User manual
GCAP v2.5.5

Manual version: v1

Translated from original manual version: v1

Creation date: January 2026

Update date: January 2026

Table of contents

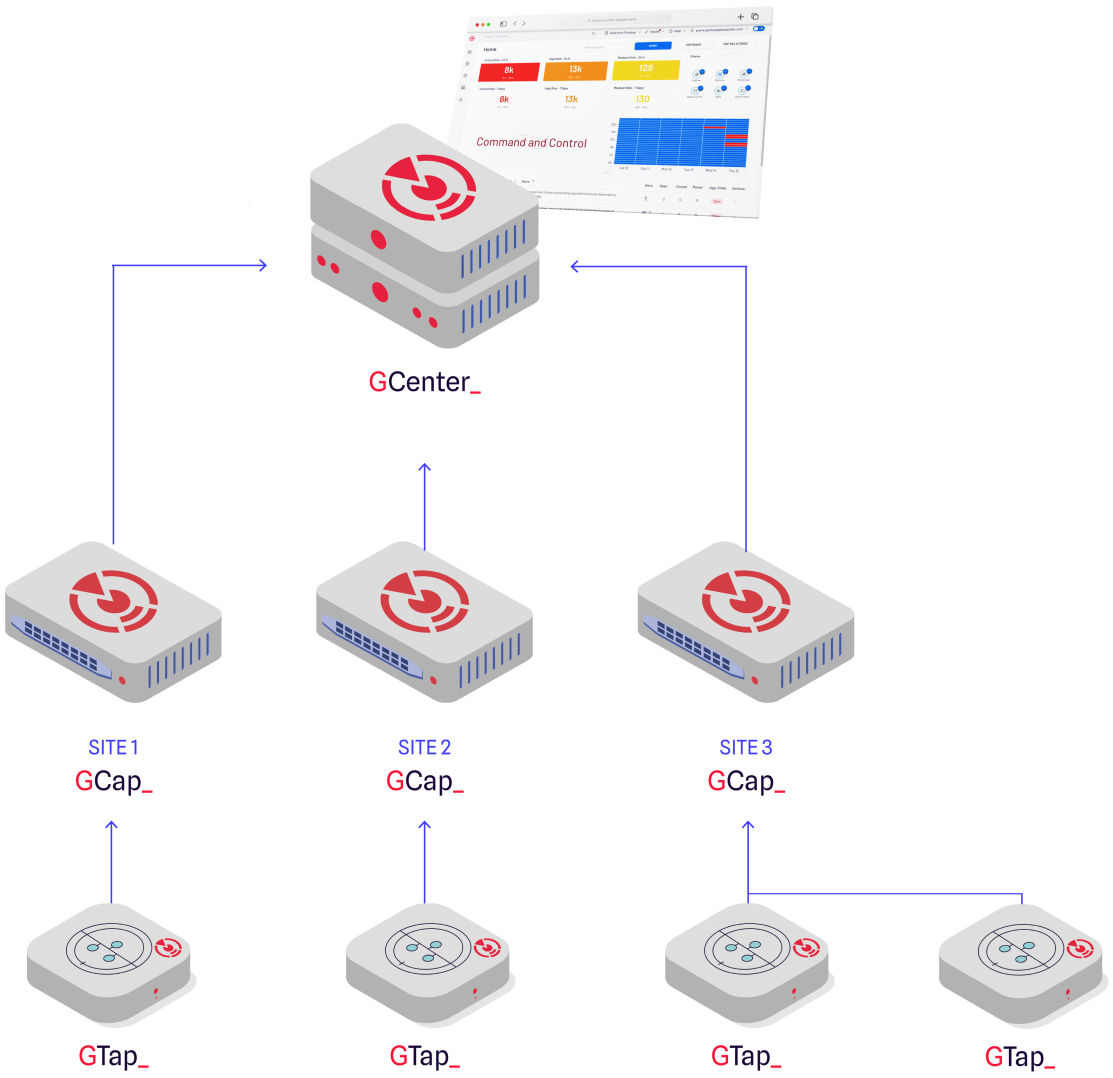
Chapter 1

Description

1.1 Introduction

The AIONIQ solution is Gatewatcher's Intrusion Detection System (IDS).
It includes:

- One or more TAPs
- One or more GCaps
- A GCenter
- reflex



1.2 TAP

A Test Access Point (TAP) is a passive device enabling the monitoring of a computer network by duplicating the flows in transit and redirecting them to an analysis and detection probe (the GCap).

It is possible to connect several TAPs to a GCap, as the latter has several capture interfaces.

1.3 Presentation of the GCap

GCap is a probe-type component.
It enables:

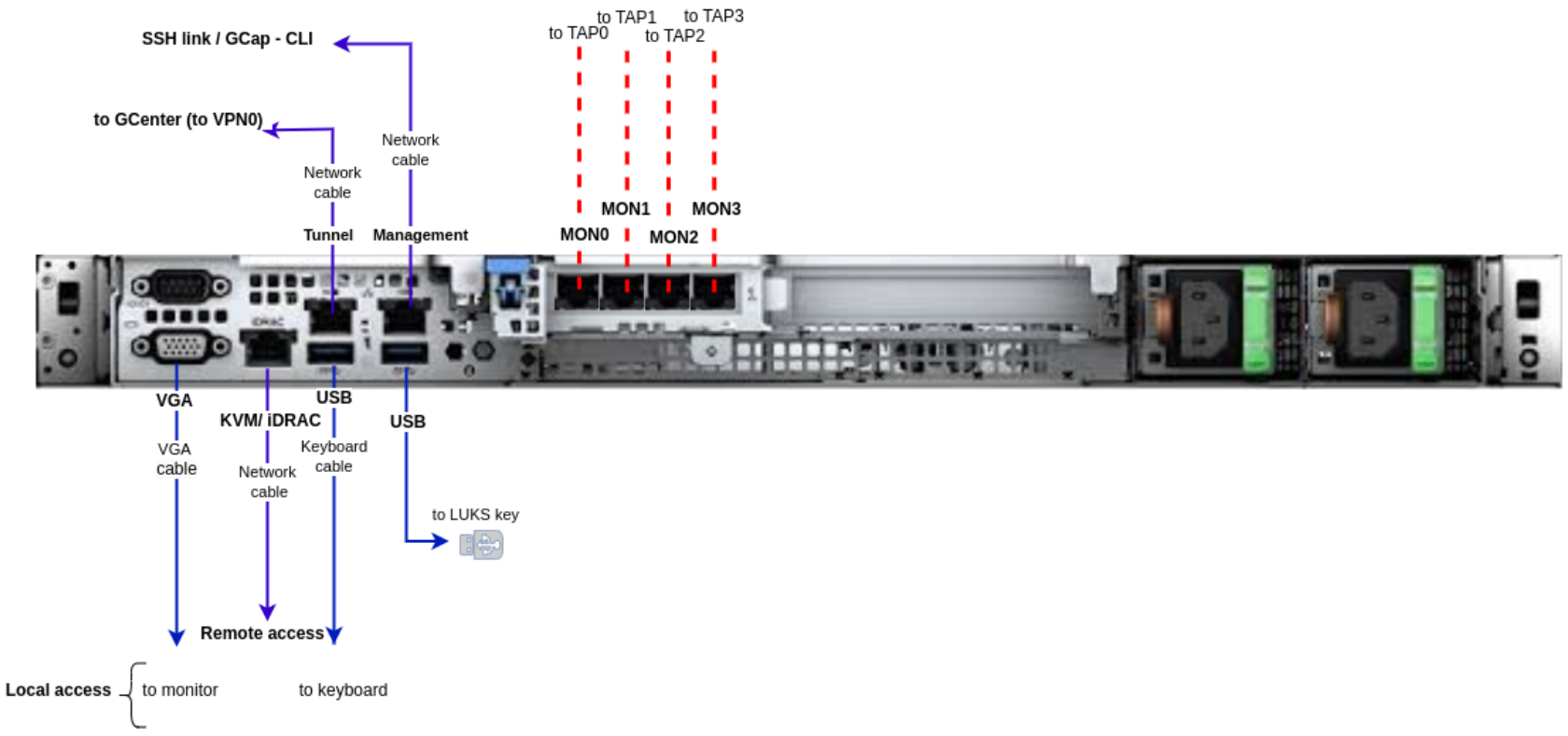
- Capturing and analyzing network traffic from TAPs
- Reconstructing the files present in the analyzed flow (according to type and size parameters)
- Carrying out an initial analysis
- Generating alerts an/or metadata type events
- Transmitting files / codes / events to the GCenter

1.3.1 Different server models

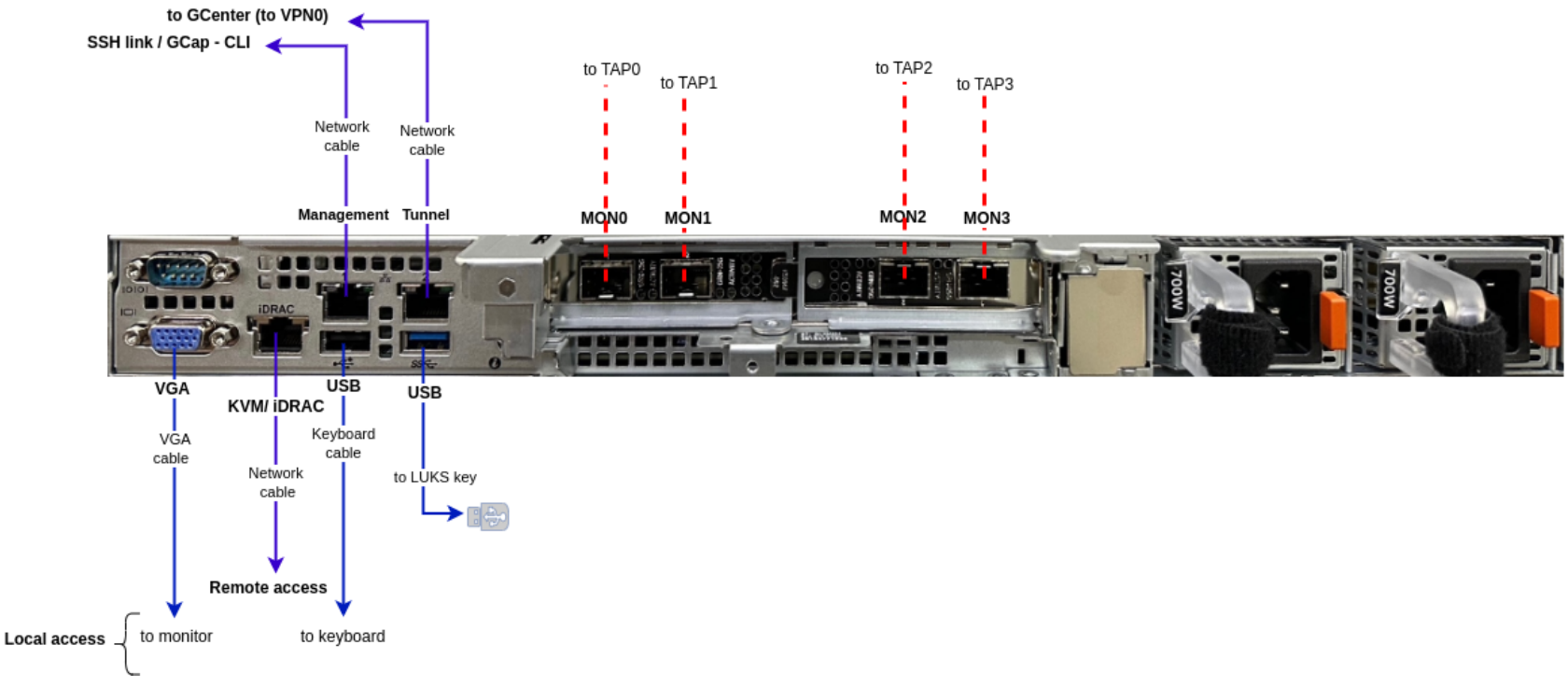
For more information, please refer to the section *Mechanical characteristics of GCap*.

1.3.2 Description of the GCap inputs / outputs

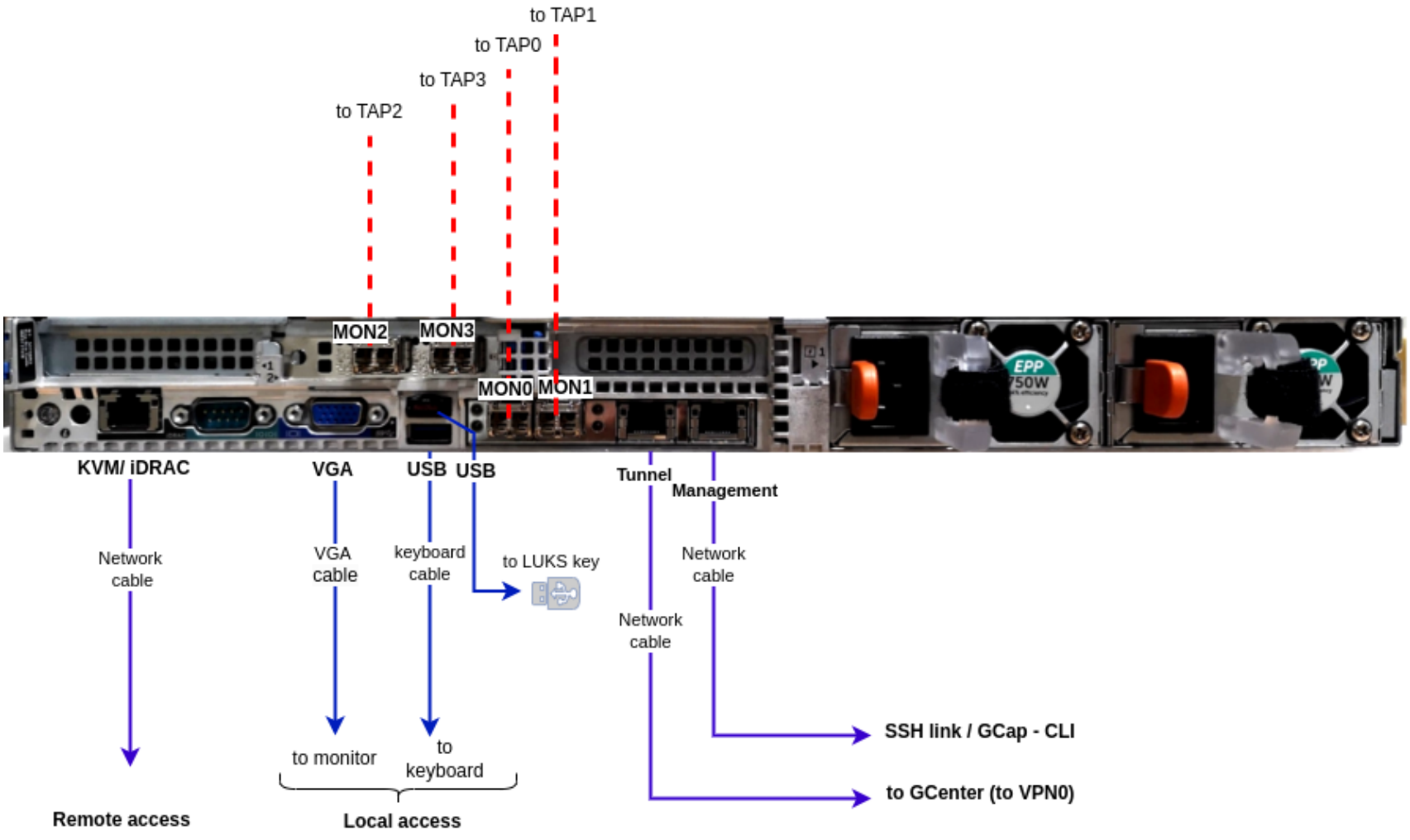
1.3.2.1 Example of a DELL R340 GCenter server



