettre à zéro les statistiques des cartes réseau.

Prérequis

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

---

Commande

`reload-drivers`

Exemple pour redémarrer un GCap

- Entrer la commande suivante.

```
(gcap-cli) system reload-drivers
```

- Valider.
  Le système affiche le résultat.

```
Reloading NIC drivers... Please wait a few seconds...
```

  Puis après quelques secondes, l'invite de commandes s'affiche pour indiquer que les pilotes ont été rechargés.

```
(gcap-cli system)
```

6.2.4.2 restart

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.

Prérequis

- **Utilisateur :** setup
- **Dépendances :** Aucune

Commande

`system restart`

Exemple pour redémarrer un GCap

- Entrer la commande suivante.

```
(gcap-cli) system restart
```

- Valider.

La connexion en SSH va être interrompue.

6.2.4.3 shutdown

Introduction

La commande `shutdown` du sous-groupe `system` permet d'éteindre le GCap.

Important:

Le Gcap une fois éteint devrat être remis sous tension via l'accès distant par l'iDRAC.

Prérequis

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

---

Commande

`system shutdown`

Exemple pour éteindre un GCap

- Entrer la commande suivante.

```
(gcap-cli) system shutdown
```

- Valider.

6.2.4.4 unlock

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.

Prérequis

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

Commande

```
system unlock {setup|gview|gviewadm}
```

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
```

6.2.5 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 chacunes des commandes. Il faut désactiver le moteur de capture pour les rendre à nouveau accessibles.
Lorsque 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. L'appairage est effectué au-travers de l'interface `gcp0` (non-configurable).

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
```

6.2.6.4 Exemple pour appairer un GCap version 2.5.3.105 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 replay

6.2.7.1 Introduction

Un fichier avec l'extension pcap est un fichier dans lequel le trafic réseau brut a été capturé .

La commande `replay` permet :

- 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.

6.2.7.2 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

---

6.2.7.3 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)

6.2.7.4 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:

name.pcap
```

6.2.7.5 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
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 5 secondes environ les compteurs :

- débit en Bps
- débit en Mbps

- débit en pps (paquets)

puis les compteurs finaux.

6.2.8 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.

6.2.8.1 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

---

Prérequis pour ?

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

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`

Utilisation de ? de suffixation

Pour lister les fichiers de configurations accessibles via la CLI :

- utiliser la commande `show config-files` suivi de `?`

```
(gcap-cli) show config-files ?
```

- valider

Le système affiche les informations suivantes:

```
(gcap-clInspect configurations
=====================

Available commands:
        - Sigflow-config: View detection engine configuration
        - rules-scirius: View user-defined detection ruleset
        - rules-files: View file-related detection ruleset
        - threshold: View threshold configuration files
```

6.2.8.2 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`

Prérequis pour `help`

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

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`

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
   - gui: Start a graphical session (deprecated)
   - exit: Exit configuration tool
```

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 :

```
Available commands:
    - start: Start the Monitoring Engine
    - status: View current Monitoring Engine status
```

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
```

6.2.9 colour

6.2.9.1 Prérequis

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

La commande `colour` permet d'activer ou désactiver les couleurs dans les sorties de l'instance en cours de gcap-cli.

6.2.9.2 Commande

```
colour {disable|enable}
```

6.2.9.3 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>
```

6.2.9.4 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>
```

6.2.10 gui (deprecated)

6.2.10.1 Introduction

La commande `gui` de `gcap-cli` permet de lancer la GUI de configuration du GCap.

La GUI est dépréciée.

6.2.10.2 Prérequis

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

6.2.10.3 Commande

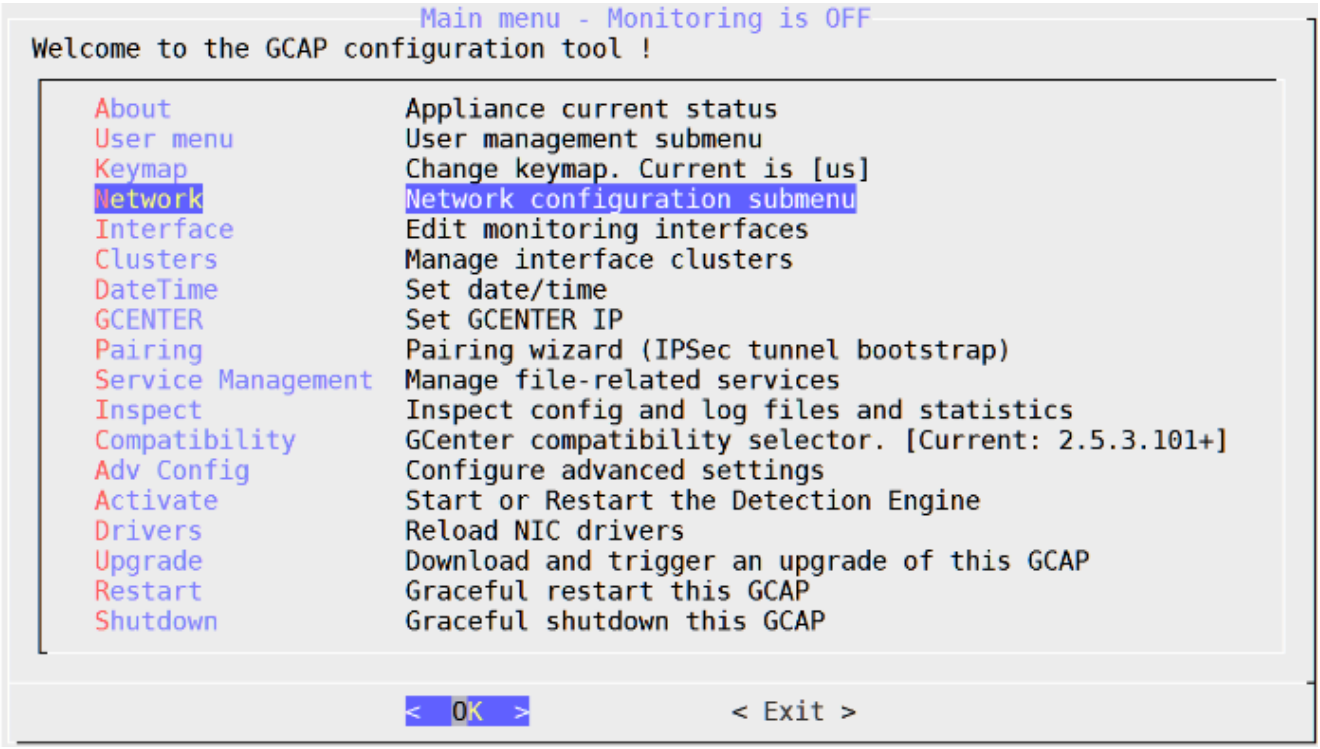
gui

6.2.10.4 Exemple pour lancer la GUI de configuration du GCap

- Entrer la commande suivante.