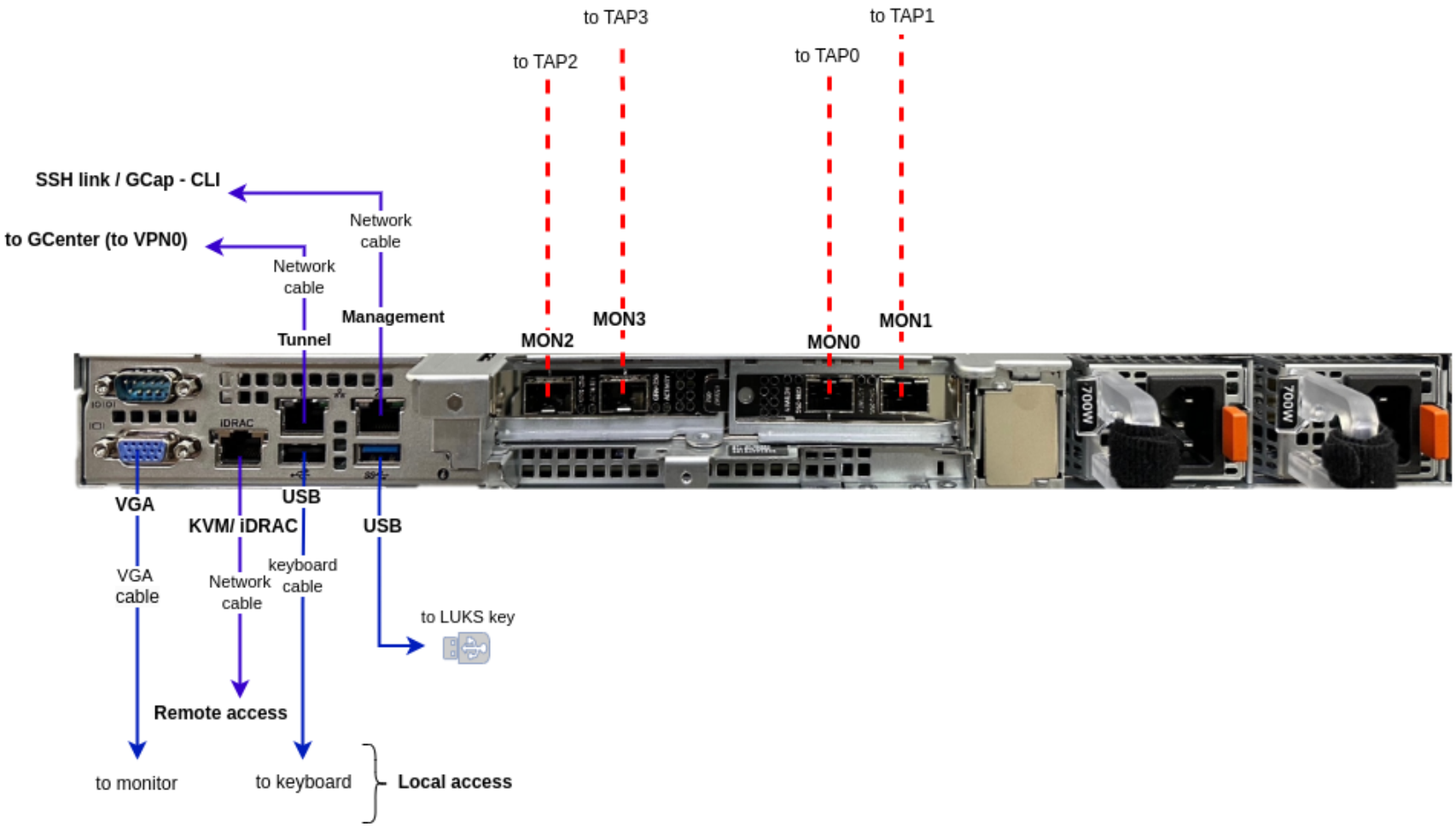
1.3.2.2 Example of a DELL R360 GCenter server



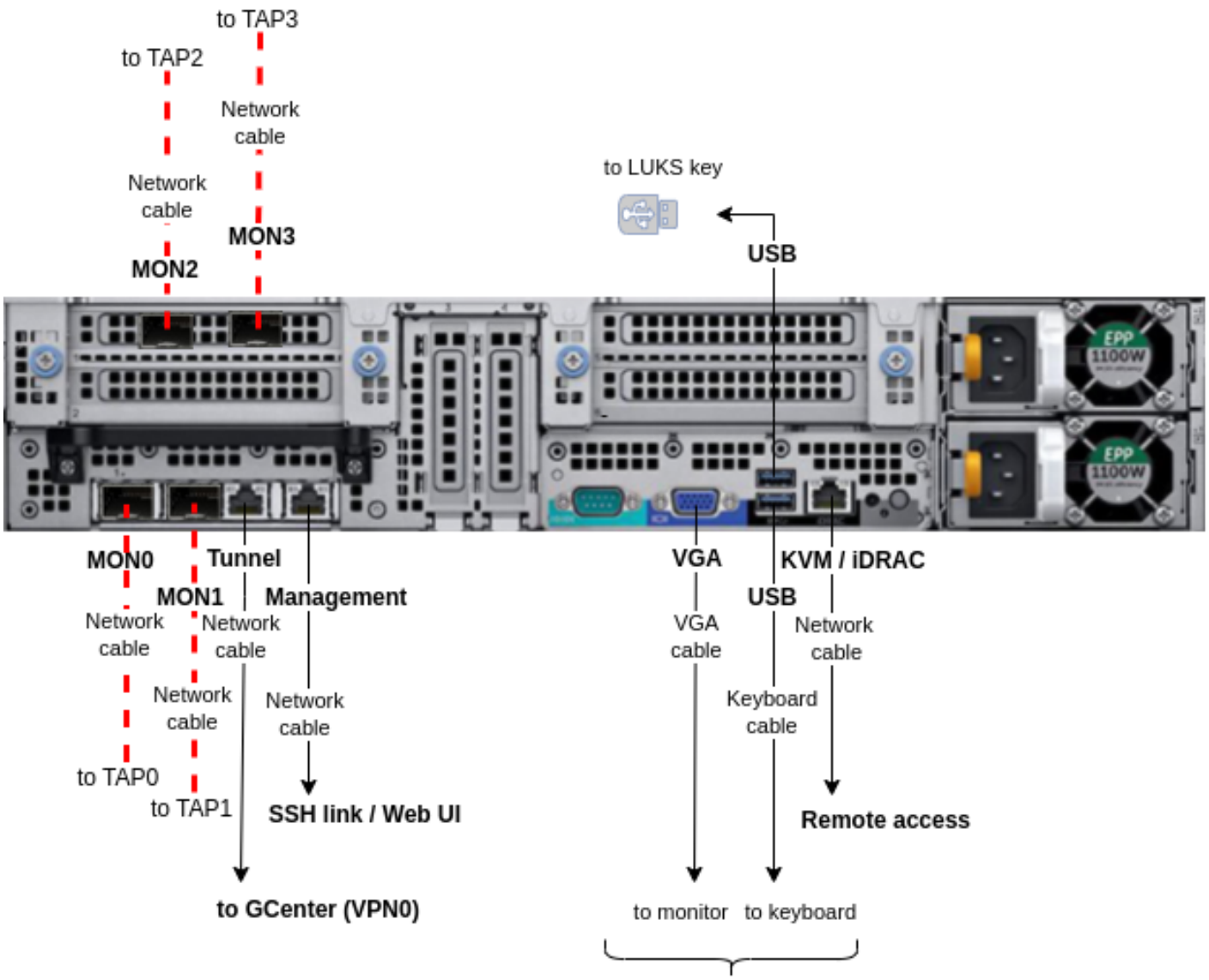
1.3.2.3 Example of a DELL R640 GCenter server



1.3.2.4 Example of a DELL R660 GCenter server



1.3.2.5 Example of a DELL R840 GCenter server



1.3.2.6 Description

Inputs/outputs	Use cases
USB and VGA connectors	Directly access a keyboard and a monitor This connection mode is deprecated in favor of KVM/IDRAC/XCC and should only be used as a last resort
USB connector	Connection of the USB key allowing the decryption of disks (standard Linux Unified Key Setup)
RJ-45 connector `KVM/IDRAC`	Access to the server's management and configuration interface
RJ-45 connector	In the double interface configuration: used for the **Management** and **tunnel** roles In the single interface configuration: used for the **Management** role only
RJ-45 connector	In the double interface configuration: used for the Dedicated VPN interface for the **tunnel** role In the single interface configuration: not used
Two power supplies	Redundant server power supplies
Connectors SFP, SFP+, RJ-45 (`MON1`, `MON0`, `MON3`, `MON2`)	capture interfaces receive the flows from the TAPs

The GCap detection probe features:

- Two RJ-45 connectors `management` and `tunnel`
- RJ-45 and/or fiber connectors for monitoring `mon0` (`capture` role)

- two power supplies.

1.3.2.7 Use of USB and VGA connectors

Connecting a keyboard and monitor enables direct access to the server's console interface.

Important:

This mode is deprecated.
it should only be used during initial installation and for advanced diagnosis.

1.3.2.8 Access to the server's management and configuration interface

Access to this management interface is via HTTPS:

- On a Dell server, this connector is called **iDRAC**. It is noted on the **KVM/IDRAC GCap** diagram
- On a Lenovo server, this connector is called **TSM**. This connector can be identified by a wrench symbol on the bottom of it

---

1.3.2.9 Management and tunnel (`gcp0`) network interfaces

Important:

Concept of role is introduced in the release 2.5.4.0.

These interfaces perform the following roles:

- Role 1: called `tunnel`, is the secure communication between the probe and GCenter through an IPSEC tunnel in order to:
  - Escalate information such as files, alerts,metadata, and so on, derived from analyzing the monitored flows
  - Report information on the health of the probe to the GCenter
  - Control the probe - analysis rules, signatures, etc
- Role 2 : called `management`, is the remote administration through the SSH protocol with access :
  - To the probe's command line interface (CLI)
  - To the graphical setup/configuration menu (deprecated)

In **single-interface configuration**, these roles are supported by one of these interfaces.
In **dual-interface configuration**, these roles is allocated over to interface (preferably, the two embedded gigabit ethernet network interfaces).

1.3.2.9.1 Configuration of the `management` and `tunnel` network interfaces

For more information on these interfaces and their configuration, refer to *Management overview of 'Management' and 'Tunnel' interfaces*.

1.3.2.10 Capture interfaces

These interfaces receive:

- The flows from the TAPs on the indicated interfaces (`mon0` and `monx`) called `capture`
- The flow from previously recorded files (pcap files) on a dedicated `monvirt` interface

Note:

The number of capture interfaces varies depending on the specifications of each model.

1.3.2.10.1 Activating the capture `monx` interfaces

For more information, please refer to the paragraph *Overview of managing the capture interfaces*.

1.3.2.10.2 Aggregation of capture interfaces `monx`

For more information, please refer to *Capture and capture interfaces 'monx' between TAP and GCap: aggregation possibility*.

1.3.3 Electrical connection

The probe has two power supplies, each of which has the necessary power to operate the equipment.
It is strongly recommended that each power supply should be connected to a separate power supply.

1.3.4 USB connector and LUKS key

During installation, the contents of the disks (excluding /boot) are encrypted using the LUKS standard.
During this process, a unique encryption key is created and placed on the USB stick connected to the probe.
It is strongly recommended to make a copy of this key because, in the event of failure, the data on the disks will no longer be accessible.
Once the system is up and running, the USB stick should be removed and placed in a secure place (e.g. in a safe).

1.4 Presentation of the GCenter

The GCenter is the component of the system working in conjunction with the GCap detection probe.
Its main functions include:

- Management of the GCap probe including managing the analysis rules, signatures, health status supervision, and so on
- In-depth analysis of the files retrieved by the probe
- Administering the system
- Displaying the results of the various analyzes in different dashboards
- Long-term data storage
- Exporting data to third-party solutions such as the Security Information and Entente Management system (SIEM)

For more information, please refer to the GCenter documentation.

1.5 Presentation of Reflex

Reflex is the solution for automation of responses to cybersecurity events offered by Gatewatcher.

It interacts with all the security equipment of the information systems before executing automated processes to process these events.

These automated processes are called playbooks in Reflex.

A playbook is a collection of pre-defined and organized sequences of actions or processes to be used to implement and / or optimize security incident response operations.

Security solutions that Reflex connects to can be, for example, Security Information and Event Management (SIEM), network security tools, data from Threat Intelligence solutions, etc.

For each third-party application on the market to which Reflex must connect, a package is assigned.

For example, the Gatewatcher-NDR package allows:

- To connect Reflex to the GCenter application of the import / export Gatewatcher solution
- To retrieve event data, to enrich it or collect alerts, and to respond to them

---

1.6 Interconnection between devices

1.6.1 Reminder of the GCap connections

Depending on the timing and configuration chosen and looking from behind from left to right, the GCap is connected via:

- A network socket for connecting a KVM / iDRAC
- A USB and VGA connector for a keyboard and monitor
- The capture interfaces `mon0`, `mon1`, `mon2`, `monx` for the connection of the TAPs
- These interfaces perform the following roles

  Depending on the chosen configuration single or dual interface, it is possible to use these network interfaces for connecting to the GCenter.
- The connectors for the GCap power supplies

For more information on the connection description, please refer to *Description of the GCap inputs / outputs*.

Note:

Remember to connect the LUKS decryption key to the USB port.

1.6.2 Capture and capture interfaces `monx` between TAP and GCap: aggregation possibility

The GCap probe must read in a single flow; the network flow that has been captured in both directions:

- An up-link
- A down-link

To do this, the flows from each of the links must be aggregated into a single flow.
There are 2 solutions for this:

- Either the flows were captured and aggregated by an aggregator TAP
- Or the flows were captured but not aggregated by a non-aggregating TAP

1.6.2.1 Capture mode with an aggregator TAP

In this situation, the GCap retrieves the flow aggregated by the TAP on a single *monx* capture interface.
This solution is preferable because it requires the least amount of GCap resources for the same flow.

1.6.2.2 Capture mode with a non-aggregating TAP: GCap mode with aggregation (”cluster”)

This functionality is necessary if the Test Access Port (TAP) present in the architecture does not provide the interface aggregation functionality.
A **qualified TAP** is at least a passive or non-intelligent (simple) TAP.
This means that it does not require its own power supply and does not actively interact with other components.
Most passive TAPs do not have an embedded configuration.

1.6.2.2.1 Connection between TAP and GCap

Unlike network interfaces where traffic is both TX (emission) and RX (reception), capture interfaces are unidirectional. Therefore, they can only receive flow, hence the following connection.
Each physical fiber link handles two links:

- An up-link, i.e. a TX link
- A down-link, i.e. an RX link

The TAP (without aggregation) is connected to the network via 2 physical links called commutator X and commutate Y.
The commutate X link connects the switch and the X input TAP and enables duplicating half the network flow.
The TX link is:

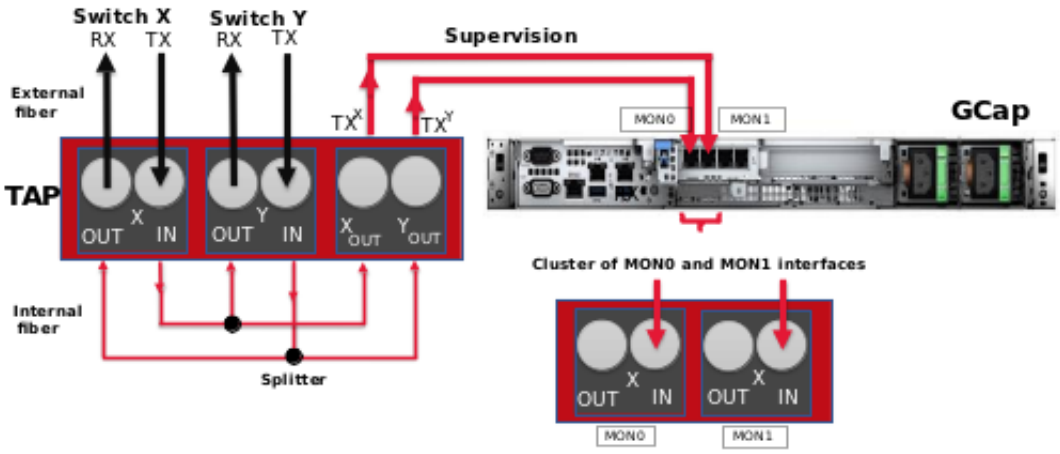
- Connected to **IN** of the **X** connector
- The flow of the TX link is copied to **OUT** of the **Y** connector: this is connected to the RX link of the *commutate Y* physical link
- The flow from the TX link is also copied to the **Xout** link which is sent to the input port of the GCap (**IN** link of the *mon1* port)

The *commutator Y* link connects the switch and the **Y** input TAP and enables duplicating the other half the network flow.
The TX link is:

- Connected to **IN** of the **Y** connector
- The flow of the TX link is copied to **OUT** of the **X** connector: this is connected to the RX link of the *commutator X* physical link
- The flow from the TX link is also copied to the **Yout** link which is sent to the input port of the GCap (**IN** link of the *mon0* port)

1.6.2.2.2 Aggregation of interfaces (or clustering)

By defining an aggregation of two interfaces, the GCap aggregates these two flows into a single one, thus enabling a correct flow interpretation.
If the GCap has this functionality, this is not neutral in terms of resources allocated to this processing, hence the configuration with an aggregator TAP should be preferred.



1.6.2.3 Using and configuring interface aggregation

To implement interface aggregation, refer to *Procedure to manage capture interface aggregation*.

1.6.3 Transferring rules between GCenter and GCap: single-tenant vs. multi-tenant

For more information, please refer to *Capture interfaces: single-tenant vs. multi-tenant*.

Chapter 2

Operation

2.1 GCap

2.1.1 GCap functions

The functions of the GCap include:

- Connecting to the TAP and retrieving duplicate packets from the network flow seen by the TAP
- Rebuilding the files from the corresponding packets using a detection engine, also referred to as Sigflow
- Intrusion detection (vulnerabilities...) is performed by several detection engines:
  - The first is the Sigflow engine. It is located in the GCap
  - The others are located in GCenter.

    It recovers the network flow sent by the GCap to perform this analysis:
    - Shellcode et Malicious Powershell Detect
    - Malcore and Retroanalyzer
    - Beacon Detect
    - Dga Detect
    - Ransomware Detect
    - Retrohunt (optional)
    - Active CTI (optional)
- The transmission of files, codes and events to GCenter
- Communication between GCap and GCenter including receiving configuration files, rulesets, and the like

2.1.2 The Sigflow engine

Sigflow performs:

- The recovery of network flows entering the Gcap via the `monx` capture interfaces
- Intrusion detection, statistical analysis of network flows to reduce the number of false positives and identify possible protocol malformations, SQL injection attempts, and so on.
- The creation of alerts or log files

The use of rules enables the Sigflow engine to define what to monitor, hence to raise alerts.
For more information, please refer to the table *Manage the detection engine*.

2.1.2.1 Filtering of the captured flow

Certain parts of the captured flow cannot be detected or reconstructed: for example, encrypted flows.
If nothing is done, the system will monopolize resources to achieve a result known in advance.
To avoid this, it is possible to create rules to filter the flow to be captured.

Note:

The visualization of the rules is done locally (*show advanced-configuration packet-filtering*)
Packet filtering must be configured in `GCaps profiles` menu of GCenter.

2.1.3 Counters of GCap activity

In order to view this information, the *show eve-stats* command enables the following counters to be viewed:

- counter `Alerts` - Number of Sigflow alerts found
- counters `Files` - Files extracted by Sigflow
- Counters `Codebreaker samples` - Files analyzed by Codebreaker
- Counters `Protocols` - List of protocols seen by Sigflow
- Counters `Detection Engine Stats` - Sigflow statistics (*monitoring-engine*)

For more information, please refer to the table *Monitoring the GCAP*.

2.2 GCap configuration

2.2.1 Configuring a GCap and its Sigflow engine

To analyze the captured flow, the following steps must be taken:

- Synchronize the date and time of the GCap on GCenter : see *Overview of date and time management*
- Managing Tunnel and Management interfaces : see *Management overview of 'Management' and 'Tunnel' interfaces*
- Manage the capture interfaces: see *Overview of managing the capture interfaces*
- Manage single-tenant vs. multi-tenant configuration of `monx` interfaces : see *Capture interfaces: single-tenant vs. multi-tenant*
- Managing the aggregation of capture interfaces : see *Capture interfaces: aggregation*
- Pairing the GCap with GCenter

  A GCap must be paired with a GCenter.

  Data exchange only starts when the VPN tunnel (IPsec) is established between the two devices.
- Activation of the Sigflow monitor engine (by default it is deactivated).

2.2.2 Overview of date and time management

When connecting for the first time, the date and time of the GCap and GCenter must be identical in order to set up the IPsec tunnel.

2.2.2.1 CLI commands

Displaying the current date and time is accomplished with the *show datetime* command in the CLI.
Modifying the current date and time is accomplished with the *set datetime* command in the CLI.

2.2.2.2 Use case procedures

For implementation, refer to *Procedure to change the date and time of the GCap*.
Thereafter, the GCap date and time are synchronized with the GCenter date and time after the IPsec tunnel is established.

2.2.3 Management overview of `Management` and `Tunnel` interfaces

Important:

Concept of role is introduced in the release 2.5.4.0.

These interfaces perform the following roles:

- Role 1: called `tunnel`, is the secure communication between the probe and GCenter through an IPSEC tunnel in order to:
  - Escalate information such as files, alerts,metadata, and so on, derived from analyzing the monitored flows
  - Report information on the health of the probe to the GCenter
  - Control the probe - analysis rules, signatures, etc
- Role 2 : called `management`, is the remote administration through the SSH protocol with access :
  - To the probe's command line interface (CLI)
  - To the graphical set / configuration menu

2.2.3.1 CLI commands

Managing the network interfaces is done using the CLI commands listed in the *Summary of orders by theme and level* table.

2.2.3.2 View or configure

To view or configure the network interfaces, refer to *Procedure to manage the network parameters of 'Tunnel' and 'Management' interfaces*.

2.2.3.2.1 Single interface configuration.

In **single-interface configuration**, role 1 and role 2 is assigned to one network interface.
To toggle from dual-interface to single-interface configuration, refer to *Procedure to switch the single-interface configuration*.

2.2.3.2.2 Dual-interface configuration

The `Management` and `Tunnel` roles are allocated over two network interfaces.

Important:

This dual-interface configuration is mandatory if using the **MPL mode** on the GCenter.

The aim of this situation is to ensure that the management flow and the interconnection flow between the GCap and GCenter are separated from each other.

Note:

Since version 2.5.4.0, you can assign role to the network of your choice.
We recommend the use of embedded gigabit interfaces.

To toggle from single-interface to dual-interface configuration, refer to *Procedure to switch to the configuration dual-interface*.

2.2.4 Overview of managing the capture interfaces

Important:

Concept of role and label is introduced in the release 2.5.4.0.

The monitoring interfaces on GCap perform the `capture` role and are, by default, four in number.
These interfaces receive the flows from the TAPs on the specified interfaces labeled:

- `mon0` for the first TAP
- `mon1` for the second TAP
- `mon2` for the third TAP
- `mon3` for the fourth TAP

For more information regarding the capture interfaces, refer to *Capture interfaces*.

Note:

The number of capture interfaces varies depending on the specifications of each model.

In some special cases, it is possible to use GCaps with eight interfaces instead of four.
In addition, there is also a virtual capture interface labeled `monvirt` enabling `.pcap` file replay directly on the GCap.
In order for the GCap to capture the flow, one or more interfaces must be activated.

2.2.4.1 CLI commands

Managing the capture interfaces is done using the CLI commands listed in the *Summary of orders by theme and level* table.

2.2.4.2 Use case procedures

To view or configure the capture interfaces, refer to *Procedure to manage the 'monx' capture interface settings*.

2.2.5 Capture interfaces: single-tenant vs. multi-tenant

2.2.5.1 GCap detection engine and rules

SIGFLOW is the name of the GCap detection engine configured:

- By a set of rules (RULESET) defined on the GCenter
- By locally defined rules, therefore not known to the GCenter

These rules must describe the characteristics of the attacks to be detected as well as being optimized to reduce false positives.
The ruleset is composed of signatures grouped by categories that were provided by sources.
This compilation is done by the administrator on the GCenter. Therefore, it can be configured differently depending on the number of GCap and their specifications.

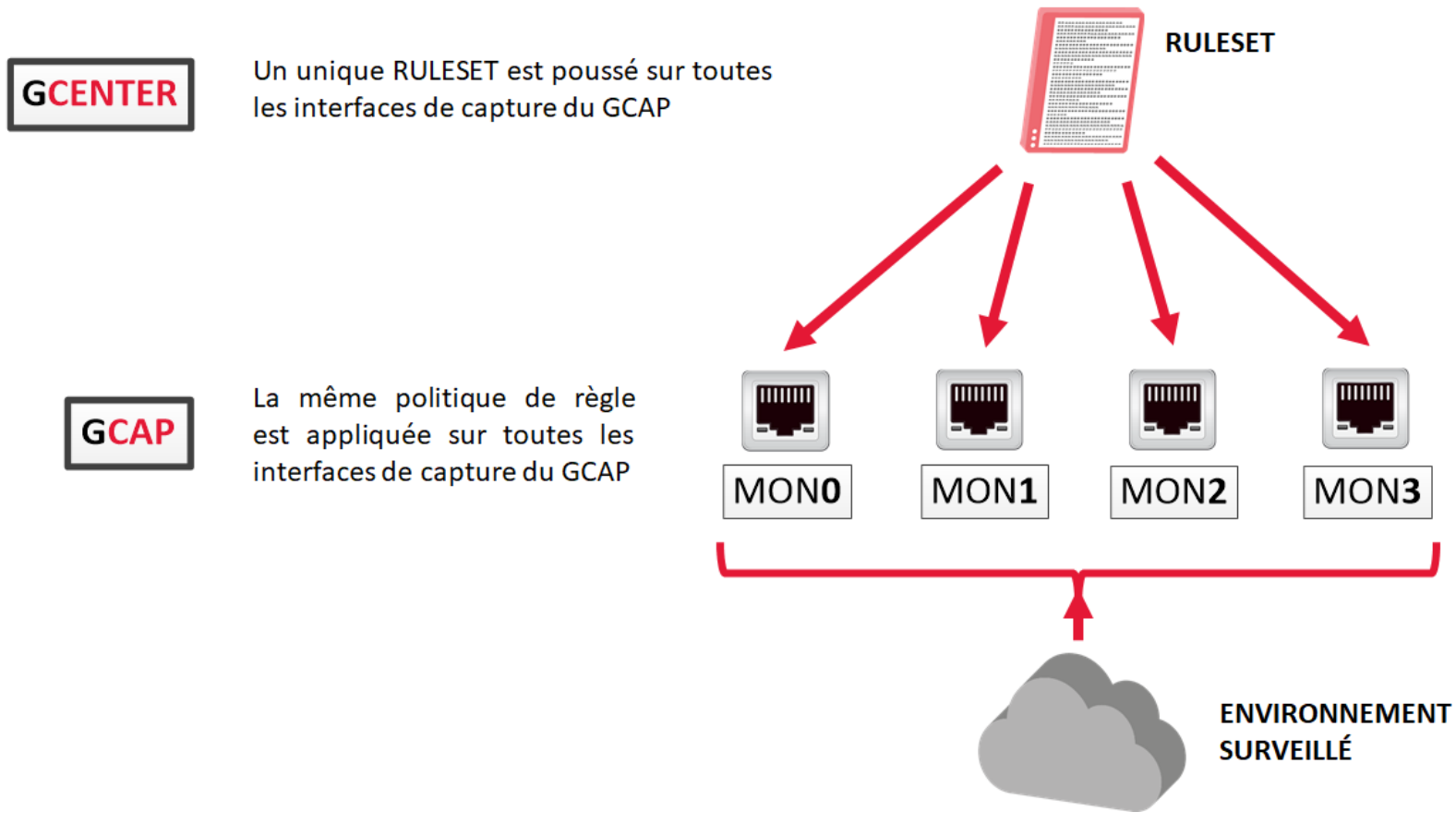
2.2.5.2 CLI commands

The ability to view and create local rules is handled differently depending on the configuration.
For more information on the rules, see the table Managing the detection engine in the section *Summary of orders by theme and level*.

2.2.5.3 Transferring the ruleset in single-tenant mode

2.2.5.3.1 Single-tenant principle

Once configured on GCenter, a single set of rules (RULESET) is sent to the GCap detection engine.
The GCap detection engine applies this ruleset to all capture interfaces: this is the single-tenant configuration.



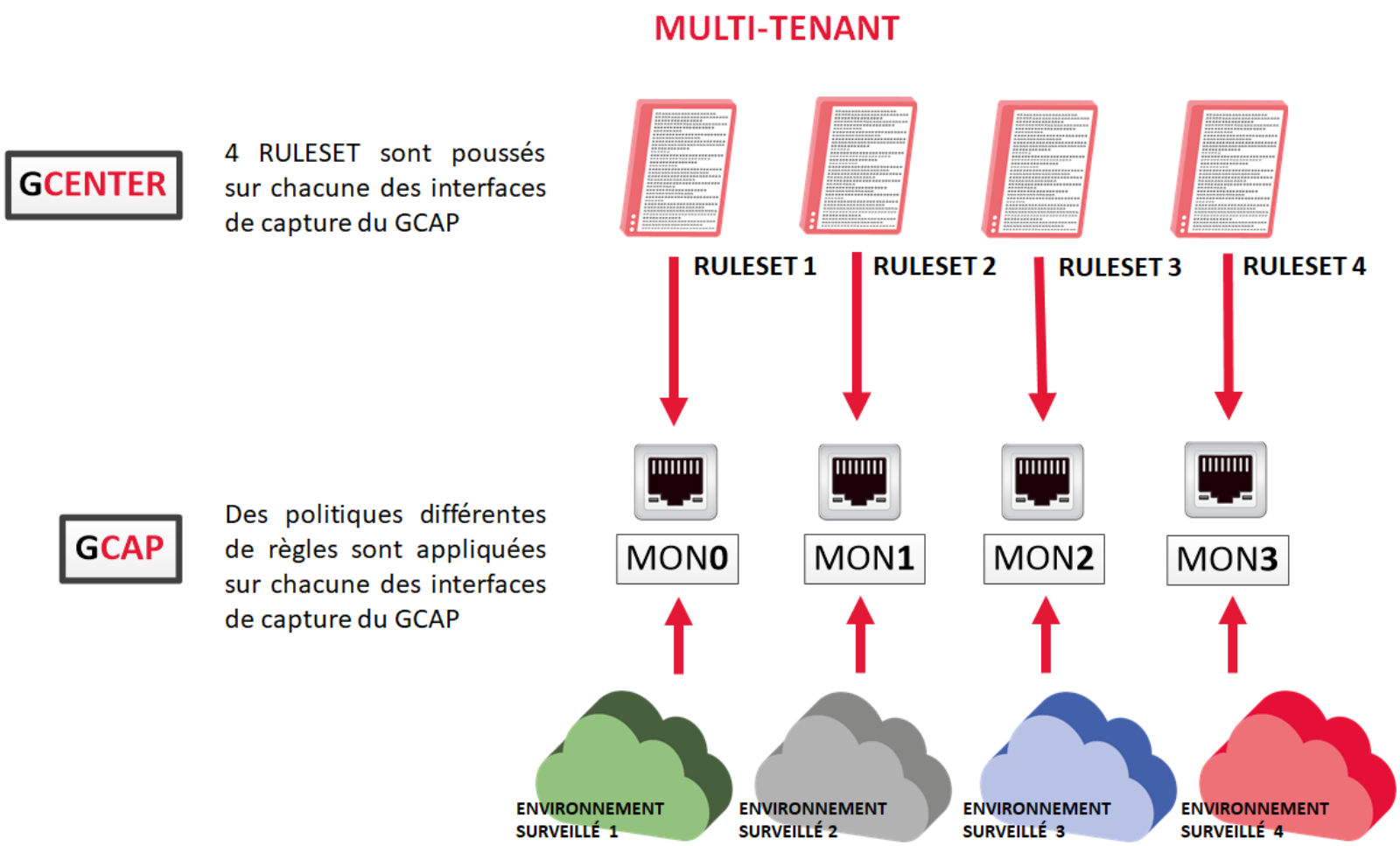
2.2.5.3.2 Configuring the single-tenant mode

In the GCenter web interface, in the `SIGFLOW - GCaps Profiles > Detection rulesets` part, the default option is single-tenant.