```
(gcap-cli) gui
```

- Valider.
  Le menu graphique est affiché :



6.2.11 exit

6.2.11.1 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`.

6.2.11.2 Prérequis

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

6.2.11.3 Commande

```
exit
```

6.2.11.4 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)
```

6.2.11.5 Exemple pour sortir de la CLI

- Entrer la commande suivante.

```
(gcap-cli) exit
```

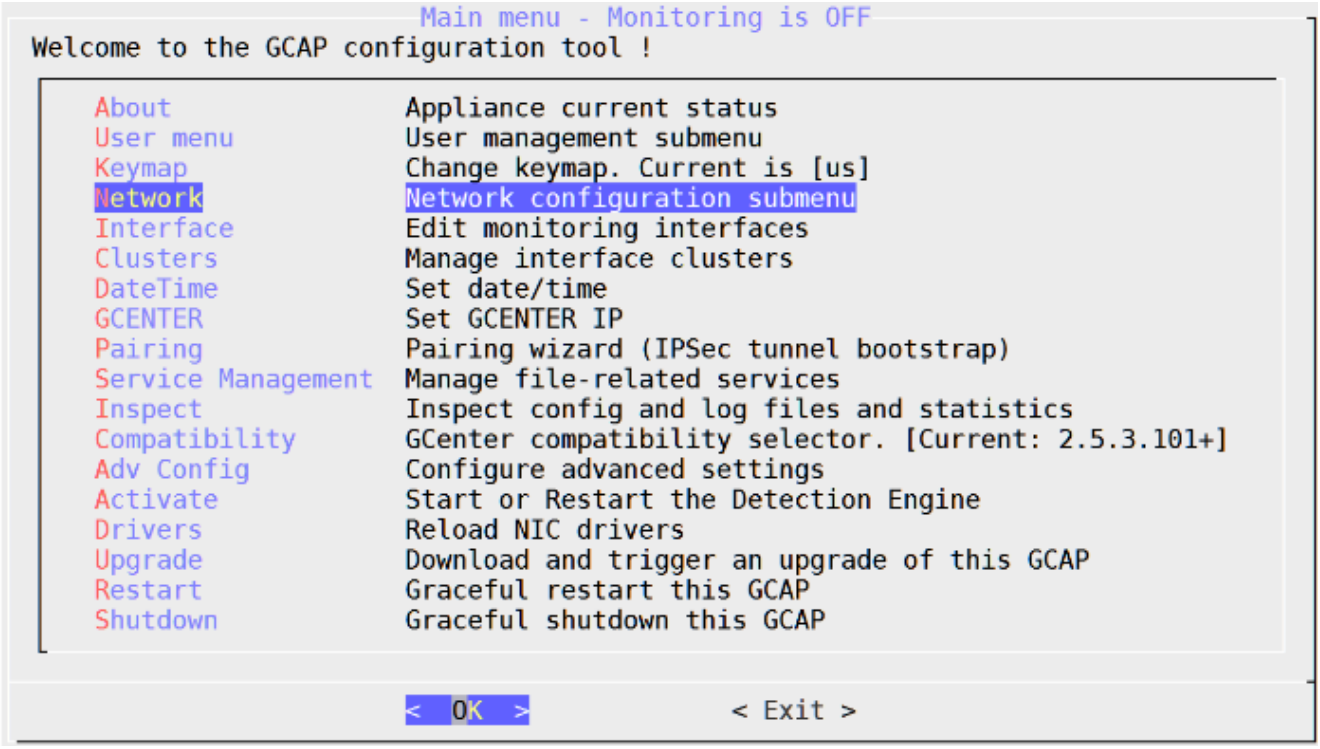
- Valider.

6.3 gui (déprécié)

Important:

Le menu GUI du GCap est déprécié. Celui-ci sera retiré en version 2.5.3.106.

Ci-dessous un aperçu du menu en GUI :



Pour accéder au menu vous pouvez le faire avec la commande *GUI* depuis la CLI.

Déconseillé : le menu GUI peut être défini par *défaut*.

Chapter 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 donne la correspondance entre les compteurs version 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	leader_status	boolean	Etat du nœud (0 : slave ou non configuré / 1 : leader)
high_availability.health_status	health_status	boolean	Capacité du nœud à devenir leader (0: non ou non configuré / 1: OK)
high_availability.last_state_change	last_state_change	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

Chapter 8

Annexes

8.1 Fichiers d'événements

Il est possible de consulter les fichiers d'événements des différents services du GCap via la commande *show logs*.

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 Evénements 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 Evénements 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 Evénements 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.

Chapter 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 GCap`

Index