2.2.5.4 Transferring the SIGFLOW rule set in multi-tenant mode

2.2.5.4.1 Multi-tenant principle

Once configured on GCenter, it is possible to define a different set of SIGFLOW rules for each of the capture interfaces.
Then each of these rulesets will be applied to its capture interface: this is the **multi-tenant** configuration.



In contrast to single-tenant, multi-tenant will enable optimising resources and costs while simplifying the process of managing detection rules per environment.
The flexibility of the architecture enables efficient refinement of detection rules, easier isolation of threats, and customisation of capture.

2.2.5.4.2 Configuring the multi-tenant mode

In the GCenter web interface, in the `SIGFLOW - GCaps Profiles > Detection rulesets` part, the default option is single-tenant.
It is also possible to choose two other options:

- 'Multi-tenant by interface' or
- 'Multi-tenant by VLAN'

In the event one of these options is selected, it offers the possibility to assign different SIGFLOW rulesets for:

- Each of the GCap interfaces or
- For the various VLAN's...

... and thus have a different supervision on various networks.

It is strongly advisable to optimize the SIGFLOW ruleset in advance before choosing this configuration option.
The rules must be adapted to the monitored environment.
This version of GCap enables compatibility with GCenter.

2.2.6 Capture interfaces: aggregation

2.2.6.1 Aggregation principle (”cluster”)

For more information, please refer to the paragraph *Capture and capture interfaces ‘monx‘ between TAP and GCap: aggregation possibility*.

2.2.6.2 CLI commands

Displaying the current aggregation is achieved with the *show interfaces* command.
Configuring the aggregation is done with the *set interfaces* command.

2.2.6.3 Use case procedures

For the implementation, refer to *Procedure to manage capture interface aggregation*.

2.2.6.4 Configuring the aggregation

Aggregation creation is done via the GCap Command Prompt (CLI).

2.2.6.5 Impact on other functionalities

The functionality of aggregating capture interfaces on the GCap results in degrading the MTU (Maximum Transmission Unit): the maximum size of a packet that can be transmitted at one time without fragmentation.
The MTU uses the largest value of the interfaces making up the aggregation.

2.2.7 Sigflow detection engine

To analyze the captured flow, the following steps must be taken:

- Activate one or more capture interfaces on the GCap
- Pair the GCap and GCenter
- Activate of the Sigflow monitor engine, by default it is deactivated

---

2.2.7.1 Activate one or more capture interfaces on the GCap

2.2.7.1.1 CLI commands

Managing the capture interfaces is done using the CLI commands listed in the *Summary of orders by theme and level* table.

2.2.7.1.2 Use case procedures

To view or configure the capture interfaces, refer to the table *Manage the network*.

2.2.7.2 Aggregation of capture interfaces `monx`

For more information on this aggregation, please refer to *Capture and capture interfaces ‘monx‘ between TAP and GCap: aggregation possibility*.
For more information on how to configure this aggregation, refer to the paragraph *Capture interfaces: aggregation*.

2.2.7.3 Pairing the GCap with GCenter

Once the network configuration is done, it is necessary to pair the GCap with GCenter.
For more information on pairing, refer to *Procedure to pair a GCap with the GCenter*.

2.2.7.4 Activating the Sigflow monitor engine

By default the GCap monitor engine is disabled.

2.2.7.4.1 Checking the status of the Sigflow monitor engine (activating procedure)

The status of the engine can be checked with the `show status` command.

2.2.7.4.2 Starting the Sigflow analysis engine

It is essential to start the Sigflow monitor engine (detection engine).
The flow capture only takes place after this start.
To do this:

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the *monitoring-engine start* command
2. Validate

```
monitoring-engine start
```

The system displays the following message indicating that the engine started.

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

Once the monitor engine is activated, the configuration possibilities of the GCap probe change.
Some of them cannot be configured while the engine is running.

Note:

The `eve-stats` command in the `show` sub-group enables displaying the Sigflow (*monitoring-engine*) statistics.

2.2.7.4.3 Grace period

The grace period is the sum of:

- The maximum starting time
- The maximum stopping time

In order to be able to load the rules of the detection engine before starting the engine, the engine cannot start until a certain time called maximum start time or startup grace period (start-timeout).

- The current value is displayed using the *show monitoring-engine start-timeout* command.
- If the number of rules loaded by the monitor engine is large then the maximum start time must be changed via the *set monitoring-engine start-timeout* command.

Similarly, there is the maximum stopping time or grace period when the engine shuts down (stop-timeout).

- The current value is displayed using the *show monitoring-engine stop-timeout* command .
- The modification of the current value is done via the *set monitoring-engine stop-timeout* command.

2.2.7.5 Deactivating the Sigflow monitor engine

2.2.7.5.1 Checking the status of the Sigflow monitor engine (deactivating procedure)

The status of the engine can be checked with the `show status` command.

2.2.7.5.2 Stopping the Sigflow monitor engine

In the same way, stopping is carried out with the *monitoring-engine stop* command:

```
monitoring-engine stop
```

The system displays the following message indicating that the engine stopped.

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

2.2.7.6 Compatibility mode

The compatibility mode between the GCap and GCenter must be specified via the *set compatibility-mode* command.

2.2.7.7 MTU

The Maximum Transfer Unit (MTU) of each GCap capture interface can be adjusted via the CLI.
Indeed, the maximum packet size to be captured at one time on an interface is configurable.

2.2.7.7.1 Display of the current MTU value

The MTU value can be displayed using the *show interfaces* command:

```
(gcap-cli) show interfaces

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

The administrator can change the MTU's value in bytes of the GCap capture interfaces.
This setting must be between 1280 and 9000 bytes.

Note:

Note that XDP Filtering features is not supported if the MTU > 3000.

2.2.7.7.2 Changing the current MTU value

Regarding the modification of the MTU, this is done with the *set advanced-configuration mtu* command followed by the parameters:

- Name of the interface, for example enp4s0
- Value, for example 1300

Note:

To change the MTU of the *enp4s0* interface to 1300 :
- Enter the *set advanced-configuration mtu enp4s0 1300* command
- Validate

```
set advanced-configuration mtu enp4s0 1300
```

The system displays the parameter update information.

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

2.2.7.8 Rebuilding files

Rebuilding files occurs on the GCap thanks to its monitor engine (Sigflow).
These files are rebuilt under certain conditions that can be set from GCenter.
These conditions include the following:

- The size of the observed file
- The type of file observed, based either on the extension or on the filemagic

In addition, file reconstruction is only possible on certain protocols, the list of which varies according to the different GCap versions.
Here is the list of protocols supported by the GCap:

- HTTP
- SMTP
- SMB

Other protocols are available from GCenter.
For more information, please refer to the GCenter documentation.

Note:

Namely, the protocols on which it is possible to rebuild depends on the GCap and not the GCenter.
If the GCenter configuration instructs the GCap to rebuild a certain file type but the GCap is not capable of doing so, the rebuild will not take place.

Chapter 3

Characteristics

3.1 Mechanical characteristics of GCap

REFERENCE	DIMENSIONS (H x L x P)	RACKAGE	WEIGHT (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 Electrical characteristics of GCap

REFERENCE	LOCAL STOCKAGE	PORTS OF CAPTURE	EXTENSION OF CAPTURE PORTS	POWER SUPPLY
GCAP1010HWr2	256GB	4 x RJ45	N/A	2 x 750W
GCAP1020HWr2	256GB	4 x RJ45	N/A	2 x 750
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 Functional characteristics of GCap

3.3.1 Functional characteristics

REFERENCE	MAX THROUGHPUT	NUMBER OF FILES RECONSTRUCTED MAX PER S	NUMBER OF SESSIONS MAX	NUMBER OF MAX SESSIONS PER	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 List of protocols that can be selected for analysis

Protocol detection consists of two parts:

- **parsing**:
  - It enables SIGFLOW signature detection for a given protocol
  - If parsing is enabled for a protocol then the flow identified by a signature raises an alert
  - If parsing is disabled for a protocol then no alert is raised
- **logging**:
  - It enables generating metadata for a given protocol
  - If logging is enabled for a protocol then the observed flow will generate metadata
  - If logging is disabled for a protocol then no metadata is generated

For each interface, it is possible to:

- Enable parsing and logging
- Enable parsing only
- Disable parsing and logging

PROTOCOL	PARSING	LOGGING
DCE/RPC	supported	supported
DHCP	supported	supported
DNP3	supported	supported
DNS_udp	supported	supported
DNS_tcp	supported	supported
ENIP	supported	not supported
FTP	supported	supported
HTTP	supported	supported
HTTP2	supported	supported
IKEv2	supported	supported
IMAP	parsing detection only	not supported
Kerberos (KRB5)	supported	supported
MODBUS	supported	not supported
MQTT	supported	supported
NETFLOW	not supported	supported
NFS	supported	supported
NTP	supported	not supported
RDP	supported	supported
RFB	supported	supported
SIP	supported	supported
SMB	supported	supported
SMTP	supported	supported
SNMP	supported	supported
SHH	supported	supported
TLS	supported	supported

These options depend on the GCenter version, thus on the selected compatibility.
For more information, please refer to the GCenter documentation.

3.3.3 List of selectable protocols for file reconstruction

PROTOCOL	SUPPORTED
FTP	supported
HTTP	supported
HTTP2	supported
NFS	supported
SMB	supported
SMTP	supported

These options depend on the GCenter version, thus on the selected compatibility.
For more information, please refer to the GCenter documentation.

Chapter 4

The accounts

4.1 List of accounts

Remote or local access to the administration interface is protected by a login password.
Three generic accounts are defined with different rights levels:

Account...	intended for a...
gview	operator
gviewadm	manager
setup	system administrator

4.2 Related principles

4.2.1 Authentication mode

A user can be authenticated in two different ways :

- Username/password
- SSH key

Important:

Simultaneously connecting several accounts is not possible.

4.2.2 Password management

The current account manages its own password and potentially other accounts as well.
Details are provided in the table below:

User	can change the password setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

The *show passwords* command enables displaying the list of users managed by the current level.
The *set passwords* command enables changing the password managed by the current level.

4.2.3 Password management policy

The passwords entered must comply with the password management policy.
The default policy is as follows:

Criteria	Default value
At least x different characters are required for a password to be considered different	2
Minimum password length	12 characters
At least one lower case letter	yes
At least one lower case letter	yes
Presence of at least one capital letter	yes
Presence of at least one digit (0 to 9)	yes
Presence of at least one symbol (i.e. neither a number nor a letter)	yes

This policy is:

- Viewable via the *show password-policy* command
- Modifiable via the *set password-policy* command

4.2.4 SSH key

Authenticating SSH connections to administer GCap can be done via an SSH key.
All SSH keys authorized for an account and the list of different types of encryption are defined via the *set ssh-keys* command.
This mode is to be preferred to the user name/password pair.
Indeed, it enables defining a key per employee, thus ensuring traceability of connections and accountability of actions.

4.2.5 Rights associated with each account

The rights assigned to each account are listed in the presentation of each account.

4.3 gview profile

This account corresponds to an operator profile, member of a detection service in charge of operating the service.
The details of the accessible functions are given in the section *Use cases of the gview profile*.

4.4 gviewadm profile

This account represents an administrator profile, a member of the Detection Service with privileged rights enabling them to ensure the correct operation of the Detection Service devices.
The details of the accessible functions are given in the section *Use cases of the gviewadm profile*.

4.5 setup profile

This account represents an administrator profile, a member of the Detection Service with privileged rights enabling them to ensure the correct operation of the Detection Service devices.
The details of the accessible functions are given in the section *Use cases of the setup profile*.

Chapter 5

Use cases of the gview profile

5.1 Profile of the gview account

This account corresponds to an operator profile, member of a detection service in charge of operating the service.

Note:

Commands in the **gview** account are also found in the other **gviewadm** and **setup** accounts.

5.2 Password of the gview account

To log in to the **gview** account, the default password is: default

Note:

It is necessary to change the password the first time you log in. It should be kept in a safe place, for example, with the **GCap** encryption keys.

For more information on password management, see *Password management*.
For more information on the password policy, see *Password management policy*.

5.3 List of potential actions of the gview account

From the **gview** account, it will be possible:

- Accessing the GCap and GCenter

To perform the following task	Choose the following procedure
remote connection to GCap via an SSH tunnel	1 - *Procedure to remote connection to GCap via an SSH tunnel*
Connection to the GCenter via a web browser	1 - *Procedure to connect to the GCenter via a web browser*

- Configure the GCap

To perform the following task	Carry out the following procedures in succession
Display the current keyboard language	1 - Display: use the *show keymap* command
Modify the keyboard language.	1 - Display: use the *show keymap* command 2 - Modify: use the *set keymap* command
Enable or disable colors for the current CLI session	1 - Use the *color* command

- Manage the current account

To perform the following task	Carry out the following procedures in succession
Display the list of users	1 - Display the list: use the *show passwords* command
Modify his password	1 - Display the list: use the *show passwords* command 2 - Change passwords: use the *set passwords* command
Modify his SSH key	1 - Use the *set ssh-keys* command
Display the password policy	2 - Use the *show password-policy* command

- Manage the server

To perform the following task	Carry out the following procedures in succession
Returning to the root (gcap cli) if the prompt is elsewhere in the tree structure	1 - Use the *exit* command
Display help on the commands	1 - Use the *help* command

- Monitoring the GCAP

To perform the following task	Carry out the following procedures in succession
Display the current status of the GCap	1 - Use the *show status* command
Display the statistics of the Sigflow detection engine	1 - Use the *show eve-stats* command

Chapter 6

Use cases of the gviewadm profile

6.1 Profile of the gviewadm account

This account represents an administrator profile, a member of the Detection Service with privileged rights enabling them to ensure the correct operation of the Detection Service devices.

Note:

Commands present in the **gviewadm** account are also found in the **setup** account.

6.2 Password for the gviewadm account

To log in to the **gviewadm** account, the default password is: default

Note:

It is necessary to change the password the first time you log in. It should be kept in a safe place, for example, with the **GCap** encryption keys.

For more information on password management, see *Password management*.
For more information on the password policy, see *Password management policy*.

6.3 List of potential actions of the gviewadm account

From the **gviewadm** account, it will be possible:

- Accessing the GCap and GCenter

To perform the following task	Choose the following procedure
Remote connection to GCap via an SSH tunnel	1 - *Procedure to remote connection to GCap via an SSH tunnel*
Connect to the GCenter via a web browser	1 - *Procedure to connect to the GCenter via a web browser*

- Configure the GCap

To perform the following task	Carry out the following procedures in succession
Display the current keyboard language	1 - Display: use the *show keymap* command
Modify the keyboard language.	1 - Display: use the *show keymap* command 2 - Modify: use the *set keymap* command
Enable or disable colors for the current CLI session	1 - Use the *color* command

- Modify the passwords for gviewadm and gview

To perform the following task	Carry out the following procedures in succession
Display the list of users	1 - Display the list: use the *show passwords* command
Modify the passwords for gviewadm and gview	1 - Display the list: use the *show passwords* command 2 - Change passwords: use the *set passwords* command
Modify the authentication SSH keys for gviewadm and gview	1 - Use the *set ssh-keys* command
Display the password policy	2 - Use the *show password-policy* command

- manage the detection engine

To perform the following task	Carry out the following procedures in succession
Start the detection engine	1 - Use the *monitoring-engine start* command
Stop the Sigflow monitor engine	1 - Use the *monitoring-engine stop* command
Display the detection engine status	1 - Use the *monitoring-engine status* command
Replay a pcap file of traffic generation	1 - Use the *replay* command

- Manage the server

To perform the following task	Carry out the following procedures in succession
Returning to the root (gcap cli) if the prompt is elsewhere in the tree structure	1 - Use the *exit* command
Display help on the commands	1 - Use the *help* command

- Monitoring the GCAP

To perform the following task	Carry out the following procedures in succession
Display the current status of the GCap	1 - Use the *show status* command
Display the statistics of the Sigflow detection engine	1 - Use the *show eve-stats* command
Display GCap statistics and health information	1 - Use the *show health* command

Chapter 7

Use cases of the setup profile

7.1 Profile of the setup account

This account represents an administrator profile, a member of the Detection Service with privileged rights enabling them to ensure the correct operation of the Detection Service devices.

7.2 Password of the setup account

To log in to the **setup** account, the default password is: default

Note:

It is necessary to change the password the first time you log in. It should be kept in a safe place, for example, with the **GCap** encryption keys.

For more information on password management, see *Password management*.
For more information on the password policy, see *Password management policy*.

7.3 List of potential actions of the setup account

From the **setup** account, it will be possible:

- Accessing the GCap and GCenter

To perform the following task	Choose the following procedure
Connect to the GCap by a direct connection	1 - *Procedure to connect directly to the GCap via keyboard and screen*
Remote connection to iDRAC via HTTP	1 - *Procedure to connect the iDRAC in HTTP (DELL server)*
Remote SSH connection in serial port forwarding mode	1 - *Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
Connect to the GCenter via a web browser	1 - *Procedure to connect to the GCenter via a web browser*
Remote connection to GCap via an SSH tunnel	1 - *Procedure to remote connection to GCap via an SSH tunnel*

- Configure the GCap

To perform the following task	Carry out the following procedures in succession
Install a GCAP	1 - *Procedure to configure the GCap for the first connection* 2 - *Procedure to put a GCap into operation*
Display the current keyboard language	1 - Display: use the *show keymap* command
Modify the keyboard language.	1 - Display: use the *show keymap* command 2 - Modify: use the *set keymap* command
Configuring the Gcap interface: (GUI or CLI)	1 - Display: use the *show network-config* command 2 - Modify: use the *set network-config* command
Display the date and time	1 - Display: use the *show datetime* command
Modify the date and time	1 - Display: use the *show datetime* command 2 - Modify: refer to the *set datetime* or *Procedure to change the date and time of the GCap* command
Enable or disable colors for the current CLI session	1 - Use the *color* command
Display the current compatibility mode with the GCenter	1- Show: use the *show compatibility-mode* command
Modify the compatibility mode with the GCenter	1- Show: use the *show compatibility-mode* command 2 - Modify: use the *set compatibility-mode* command
Pairing the GCap with GCenter	1 - Refer to the *pairing* or *Procedure to pair a GCap with the GCenter* command
Unpair the GCap	1 - Refer to the *exit* command

- Manage the accounts

To perform the following task	Carry out the following procedures in succession
Display the list of users	1 - Display the list: use the *show passwords* command
Modify the passwords	1 - Display the list: use the *show passwords* command 2 - Change passwords: use the *set passwords* command
Change the SSH keys	1 - Use the *set ssh-keys* command
Display the password policy	2 - Use the *show password-policy* command
Unlock blocked accounts	1 - Use the *system unlock* command
Modify the password management policy	1 - Use the *set password-policy* command
Display the protection policy against brute force attacks	1 - Use the *show bruteforce-protection* command
Modify the protection policy against brute force attacks	1 - Use the *set bruteforce-protection* command
Display the duration of inactivity before disconnection	1 - Use the *show session-timeout* command
Modify the duration of inactivity before disconnection	1 - Use the *set session-timeout* command

- manage the detection engine

To perform the following task	Carry out the following procedures in succession
Display advanced options of the Sigflow configuration	1 - Use the *show monitoring-engine* command
Apply a Sigflow advanced configuration	1 - Use the *set monitoring-engine* command
Start the Sigflow detection engine	1 - Use the *monitoring-engine start* command
Stop the Sigflow monitor engine	1 - Use the *monitoring-engine stop* command
Display the detection engine status	1 - Use the *monitoring-engine status* command
Replay a pcap file of traffic generation	1 - Use the *replay* command

- Manage the network

To perform the following task	Carry out the following procedures in succession
Display the information of the network interfaces (capture, `tunnel`>, ```management>)	1 - Use the *show interfaces* command
Modify the `management` or `tunnel` interface configuration :	1 - Use the *set network-config* command
Managing Tunnel and Management interfaces	1 - refer to *Procedure to manage the network parameters of 'Tunnel' and 'Management' interfaces*
Switch to the single-interface configuration	1 - Refer to *Procedure to switch the single-interface configuration*
Switching to the dual-interface configuration	1 - Refer to *Procedure to switch to the configuration dual-interface*
Modify the GCap domain name	1 - Use the *set network-config* command
Display the IP address of the GCenter with which the GCap is paired	1 - Use the *show gcenter-ip* command
Modify the IP address of the GCenter to which the GCap will be paired	1 - Use the *set gcenter-ip* command
Display the MTU value of the network interfaces (capture, `tunnel`, `management`)	1 - Use the *show interfaces* command
Modify the MTU value of the network interfaces (capture, `tunnel`, `management`)	1 - Enter the *set advanced-configuration mtu* command
Manage the capture interfaces `monx`	1 - Use the *set interfaces* command
Manage the capture interfaces `monx`	1 - refer to *Procedure to manage the 'monx' capture interface settings*
Configure the aggregation of capture interfaces `monx`	1 - refer to *set interfaces* ou *Procedure to manage capture interface aggregation*

- Manage the server

To perform the following task	Carry out the following procedures in succession
Display help on the commands	1 - Use the *help* command
Exit the current context	1 - Use the *exit* command
Leave the SSH session	1 - Use the *exit* command
System: shut down the GCap	1 - Use the *system shutdown* command
Système : restart the GCap	1 - Use the *system restart* command

- Monitoring the GCAP

To perform the following task	Carry out the following procedures in succession
Display the current status of the GCap	1 - Use the *show status* command
Display the statistics of the Sigflow detection engine	1 - Use the *show eve-stats* command
Display statistics and health information	1 - Use the *show health* command
Extract the information from the GCap as requested by technical support	1 - Use the *show tech-support* command

7.4 How to connect to Gcap?

Access to the GCap can be made:

- Either by a direct connection (connect directly to the server)
  This is necessary if the network configuration is not yet completed on the GCap
  For implementation, refer to *Procedure to connect directly to the GCap via keyboard and screen*
- Or by a HTTP remote connection (iDRAC function for a Dell server)
  This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems
  For implementation, refer to *Procedure to connect the iDRAC in HTTP (DELL server)*
- Or by a remote connection to the CLI in SSH via the iDRAC interface in serial port redirection mode
  This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems
  For implementation, refer to *Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
- Or by a remote connection to the CLI in SSH via the network interface with the role `management`
  This connection is the nominal way to access the GCap
  For more information, refer to *Procedure to remote connection to GCap via an SSH tunnel*

Note:

The list of physical connectors to use was described in the PRESENTATION - General section.

7.5 Remote connection to the GCenter

Remote access to the GCenter is done either:

- By SSH to configure the GCenter.
  For more information, please refer to the GCenter documentation.
- via a web browser in order to pair the GCap.
  For more information, refer to *Procedure to connect to the GCenter via a web browser*.

Chapter 8

List of procedures

8.1 List of potential actions

8.1.1 Accessing the GCap and GCenter

To perform the following task	Choose the following procedure
Connect to the GCap by a direct connection	1 - *Procedure to connect directly to the GCap via keyboard and screen*
Remote connection to iDRAC via HTTP	1 - *Procedure to connect the iDRAC in HTTP (DELL server)*
Remote SSH connection in serial port forwarding mode	1 - *Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
Connect to the GCenter via a web browser	1 - *Procedure to connect to the GCenter via a web browser*
Remote connection to GCap via an SSH tunnel	1 - *Procedure to remote connection to GCap via an SSH tunnel*

8.1.2 Configuring the GCap

To perform the following task	Carry out the following procedures in succession
Install a GCAP	1 - *Procedure to configure the GCap for the first connection* 2 - *Procedure to put a GCap into operation*
Display the current keyboard language	1 - Display: use the *show keymap* command
Modify the keyboard language.	1 - Display: use the *show keymap* command 2 - Modify: use the *set keymap* command
Configuring the Gcap interface: (GUI or CLI)	1 - Display: use the *show network-config* command 2 - Modify: use the *set network-config* command
Display the date and time	1 - Display: use the *show datetime* command
Modify the date and time	1 - Display: use the *show datetime* command 2 - Modify: refer to *Procedure to change the date and time of the GCap*
Enable or disable colors for the current CLI session	1 - Use the *color* command
Compatibility mode with the GCenter	1- Show: use the *show compatibility-mode* command 2 - Modify: use the *set compatibility-mode* command
Pairing the GCap with GCenter	1 - Refer to *Procedure to pair a GCap with the GCenter*

8.1.3 Managing accounts

To perform the following task	Carry out the following procedures in succession
Display the list of users	1 - Display the list: use the *show passwords* command
Modify the passwords	1 - Display the list: use the *show passwords* command 2 - Change passwords: use the *set passwords* command
Change the SSH keys	1 - Use the *set ssh-keys* command
Display the password policy	2 - Use the *show password-policy* command
Unlock blocked accounts	1 - Use the *system unlock* command
Modify the password management policy	1 - Use the *set password-policy* command
Display the protection policy against brute force attacks	1 - Use the *show bruteforce-protection* command
Modify the protection policy against brute force attacks	1 - Use the *set bruteforce-protection* command
Display the duration of inactivity before disconnection	1 - Use the *show session-timeout* command
Modify the duration of inactivity before disconnection	1 - Use the *set session-timeout* command

8.1.4 Manage the network

To perform the following task	Carry out the following procedures in succession
Managing Tunnel and Management interfaces	1 - refer to *Procedure to manage the network parameters of 'Tunnel' and 'Management' interfaces*
Display the GCenter IP address	1 - Use the *show gcenter-ip* command
Modify the IP address of the GCenter	1 - Use the *set gcenter-ip* command
Manage the capture interfaces `monx`	1 - refer to *Procedure to manage the 'monx' capture interface settings*
Manage interface aggregation of capture	1 - refer to *Procedure to manage capture interface aggregation*
Switch to the single-interface configuration	1 - Refer to *Procedure to switch the single-interface configuration*
Switching to the dual-interface configuration	1 - Refer to *Procedure to switch to the configuration dual-interface*

8.1.5 Manage the detection engine

To perform the following task	Carry out the following procedures in succession
Display advanced options of the Sigflow configuration	1 - Use the *show monitoring-engine* command
Apply a Sigflow advanced configuration	1 - Use the *set monitoring-engine* command
Start the Sigflow detection engine	1 - Use the *monitoring-engine start* command
Stop the Sigflow monitor engine	1 - Use the *monitoring-engine stop* command
Display the detection engine status	1 - Use the *monitoring-engine status* command
Replay a pcap file of traffic generation	1 - Use the *replay* command

8.1.6 Managing server

To perform the following task	Carry out the following procedures in succession
Display help on the commands	1 - Use the *help* command
Exit the current context	1 - Use the *exit* command
Leave the SSH session	1 - Use the *exit* command
Restart the GCap	1 - Use the *system restart* command
Shut down the GCap	1 - Use the *system shutdown* command

8.1.7 Monitoring the GCAP

To perform the following task	Carry out the following procedures in succession
Display the current status of the GCap	1 - Use the *show status* command
Display the statistics of the Sigflow detection engine	1 - Use the *show eve-stats* command
Display statistics and health information	1 - Use the *show health* command
Extract the information from the GCap as requested by technical support	1 - Use the *show tech-support* command

8.2 Procedure to configure the GCap for the first connection

A - Introduction

The procedure described here explains how to set up the GCap when it is first installed.

To perform this procedure, you must perform all the steps described in the following sections:

- *B - Preliminary operations*
- *C - Procedure*

B - Prerequisites

- **User:** setup

B - Preliminary operations

1. Check that the LUKS key is connected to the GCap

   Note:

   If there is no LUKS key or if it is the wrong one, the operating system will not be able to access the contents on the hard drives
   In case of problems, check:

   - Whether the correct key is used and not one from another GCap...
   - The USB port is working properly: change the USB port

2. Connect to the GCap
3. Depending on the situation:
   - Either connect directly to the GCap via keyboard and screen (see *Procedure to connect directly to the GCap via keyboard and screen*)
   - Either connect directly to the GCap via the iDRAC (see *Procedure to connect the iDRAC in HTTP (DELL server)*)
4. Connect as **setup**

   Note:

   The first time you log in to the GCap, a prompt to change your password will be displayed
   Make sure the keyboard configuration is correct (fr or en version)

C - Procedure

1. Manage passwords (passwords, SSH keys, and the like): see the *Managing accounts* table
2. Manage network interfaces with `Tunnel` and `Management` roles: see the *Manage the network* table
   1. Configure the IP addressing
   2. Enter the GCap name and the domain name
   3. Configure the MTU value if necessary

      To do this, refer to *Procedure to manage the network parameters of 'Tunnel' and 'Management' interfaces*
3. Connect to the GCap via a remote connection through an SSH tunnel (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
4. Set the operating mode for the SSH link to single-interface or dual-interface

   To do this, refer to *Procedure to switch the single-interface configuration* or *Procedure to switch to the configuration dual-interface*
5. Manage the GCap date and time, refer to *Procedure to change the date and time of the GCap*
6. Manage the capture interfaces : see the *Manage the network*
   1. Activate the desired interfaces
   2. Configure the MTU value

      To do this, refer to *Procedure to manage the 'monx' capture interface settings*
7. If needed, manage the aggregation of detection interfaces: refer to *Procedure to manage capture interface aggregation*
8. Pair the GCap with the GCenter : refer to *Procedure to pair a GCap with the GCenter*

8.3 Procedure to put a GCap into operation

A - Introduction

After configuring the GCap, this procedure describes how to start operating the GCap.

To perform this procedure, you must perform all the steps described in the following sections:

- *C - Preliminary operations*
- *D - Procedure to be followed on the GCap*
- *E - Procedure to be carried out on the GCenter*

B - Prerequisites

- **User:** setup

C - Preliminary operations

1. Perform the *Procedure to configure the GCap for the first connection*
2. Activate the required `monx` capture interfaces: refer to *Procedure to manage the 'monx' capture interface settings*

D - Procedure to be followed on the GCap

1. Start the detection engine: refer to *Manage the detection engine* table
   The system displays the following command prompt:

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

   The command prompt indicates the status of the detection engine : here it is stopped.

2. Enter the command

   ```
   monitoring-engine start
   ```

3. Validate
4. Wait for the engine to be up and running
5. Check the status of the detection engine
   The system displays the following command prompt:

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

   The command prompt indicates the status of the detection engine : here it is started

---

E - Procedure to be carried out on the GCenter

1. Apply a ruleset to the GCap
2. Enable or disable the shellcode detection
3. Enable or disable powershell detection
4. Configure the Sigflow specific parameters, namely Base variables, Net variables and File rules management

---

8.4 Procedure to connect directly to the GCap via keyboard and screen

A - Introduction

This connection is not the normal way to access the GCap but is necessary when the network configuration has not yet been performed on the GCap (or in case of unawareness of the network address)
The first connection to the GCap can be done by a direct connection with a keyboard and monitor
There is no specific configuration required other than knowing the iDRAC login name and password.

Note:

The default login and password are provided in the server manufacturer's documentation.

To perform this procedure, you must perform all the steps described in the following sections:

- *C - Preliminary operations*
- *D - Procedure for connecting the screen and keyboard*
- *E - Procedure to obtain the network settings via the BIOS*
- *F - Procedure to access the CLI*

B - Prerequisites

- **User:** setup

C - Preliminary operations

1. Connect the GCap power cables
2. Connect the network cables of the GCap (refer to *Description of the GCap inputs / outputs*)

D - Procedure for connecting the screen and keyboard

1. Connect the screen to the VGA connector of the GCap
2. Connect the keyboard to the USB connector of the GCap
3. Switch on the server

E - Procedure to obtain the network settings via the BIOS

1. Press **F2** during the boot up self-test (POST)
2. On the `` `System Setup Main Menu` `` page (main menu of the configuration of the system), click on `` `iDRAC Settings` ``
   The `` `Paramètres iDRAC` `` page appears
3. Click on `` `Réseau` ``
   The `` `Réseau` `` page appears
4. Note the network settings in the `` `Network Settings` `` settings
5. After noting down the network settings, exit the BIOS
6. Click successively on `` `Retour` ``, `` `Terminer` `` and `` `Non` ``

F - Procedure to access the CLI

A progress bar is displayed:

```
gcap-protor login:
```

1. Enter the login and the corresponding password
   The command prompt is displayed

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

Note:

The first time you log in to the GCap, a prompt to change your password will be displayed.

Note:

- Press **Tab** to display all available commands
- Press **Entrée** to display all available commands along with a short explanation

Tip:

- If a password error occurs, the protection system will be activated
- To view the policy setting on the Gcap, use the `show bruteforce-protection` command
  After a certain number of failures, the account will be locked
- To unlock it: either wait, or use the `system unlock` command with a higher privilege level account

8.5 Procedure to connect the iDRAC in HTTP (DELL server)

A - Introduction

This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
This procedure describes the remote connection from a distant PC using :

- The network connection to the iDRAC port of the GCap
- A WEB browser

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

From the iDRAC web page, it is possible to:

- View the material resources, their status and the BIOS configurations
- Interact with the server to turn it on, off and restart it
- Connect to the GCap via the CLI console

Tip:

- If a password error occurs, the protection system will be activated
- To view the policy setting on the Gcap, use the `` `show bruteforce-protection` `` command
  After a certain number of failures, the account will be locked
- To unlock it: either wait, or use the `` `system unlock` `` command with a higher privilege level account

To perform this procedure, you must perform all the steps described in the following sections:

- *C - Preliminary operations*
- *D - Procedure*
- *E - Special cases*

B - Prerequisites

- **User:** setup

C - Preliminary operations

- Perform the network configuration (IP address of the iDRAC) : otherwise, use *Procedure to connect directly to the GCap via keyboard and screen* to connect to the GCap

---

D - Procedure

1. On the remote PC, open a web browser
2. Enter the IP address of the GCap iDRAC interface and confirm
   The `` `Login` `` window is displayed
3. Enter the requested parameters:
   - `` `Username` ``: login name
   - `` `Password` `` : password of the entered login
   - `` `Domain` `` : select `` `This IDRAC` ``
4. Click on the `` `Submit` `` button
5. Launch the virtual console (`` `Virtual console Preview` `` zone, `` `Launch` `` button)
   Following this action, a new page will open. It will be possible to interact with the GCap
6. Connect to the CLI (`` `gcap-cli` `` command)
   After connection, the following message is displayed:

```
(gcap-cli)
```

Note:

- Press **Tab** to display all available commands
- Press **Entrée** to display all available commands along with a short explanation

---

E - Special cases

It is possible to open an SSH connection, run a CLI command line and then close the connection
To do this:

1. Enter the command

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

2. Validate

   The system:
   - Opens the SSH connection
   - Executes the command (here `show status`) then
   - Closes the SSH connection

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

8.6 Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode

A - Introduction

This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
This procedure describes the remote connection from a distant PC using :

- The network connection to the iDRAC port of the GCap
- A connection tool via SSH

This access requires:

- Knowledge of the iDRAC login name and password (iDRAC access)
- The network configuration is complete (IP address of the iDRAC is known)

From the interface, it is possible to:

- View the operating system messages
- Connect to the GCap via the CLI console

Tip:

- If a password error occurs, the protection system will be activated
- To view the policy setting on the Gcap, use the `` `show bruteforce-protection` `` command
  After a certain number of failures, the account will be locked
- To unlock it: either wait, or use the `` `system unlock` `` command with a higher privilege level account

To perform this procedure, you must perform all the steps described in the following sections:

- *B - Preliminary operations*
- *C - Procedure*
- *D - Special cases*

B - Prerequisites

- **User:** setup

B - Preliminary operations

1. Perform the network configuration (IP address of the iDRAC)
   Otherwise, use *Procedure to connect directly to the GCap via keyboard and screen* to connect to the GCap

---

C - Procedure

1. - On the remote PC running Linux:
   1. Open a command prompt
   2. Enter the command

      ```
      ssh identifiant@adresse_ip
      ```

      For example, `` `ssh setup@gcenter` `` where

      - `` `setup` `` is the identifier and
      - x.x.x.x is the IP address of the GCap's iDRAC port
   3. Validate the command
   4. Enter password of the entered login
   5. Press `` `Enter` `` to display all available commands and a short explanation
   - On a Windows PC:
   1. Open an SSH client software, such as Putty
   2. Enter the IP address of the GCap iDRAC interface and confirm
2. Enter the command

   ```
   racadm>>console com2
   ```
3. Validate
   The system now displays the graphical interface of the device
   Following this action, a new page will open. It will be possible to interact with the GCap
4. Log on to the CLI.

```
gcap-cli
```

5. Validate
   After connection, the following message is displayed:

```
(gcap-cli)
```

> **Note:**
> - Press **Tab** to display all available commands
> - Press **Entrée** to display all available commands along with a short explanation

---

D - Special cases

It is possible to open an SSH connection, run a CLI command line and then close the connection.
To do this:

1. Enter the command

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

2. Validate
   The system:
   - Opens the SSH connection
   - Executes the command (here `show status) then
   - Closes the SSH connection

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

8.7 Procedure to remote connection to GCap via an SSH tunnel

A - Introduction

This procedure describes how to connect from a remote PC securely using an SSH tunnel.
Remote access to the GCap CLI is achieved via the network connection to the port:

- with the `management` role (dual-interface configuration)
- with the `management-tunnel` role (single interface configuration)

Tip:

- If a password error occurs, the protection system will be activated
- To view the policy setting on the Gcap, use the `show bruteforce-protection` command
  After a certain number of failures, the account will be locked
- To unlock it:
  - either wait
  - or use the `system unlock` command with a higher privilege level account

To perform this procedure, you must perform all the steps described in the following sections:

- *B - Preliminary operations*
- *C - Procedure*

B - Prerequisites

- **User:** setup, gviewadm, gview

B - Preliminary operations

1. Make an initial connection to the GCap (see *Procedure to connect directly to the GCap via keyboard and screen*)
2. Learn the name of the GCap or its IP address (refer to *Procedure to manage the network parameters of 'Tunnel' and 'Management' interfaces*)

C - Procedure

- On the remote PC running Linux:
  1. Open a command prompt
  2. Enter the command:

     ```
     ssh identifiant@adresse_ip```
     ```

     For example, `ssh setup@gcenter` where

     - `setup` is the identifier and
     - `IPADDRESS` is the IP address of the GCap's iDRAC port
  3. Validate the command
  4. Enter password of the entered login
  5. Press `Enter` to display all available commands and a short explanation
- On a Windows PC:
  1. Open an SSH client software, such as Putty
  2. Enter the IP address of the GCap then validate

The command prompt is displayed.

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

Note:

- Press `Tab` to display all available commands
- Press `Enter` to display all available commands and a short explanation

---

8.8 Procedure to connect to the GCenter via a web browser

A - Introduction

This procedure describes how to connect from a remote PC to the GCenter via a web browser.

To perform this procedure, you must perform all the steps described in the following sections:

- *B - Preliminary operations*
- *C - Procedure*

B - Preliminary operations

1. Know the name of the GCenter or its IP address
2. Connect to a PC linked to the GCap and GCenter network

C - Procedure

On the remote PC:

1. Open a web browser
2. Enter the following URL:
   - `ssh identifiant@adresse_ip`
   - or `ssh identifiant@FQDN`

   For example: `ssh setup@gcenter.domain.com` with:
   - The identifier is `setup`
   - the FQDN is `gcenter.domain.com`
3. Validate

   The GCenter login window is displayed
   - Enter the identifier
   - Enter the password
   - Validate

The GCenter graphical interface is displayed.

Note:

Refer to the GCenter documentation

8.9 Procedure to change the date and time of the GCap

A - Introduction

Before pairing between the GCap and the GCenter, it is necessary to ensure that both systems are at the same time.
Once the pairing is functional, the GCenter acts as the NTP server for the GCap so that the clocks of the equipment are synchronized.
When connecting for the first time, these items must be set via the *show datetime* command in the CLI.
The adjustment is necessary for establishing the IPsec tunnel.
The datetime of the GCap and the GCenter must be the same to within 1 minute.

Important:

If there is a discrepancy between the GCap and the GCenter, the GCap time is the one to be changed.

To perform this procedure, you must perform all the steps described in the following sections:

- *B - Prerequisites*
- *C - Preliminary operations*
- *D - Procedure to view the date and time on the GCap and GCenter*
- *F - Procedure to change the date and time of the GCap*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show datetime*
  - *set datetime*

C - Preliminary operations

1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
2. Connect as **setup**

D - Procedure to view the date and time on the GCap and GCenter

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show datetime
   ```

2. Validate

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

   The `datetime` command of the `show` sub-group enables displaying the date and time of the GCap in the format `YYYY-MM-DD HH:MM:SS`.

3. Log in to the GCenter
4. Display the GCenter date and time and note them down
   If there is a discrepancy between the GCap and the GCenter, the GCap time is the one to be changed
   To correct this, perform the following procedure

F - Procedure to change the date and time of the GCap

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the *show datetime* command followed by the parameters in the following order {YYYY-MM-DDThh :mm :ssZ}
   Example: set datetime 2022-01-26T16:00:00Z
   - YYYY indicates a four-digit year from 0000 to 9999
   - MM indicates a two-digit year from 01 to 12
   - DD indicates a two-digit year from 01 to 31

- T indicates the beginning of the field defining the time format
- hh indicates the two-digit hour from 00 to 23
- mm indicates the two-digit minutes from 00 to 59
- ss indicates the two-digit seconds from 00 to 59
- Z indicates CUT (Coordinated Universal Time)

```
set datetime 2022-01-26T16:00:00Z
```

2. Validate

   A confirmation window is displayed

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

8.10 Procedure to manage the network parameters of `Tunnel` and `Management` interfaces

A - Introduction

This procedure describes:

- Viewing the network settings
- Modifying these parameters

For...	Use the command	carry out the procedures successively
obtain an overview of the information on all network interfaces	*show network-config*	1 - *C - Preliminary operations* 2 - *D - Procedure to display the network configuration*
display for each interface: MAC address, carrier presence, speed, and type of connection	*show network-config*	1 - *C - Preliminary operations* 2 - *E - Procedure to display the status of the GCap network interfaces*
display or change the domain name	*show network-config domain* or *set network-config domain*	1 - *C - Preliminary operations* 2 - *F - Procedure to display/change the GCap domain name*
display or change the system name	*show network-config hostname* or *set network-config hostname*	1 - *C - Preliminary operations* 2 - *G - Procedure to display or change the GCap name*
display or modify the interface used in SSH for administering the GCap and the GCap GCenter link	*show network-config ssh* or *set network-config ssh*	1 - *C - Preliminary operations* 2 - *H - Procedure to display or modify the interface used to manage the GCap in SSH*
display or modify the MTU value of the interfaces show	*show interfaces* or *set advanced-configuration mtu*	1 - *C - Preliminary operations* 2 - *I - Procedure to display or change the MTU value*
display or modify the TCP/IP settings of the Management / Tunnel interfaces	*show network-config gcp0*	1 - *C - Preliminary operations* 2 - *J - Procedure to display or modify the TCP/IP settings of a 'management' and/or 'tunnel' interface*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show network-config*
  - *show interfaces*
  - *show network-config domain*
  - *set network-config domain*
  - *show network-config hostname*
  - *set network-config hostname*
  - *show network-config ssh*
  - *set network-config ssh*
  - *set network-config*
  - *set advanced-configuration mtu*
  - *show network-config management*
  - *set network-config management*
  - *show network-config gcp0*

C - Preliminary operations

- Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
- Stop the Sigflow detection engine (refer to *monitoring-engine*)

D - Procedure to display the network configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show  network-config configuration
   ```

2. Validate
   The system displays the information of all network interfaces
   In this procedure, only the information on the management and tunnel network interfaces is detailed
   For information on capture interfaces `monx`, refer to *Procedure to manage the 'monx' capture interface settings*
   The system displays the following information:
   - System name (**hostname**)
   - Domain name (**domain_name**)
   - Details of the TCP/IP settings for each network interface (`management` and `tunnel`)
   - Whether or not the interface is enabled


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


Note:

The configuration in the above example is dual interface.

E - Procedure to display the status of the GCap network interfaces

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show interfaces
   ```

2. Validate.
   The system displays the status of the GCap network interfaces.

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

   For each interface, the following information is displayed:

   - `Label`: the label name of the interface
   - `Name`: the system name of the interface
   - `Role`: the role assigned to the interface
   - `Capture capability`: if the interface can capture traffic
   - `MTU`: the MTU of the interface
   - `Physical Address`: the MAC address of the interface
   - `Speed`: the interface speed
   - `Type`: the type of cable/sfp connected to the physical port

- `Vendor ID`: the Vendor ID of the network card
- `Device ID`: the ID of the network card
- `PCI bus`: PCI bus number used by the network card

F - Procedure to display/change the GCap domain name

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the current name:
   1. Enter the command

      ```
      show network-config domain
      ```

   2. Validate

      The system displays the domain name

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

2. To change the current name:
   1. Enter the command

      ```
      set network-config domain-name gatewatcher.com
      ```

   2. Validate

      ```
      Setting hostname/domain name to:
         - Hostname: gcap-int-129-dag
         - Domain name: gatewatcher.com
      Do you want to appl.. _proc9E:y this new configuration? (y/N)
      ```

   3. Press the <y> button
   4. Validate

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

3. To check the value modification:
   1. Enter the following command

      ```
      show network-config domain
      ```

   2. Validate

      The system displays the domain name

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

G - Procedure to display or change the GCap name

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the current name:
   1. Enter the command

      ```
      show network-config hostname
      ```

   2. Validate

      The system displays the interface the host name of the GCap

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

2. To change the current name:
   1. Enter the command

      ```
      set network-config hostname gcap-name
      ```

   2. Validate

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

   3. Press the <y> button
   4. Validate

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

3. To check the value modification:
   1. Enter the following command

```
show network-config hostname
```

   2. The system displays the host name of the GCap.

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

H - Procedure to display or modify the interface used to manage the GCap in SSH

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the current configuration:
   1. Enter the command

```
show interfaces
```

   2. Validate

      The system displays the role of the different interface of GCap (`management` for SSH connection management, `tunnel` for IPSec tunnel, `management-tunnel` for both)
      - In the case of the single-interface configuration, the system displays:

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

      - In the case of the dual-interface configuration, the system displays:

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

2. To configure the `enpXXXX` interface for SSH and the `enpYYYY` interface for IPSec :
   1. Enter the command

```
set interfaces assign-role enpXXXX management
```

   2. Validate
   3. Enter the command

```
set interfaces assign-role enpYYYY tunnel
```

   4. Validate
   5. Enter the command

> **Note:**
>
> Replace in the following commands:
> - IP by its value
> - GATEWAY by its value
> - MASK by its value

```
set network-config management ip-address IP gateway GATEWAY mask MASK
```

   6. Validate
   7. Enter the command

```
set network-config tunnel ip-address IP gateway GATEWAY mask MASK
```

   8. Validate
3. To configure the `enpXXXX` interface for SSH and IPSec:

> **Note:**
>
> No other interface is not used.

   1. Enter the command

```
set interfaces assign-role enpXXXX management-tunnel
```

   2. Validate

3. Enter the command

```
set network-config management ip-address IP gateway GATEWAY mask MASK
```

4. Validate

I - Procedure to display or change the MTU value

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the current configuration of enabled interfaces:
   1. Enter the command

      ```
      show interfaces
      ```

   2. Validate

      The system displays the result

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

      The values are displayed for all enabled network interfaces.

2. To change the current configuration of enabled interfaces: e.g. to change the MTU value of the `management` interface:
   1. Enter the command

      ```
      set advanced-configuration mtu enp19s0 2000
      ```

   2. Validate

      The system displays the result

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

J - Procedure to display or modify the TCP/IP settings of a `management` and/or `tunnel` interface

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the `management` and `tunnel` interface configuration :
   1. Enter the command

      ```
      show network-config management
      ```

   2. Validate

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

2. To change the configuration of the `management` interface address :
   1. Enter the command

      ```
      set network-config management ip-address IP gateway GATEWAY mask MASK conf
      ```

   2. Validate

      The system displays the `management` interface configuration.

      ```
      Setting interface management to configuration :
         - IP Address:
         - Mask:
      ```

(continues on next page)

(continued from previous page)

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

3. Press the <y> button
4. Validate

8.11 Procedure to manage the `monx` capture interface settings

A - Introduction

This procedure describes:

- Viewing the network settings
- Modifying these parameters

For...	Use the command	carry out the procedures successively
obtain an overview of the information on all network interfaces	*show network-config*	1 - *C - Preliminary operations* 2 - *D - Procedure to display the network configuration*
display the MTU value of the interfaces	*show interfaces*	1 - *C - Preliminary operations* 2 - *E - Procedure to display or change the MTU value*
modify the MTU value of the interfaces	*set advanced-configuration mtu*	1 - *C - Preliminary operations* 2 - *E - Procedure to display or change the MTU value*
Display the available capture interfaces	*show interfaces*	1 - *C - Preliminary operations* 2 - *F - Procedure to display, activate or deactivate the capture interfaces*
manage the available capture interfaces	*set interfaces*	1 - *C - Preliminary operations* 2 - *F - Procedure to display, activate or deactivate the capture interfaces*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show network-config*
  - *set advanced-configuration mtu*
  - *show interfaces*
  - *set interfaces*

C - Preliminary operations

1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
2. Stop the Sigflow detection engine (refer to *monitoring-engine*)

D - Procedure to display the network configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show interfaces
   ```

2. Validate
   The system displays the information of all network interfaces

```
(gcap-cli) show interfaces

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

Note:

The `mon0`, `mon1`, `mon2` interface is enabled (field: **role**, value : **capture**)
The `enp27s0` interface is disabled (field: **role**, value : **inactive**)

E - Procedure to display or change the MTU value

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the current configuration of enabled interfaces:
   1. Enter the command

      ```
      show interfaces
      ```

   2. Validate
      The system displays the result

      ```
      (gcap-cli) show interfaces

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

      The values are displayed for all enabled network interfaces (*MTU* field)

2. In our example, to change the current configuration of enabled interfaces: e.g. to change the MTU value of the `mon0` interface
   The command prompt is displayed

   ```
   (gcap-cli)
   ```

   1. Enter the command

      ```
      set advanced-configuration mtu mon1 2000
      ```

   2. Validate
      The system displays the result

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

F - Procedure to display, activate or deactivate the capture interfaces

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the information on the capture interfaces:
   1. Enter the command

      ```
      show interfaces
      ```

   2. Validate
      The system displays the available capture interfaces

```
(gcap-cli) show interfaces

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

The information displayed is:

- `Label`: the label name of the interface
- `Name`: the system name of the interface
- `Role`: the role assigned to the interface
- `Capture capability`: if the interface can capture traffic
- `MTU`: the MTU of the interface
- `Physical Address`: the MAC address of the interface
- `Speed`: the interface speed
- `Type`: the type of cable/sfp connected to the physical port
- `Vendor ID`: the Vendor ID of the network card
- `Device ID`: the ID of the network card
- `PCI bus`: PCI bus number used by the network card
- In our example, `mon0`, `mon1` et `mon2` are enabled (field: **role**, value : **capture**).

2. To activate an interface (here enp27s0 for example):
   1. Enter the command

```
set interfaces assign-role enp27s0 capture
```

   2. Validate
   3. then to check the new configuration

```
show interfaces
```

   4. Validate

      The system displays the available capture interfaces

```
Label       Name      Role        Capture capability MTU   Physical Address   Speed  Type  Vendor ID  Device ID  PCI bus
mon0        enp4s0    capture     Available          1500  00:50:56:91:8d:35  1Gb    RJ45  0x8086     0x10d3     04:00.0
tunnel      enp11s0   tunnel      Available          1500  00:50:56:00:03:01  10Gb   RJ45  0x15ad     0x07b0     0b:00.0
mon1        enp12s0   capture     Available          1500  00:50:56:91:d4:30  1Gb    RJ45  0x8086     0x10d3     0c:00.0
management  enp19s0   management  Available          1500  00:50:56:00:03:02  10Gb   RJ45  0x15ad     0x07b0     13:00.0
mon2        enp20s0   capture     Available          1500  00:50:56:91:c3:e3  1Gb    RJ45  0x8086     0x10d3     14:00.0
mon4        enp27s0   capture     Available          1500  00:50:56:00:03:03  1Gb    RJ45  0x8086     0x10d3     1b:00.0
monvirt     monvirt   capture     Available          1500  N/A                N/A    N/A   N/A        N/A        N/A
```

3. To deactivate an interface (here `mon0` for example):
   1. Enter the command

```
set interfaces assign-role enp27s0 inactive
```

   2. Validate
4. To change the interface startup delay by five seconds for example
   1. Enter the command

```
set interfaces delay 5
```

   2. Validate

8.12 Procedure to switch the single-interface configuration

A - Introduction

In single-interface configuration, the SSH connection for managing the GCap and the VPN communication are handled by one interface with the role `management-tunnel`.
In dual-interface configuration:

- The VPN communication is controlled by one interface with the role `tunnel`
- The SSH connection for GCap management is handled by the interface with the role `management`

This procedure outlines the switchover from a dual-interface configuration to a single-interface configuration.

Important:

The user will lose the session if the connection between the GCap and the user's PC is made remotely via SSH.
In order to avoid this disconnection, connect to the GCap:

- Either by a direct connection (connect directly to the server)
- Or by a HTTP remote connection (iDRAC function for a Dell server)
- Or by a remote connection to the CLI in SSH via the iDRAC interface in serial port redirection mode

For...	Use the command	carry out the procedures successively
Display the current configuration	*show interfaces*	1 - *C - Preliminary operations* 2 - *D - Procedure to display the current configuration*
Switch from dual to single interface configuration	*unpair* *set network-config* *set network-config*	1 - *C - Preliminary operations* 2 - *E - Procedure to switch from dual to single interface configuration*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show interfaces*
  - *set network-config*
  - *set network-config*
  - *unpair*

C - Preliminary operations

- Depending on the situation, refer to:
  - the *Procedure to connect directly to the GCap via keyboard and screen*
  - the *Procedure to connect the iDRAC in HTTP (DELL server)*
  - the *Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
- Stop the Sigflow detection engine (refer to *monitoring-engine*).

D - Procedure to display the current configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the `management` and `tunnel` interface configuration :
   1. Enter the command

      ```
      show interfaces
      ```

   2. Validate
      The system displays the `management` and `tunnel` interfaces configuration
      - The **single interface configuration**
        The SSH and VPN connections are handled by the `enp19s0` interface.

In this case, the system displays:

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

In our example, the current configuration is single-interface (field: role, value : management-tunnel)
In this case, there is nothing to do.

- **In dual-interface configuration**
  The VPN communication is controlled by the `enp11s0` interface.
  The SSH connection for GCap management is handled by the `enp19s0` interface.
  In this case, the system displays:

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

  The role tunnel and role management indicates that the current configuration is dual-interface.

- In this case, continue with this procedure.

E - Procedure to switch from dual to single interface configuration

1. Use the following command to unpair the GCap

```
unpair
```

2. To use the same IP configuration as the interface with `management` role:
   1. Enter the following command to disable the configuration of current `tunnel` interface

```
set interfaces assign-role enp11s0 inactive
```

   2. Validate
   3. Then enter the following command to assign the role `management-tunnel` to the current `management` interface

```
set interfaces assign-role enp19s0 management-tunnel
```

   4. Validate
3. To use another IP configuration than the interface with `management` role:

> **Note:**
>
> Replace in the following commands:
> - IP by its value
> - GATEWAY by its value
> - MASK by its value

   1. Enter the following command to reconfigure the management interface:

```
set network-config management ip-address IP gateway GATEWAY mask MASK confirm
```

   2. Validate
   3. Enter the following command to disable the configuration of current `tunnel` interface:

```
set interfaces assign-role enp11s0 inactive
```

   4. Validate
   5. Then enter the following command to assign the role `management-tunnel` to the current `management` interface

```
set interfaces assign-role enp19s0 management-tunnel
```

   6. Validate

> **Note:**
>
> To apply the IP configuration of current tunnel interface to current management interface, configure current tunnel interface with another network configuration before configuring the management interface.

4. Rewire the GCap network cables if necessary

> **Note:**
>
> It is necessary to add the command attribute 'confirm' at the end of the command (set network-config management) if the pairing with the GCenter is active.

8.13 Procedure to switch to the configuration dual-interface

A - Introduction

In single-interface configuration, the SSH connection for managing the GCap and the VPN communication are handled by one interface with the role `management-tunnel`.
In dual-interface configuration:

- The VPN communication is controlled by one interface with the role `tunnel`
- The SSH connection for GCap management is handled by the interface with the role `management`

This procedure outlines the switchover from a single-interface configuration to a dual-interface configuration.

Important:

The user will lose the session if the connection between the GCap and the user's PC is made remotely via SSH.
In order to avoid this disconnection, connect to the GCap:

- Either by a direct connection (connect directly to the server)
- Or by a HTTP remote connection (iDRAC function for a Dell server)
- Or by a remote connection to the CLI in SSH via the iDRAC interface in serial port redirection mode

For...	Use the command	carry out the procedures successively
Display the current configuration	*show interfaces*	1 - *C - Preliminary operations* 2 - *D - Procedure to display the current configuration*
Switch from single to dual interface configuration	*unpair* *set network-config* *set network-config*	1 - *C - Preliminary operations* 2 - *E - Procedure to switch from single to dual interface configuration*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show interfaces*
  - *set network-config*
  - *set network-config*
  - *unpair*

C - Preliminary operations

- Depending on the situation, refer to:
  - *Procedure to connect directly to the GCap via keyboard and screen*
  - *Procedure to connect the iDRAC in HTTP (DELL server)*
  - *Procedure to remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
- Stop the Sigflow detection engine (refer to *monitoring-engine*).

D - Procedure to display the current configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the `management` and `tunnel` interface configuration :
   1. Enter the command

      ```
      show interfaces
      ```

   2. Validate
      The system displays the `management` and `tunnel` interfaces configuration
   - **In dual-interface configuration**

The VPN communication is controlled by the `enp11s0` interface
The SSH connection for GCap management is handled by the `enp19s0` interface
In this case, the system displays:

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

The role tunnel and role management indicates that the current configuration is dual-interface.
In this case, there is nothing to do.

- The **single interface configuration**
  The SSH and VPN connections are handled by the `enp19s0` interface.
  In this case, the system displays:

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

In our example, the current configuration is single-interface (field: role, value : management-tunnel)
In this case, continue with the following procedure.

E - Procedure to switch from single to dual interface configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Use the following command to unpair the GCap

```
unpair
```

2. Enter the following command to configure the current `management-tunnel` interface with the role `management`

```
set interfaces assign-role enp19s0 management
```

3. Validate
4. Enter the following command to configure the selected interface with the role `tunnel`

```
set interfaces assign-role enp11s0 tunnel
```

5. Validate
6. Enter the following command to configure the tunnel interface IP

> **Note:**
>
> Replace in the following command:
> - IP by its value
> - GATEWAY by its value
> - MASK by its value

```
set network-config tunnel ip-address IP gateway GATEWAY mask MASK confirm
```

7. Validate
8. Rewire the GCap network cables if necessary

8.14 Procedure to manage capture interface aggregation

A - Introduction

This procedure describes the capture interface aggregation.
For more information on aggregation, refer to paragraph *Monx capture interfaces between TAP and GCap: possibility of aggregation*.
The aggregation functionality of the capture interfaces on the GCap leads to impacting some related functions:

- Maximum Transmission Unit (MTU): the maximum size of a packet that can be transmitted at one time without fragmentation.
  set advanced-configuration mtu : takes the largest value of the interfaces that make up the aggregation.
- Static rules for filtering flows captured by capture interface: XDP (eXpress Data Path) filter function.
  XDP filtering is not applied by default to the aggregation created but rather to the interfaces that comprise it.
  It must therefore be applied individually to each aggregated interface.
- File rebuilding rules *Rebuild rule<http://file_capability.html#capacité-de-reconstruction-de-fichiers>* : When enabling interface aggregation and multi-tenant detection, file rebuild rules are not generated.

For...	Use the command	carry out the procedures successively
Display the interfaces aggregation of capture	*show interfaces*	1 - *C - Preliminary operations* 2 - *D - Procedure to manage capture interface aggregation*
Create an interface aggregation	*set network-config*	1 - *C - Preliminary operations* 2 - *E - Procedure to create an interface aggregation*
Display the created aggregation status	*show interfaces*	1 - *C - Preliminary operations* 2 - *F - Procedure to display the created aggregation status*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show interfaces*
  - *set network-config*

C - Preliminary operations

1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
2. Stop the Sigflow detection engine (refer to *monitoring-engine*)

D - Procedure to manage capture interface aggregation

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show interfaces
   ```

2. Validate
   The system displays the information of all network interfaces

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

A specific role is available for cluster: `capture-cluster`
In our example, we don't see this role, so there is no cluster

---

E - Procedure to create an interface aggregation

In our case, we are going to create a cluster with `enp4s0` and `enp12s0`.
The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

```
set interfaces assign-role enp4s0 capture-cluster
set interfaces assign-role enp12s0 capture-cluster
```

2. Validate

F - Procedure to display the created aggregation status

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

```
show interfaces
```

2. Validate
   The system displays the created aggregation

Label	Name	Role	Capture capability	MTU	Physical Address	Speed	Type	Vendor ID	Device ID	PCI bus
cluster0	enp4s0	capture-cluster	Available	1500	00:50:56:91:8d:35	1Gb	RJ45	0x8086	0x10d3	04:00.0
tunnel	enp11s0	tunnel	Available	1500	00:50:56:00:03:01	10Gb	RJ45	0x15ad	0x07b0	0b:00.0
cluster0	enp12s0	capture-cluster	Available	1500	00:50:56:91:d4:30	1Gb	RJ45	0x8086	0x10d3	0c:00.0
management	enp19s0	management	Available	1500	00:50:56:00:03:02	10Gb	RJ45	0x15ad	0x07b0	13:00.0
mon0	enp20s0	capture	Available	1500	00:50:56:91:c3:e3	1Gb	RJ45	0x8086	0x10d3	14:00.0
	enp27s0	inactive	Available	1500	00:50:56:00:03:03	1Gb	RJ45	0x8086	0x10d3	1b:00.0
monvirt	monvirt	capture	Available	1500	N/A	N/A	N/A	N/A	N/A	N/A

In this example, `enp4s0` and `enp27s0` are now aggregated with the role `capture-cluster` in `cluster0`.

8.15 Procedure to pair a GCap with the GCenter

A - Introduction

This procedure describes the pairing between a GCap and a GCenter.
The following operations must be performed:

- On the GCenter, get the IP address of the GCenter
- On the GCap, enter the IP address of the GCenter
- On the GCenter, declare the GCap and generate the One Time Password (OTP)
- On the GCap, pair the GCap and the GCenter

For...	Use the command	carry out the procedures successively
Display the IP address of the GCenter	N/A	1 - *C - Preliminary operations* 2 - *D - Procedure to display the IP address of the GCenter*
Set the compatibility mode on the GCap	*show compatibility-mode* *set compatibility-mode*	1 - *C - Preliminary operations* 2 - *E - Procedure to set the compatibility mode on the GCap*
Set the GCenter IP on the GCap	*show gcenter-ip* *set gcenter-ip*	1 - *E - Procedure to set the compatibility mode on the GCap* 2 - *F - Procedure to set the GCenter IP on the GCap*
Declare the GCap in the GCenter	N/A	1 - *F - Procedure to set the GCenter IP on the GCap* 2 - *G - Procedure to declare the GCap in the GCenter*
Pair the GCap and the GCenter	*pairing otp* *show status*	1 - *G - Procedure to declare the GCap in the GCenter* 2 - *H - Procedure to pair the GCap and the GCenter*
Remove the pairing between a GCap and the GCenter	*unpair*	1 - *C - Preliminary operations* 2 - *I - Procedure to remove the pairing between a GCap and the GCenter*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show compatibility-mode*
  - *set compatibility-mode*
  - *show gcenter-ip*
  - *set gcenter-ip*
  - *show status*
  - *pairing otp*
  - *unpair*

C - Preliminary operations

1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
2. Know the FQDN of the GCap and its IP address
3. Know the FQDN of the GCenter and its IP address
4. Check that the date and time of the GCenter and the GCap match : refer to *Procedure to change the date and time of the GCap*

D - Procedure to display the IP address of the GCenter

1. Connect to the GCenter and display the GCenter network settings
   For more information, please refer to the GCenter documentation

---

E - Procedure to set the compatibility mode on the GCap

1. To view the software version of the GCenter : Log into the GCenter and view the GCenter version number
   The information is located at the bottom left of the GCenter page (GCenter v2.5.3.101-7173-HF3 for example)
2. To display the current compatibility mode between the GCap and the GCenter:
   1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
      The command prompt is displayed

      ```
      (gcap-cli)
      ```

   2. enter the command

      ```
      show compatibility-mode
      ```

   3. Validate
      The system displays the current compatibility mode

      ```
      Current compatibility mode: 2.5.3.101
      ```

   4. Compare the version between the one displayed on the GCap and the one on the GCenter
      In this case:
      - On the GCenter, the version is: v2.5.3.101
      - On the GCap, the mode is: 2.5.3.101

      Thus, the GCap is well configured
      In this example, it is not necessary to modify the compatibility mode
      However, if it is necessary to change the mode, use the following procedure

3. To change the GCap compatibility mode:
   1. Enter the following command (for example for 2.5.3.102 version)

      ```
      set compatibility-mode 2.5.3.102
      ```

   2. Validate

F - Procedure to set the GCenter IP on the GCap

The command prompt is displayed.

```
(gcap-cli)
```

1. To display the GCenter IP:
   1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
   2. Enter the following command

      ```
      show gcenter-ip
      ```

   3. Validate
      The system displays the IP address of the current GCenter : make sure it is the IP address of the GCenter to be paired

      ```
      Current GCenter IP:
      ```

      If there is no paired Gcenter then the following message is displayed :

      ```
      Current GCenter IP: None
      ```

   4. Check that the IP address displayed is that of the GCenter to be paired. If there is a change, continue this procedure
2. To change the GCenter IP:

   Note:

   Replace in the following commands:
   - IP by its value

   1. Enter the command

      ```
      set gcenter-ip IP
      ```

Example: set gcenter-ip X.X.X.X

2. Validate
   The system displays the new IP address of the GCenter

```
Setting GCenter IP to X.X.X.X
```

G - Procedure to declare the GCap in the GCenter

1. Obtain the FQDN (hostname.domain) of the GCap via the `show status` command
2. Connect to the GCenter via a web browser
3. Enter the FQDN (refer to the GCenter documentation)
4. Click on the `Start Pairing` button
   The One Time Password (OTP) is displayed at the top left of the web page
   For example: pcmqsnf7iyo34ianzzi7gbgrr
5. Copy the OTP

H - Procedure to pair the GCap and the GCenter

1. Log on to the GCap CLI
   The command prompt is displayed

```
(gcap-cli)
```

2. Enter the command

```
pairing otp
```

3. Insert the OTP previously generated by the GCenter after positioning the cursor after the text

```
pairing otp pcmqsnf7iyo34ianzzi7gbgrr
```

4. Validate
   The GCap connects to the GCenter via the IP address of the GCenter set on the GCap earlier
   The GCap then calculates the fingerprint using the FQDN of the GCap
   It asks the user to compare it with the fingerprint calculated by the GCenter, which was itself calculated using the FQDN entered
   The system displays the following message:

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

Fingerprint for GCenter x is
e65145b25e229186a32bd3943a3fde70b2c6c3988457e80
0f08b#. Is it correct? (y/N)
```

5. Compare the GCenter fingerprint retrieved by the GCap in the CLI with the one present in the `GCaps pairing..` part under the `GcenterSSH fingerprint` text in the GCenter web interface on the web browser.
   - If the fingerprints are not identical:
     - Check the GCenter IP address and the value entered in the GCap
     - Check the GCap FQDN and the name entered in the GCenter
   - If they are identical, press <Y> and validate

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

6. On the GCenter Web UI, check that the GCap is now Online in the `GCaps pairing and status` menu page.
   For more information, please refer to the GCenter documentation.
7. On the GCap, enter the following command.

```
show status
```

The system displays the following message:

```
Gcap FQDN          : gcap.gatewatcher.com
Version            : #.#.#.0
Overall status     : Running
Tunnel             : Up
Detection Engine   : Up and running
Configuration      : Complete

Gcap name             : gcap
```

(continues on next page)

(continued from previous page)

```
Domain name           : gatewatcher.com
Tunnel interface      :
Management interface  :
Gcenter version       : #.#.#.103
Gcenter IP            :
Paired on Gcenter     : Yes
Monitoring interfaces : mon0,mon2,mon4,monvirt

 © Copyright GATEWATCHER 2024
```

The `Paired on GCenter` field takes the value `Yes`or `No`.

I - Procedure to remove the pairing between a GCap and the GCenter

1. Log on to the GCap CLI
   The command prompt is displayed

   ```
   (gcap-cli)
   ```

2. Enter the command

   ```
   unpair
   ```

3. Validate

8.16 Procedure to optimize performances

A - Introduction

Performance optimization can be achieved in the following ways:

- **Subject 1: adapting the GCap to the network characteristics**
  - Inconsistency between the MTU defined on the GCap and that of the captured frames.
    To modify the MTU, see *D - Procedure to adjust the captured packet size*.
  - Check that the characteristics of the GCap, such as maximum throughput, number of sessions, etc., match those of the network to be monitored.
    For this purpose, consult the GCap data-sheets.
- **Subject 2: optimizing GCap resources**
  - The number of CPUs allocated to the detection engine is too low.
    The CPUs may be overloaded and potentially packets may go unanalysed and therefore dropped.
  - Prefer using a TAP aggregator as opposed to the GCap ”cluster” function.
    The solution with an aggregator TAP is preferable because it is the one that requires the least resources of the identical flow GCap.
- **Subject 3: optimizing the network flow to be analyzed**
  - One or more CPUs are being overloaded because there are too many packets being analyzed.
    - To reduce the size of the captured network, it is possible to suppress the unnecessarily analyzed flow.
    - To manage this packet filtering, see the procedure for defining flow filtering rules.
  - Only one CPU is being overloaded.
    In this case, the flow load is poorly distributed between the CPUs.
    - To change this, it is possible to define a rule or more certainly modify an existing rule.
      A flow was defined but it was too large. It must therefore be subdivided so that each part is analyzed by several CPUs.
    - To modify the rules, see the procedure for defining static packet filtering rules.
  - Change the analyzed protocols.
    - To modify this list, this action must be performed on the paired GCenter.
      Refer to the GCenter documentation.
- **Subject 4: optimizing the detection engine rules**
  The rules define:
  - Detection rules
  - File rebuilding rules
  - Rules defining thresholds or limits under the `threshold` heading
    Refer to the GCenter documentation for more information.
- **Subject 5: monitoring the solution**
  A monitoring service known as Netdata, embedded in the GCenter, enables real time information to be collected on the status of CPUs, load, disks, detection engines, and filtering.
  This feature is available at https://Nom_du_GCenter/gstats.
  On the GCap, Netdata enables more information on protocol counters, number of sessions, flows, and hash table status from ’Stats.log’.

For...	Use the command	carry out the procedures successively
Adjust the captured packet size	*show interfaces* *set advanced-configuration mtu*	1 - *C - Preliminary operations* 2 - *D - Procedure to adjust the captured packet size*
Define flow filtering rules	*show advanced-configuration packet-filtering*	1 - *C - Preliminary operations* 2 - *E - Procedure to define flow filtering rules*

B - Prerequisites

- **User:** setup
- **Commands used in this procedure:**

- *show interfaces*
- *set advanced-configuration mtu*
- *show advanced-configuration packet-filtering*

C - Preliminary operations

1. Connect to the GCap (refer to *Procedure to remote connection to GCap via an SSH tunnel*)
2. Stop the Sigflow detection engine (refer to *monitoring-engine*).

D - Procedure to adjust the captured packet size

This setting enables adjusting the size of the captured packet to match the size of those packets circulating on the network.

Danger:

XDP Filtering features is not supported if the MTU > 3000.

1. Use the *show interfaces* command to display the MTU value in bytes of all enabled network interfaces.
2. Use the *set advanced-configuration mtu* command to change the MTU of a network interface.

E - Procedure to define flow filtering rules

Tip:

The CPU(s) present is overloaded and part of the flow cannot be analyzed, a number of packets is dropped:

- To view the number of dropped packets per CPU core, use the `` `show health` `` command, details of softnet counters - Statistics on received packets based on processor cores.

  Part of the captured flow cannot be detected, nor reconstructed: for example, encrypted flows.

If nothing is done, the system will monopolize resources to achieve a result known in advance.
To avoid this, it is possible to create rules to filter the flow to be captured.

1. Use the *show advanced-configuration packet-filtering* command to display static packet filter rules.

Chapter 9

CLI

9.1 Overview of the CLI

9.1.1 Introduction to the CLI

The Command Line Interface (CLI) is the means used to administer and configure the GCap.
It is therefore necessary to enter commands in text mode following the command prompt.

For the initial GCap configuration and to do advanced configurations or checks, it is necessary to use the CLI.
For most functions, the use of this interface is adequate.
The tables listed in the ../8-procedures/0-list_procedures_menu section enable a general overview of the most common actions.

9.1.2 Overview of the command prompt

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

It includes:

- The status of the Sigflow detection engine (here `Monitoring down`)
- The name of the GCap (here `gcap-name`)
- The level information in the tree :
  - Here (`gcap-cli`): means the command prompt is at the root of the commands
  - For example (`gcap-cli show`): means the command prompt is in the `show` sub-group

---

9.1.3 Accessible commands grouped by sub-group

The commands are grouped by sub-group (show, set, etc.).
The detailed list of commands is provided in the CLI section.

The set...	is used to...
show	display the system configuration
set	modify the system configuration
system	manage system operations

These sets are accessible from the root.

Note:

The set of commands in the GCap CLI is calculated dynamically.
The list of orders depends on:

- du type d'utilisateur courant
- The status of the GCap

This information can be found in the documentation.

Note:

- If a command is entered in the wrong set, or If the access level is not the correct one
- If the access level is not the correct one

... then the command is not recognized and the message *Command 'X* is not recognized' is displayed.

Note:

User type or context elements are specified where necessary.

9.1.4 Directly accessible commands

The commands below are directly accessible:

Use the command...	For...
monitoring-engine	manage the detection engine
pairing	Pair the GCap and GCenter
unpair	Pair the GCap and GCenter
help	obtain help with the available commands
color	enable or disable colors for the current CLI session
exit	return to the root of the CLI or exit the CLI

9.1.5 Completion

To complete the name of a command or an argument, it is possible to use the completion, i.e. :

- Start by entering a command, then
- Use the tab key on the keyboard

The system proposes the possible values.
Example: by asking for a completion on the command below, the system displays the supported values of `set keymap`:

```
set keymap

fr us
```

9.1.6 Navigating in the command tree

9.1.6.1 To go from the root to a set

To access the commands of a set from the root, enter the name of the set.
Example :

```
(gcap-cli)
```

1. Enter the `show`.

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

   The prompt changes to inform the user that the set has changed.
   Now the commands of `show` sub-group are accessible.
   Commands can also be accessed directly from the prompt **(gcap-cli)** by issuing the complete command : for example `show interfaces` for the `interfaces` command of `show` sub-group.

9.1.6.2 To return to the root

To exit the current set and return to the **root**, enter the `exit` command.
Example :

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

Only the commands in the show sub-group are accessible.

1. Use the `exit` command.

```
(gcap-cli)
```

The prompt changes to inform the user that the command prompt is at the root.
At this level, all command sub-groups are accessible.
The **CTRL + D** shortcut enables calling the `exit` command.

9.1.7 Launching a command

A command can be launched in two different ways:

- Either with only the command name but the command prompt must be at the set level
- Or from the root but the name of the set must be entered followed by the name of the command

---

9.1.7.1 Example of launching from the root for the `show interfaces` command

```
(gcap-cli)
```

1. Enter the `show interfaces` command then validate

9.1.7.2 Example of launching the `show interfaces` command from the `show` sub-group

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

1. Enter the `interfaces` command then validate

9.1.8 Obtaining information on commands via Help

To receive help on the available commands, it is possible to use the `?` or `help` command.
To obtain help with a specific command, it is possible to:

- Prefix it with `help` (example `help pairing`)
- Suffix the command with `?` (example `pairing?`)

For more information on assistance, see the paragraph on *help*.

9.1.9 Exit

If the GCap interactive CLI is used, the `exit` command must be used to return to the root of the command tree.
For more information on the `exit` command, see the paragraph *exit*.

9.2 Summary of orders by theme and level

Table 1: Configuring the GCap

Function per level	setup	gviewadm	gview
Display the current keyboard language	*show keymap*	*show keymap*	*show keymap*
Modify the keyboard language.	*set keymap*	*set keymap*	*set keymap*
Display the date and time	*show datetime*	N/A	N/A
Modify the date and time	*set datetime*	N/A	N/A
Enable or disable colors for the current CLI session	*color*	*color*	*color*
Display the compatibility mode with the GCenter	*show compatibility-mode*	N/A	N/A
Modify the compatibility mode with the GCenter	*set compatibility-mode*	N/A	N/A
Pair the GCap with the GCenter	*pairing*	N/A	N/A
Unpair the GCap	*unpair*	N/A	N/A

Table 2: Managing accounts

Function per level	setup	gviewadm	gview
Display the list of users	*show passwords* for all accounts	*show passwords* for gviewadm and gview	*show passwords* only for gview
Modify the passwords	*set passwords* for all accounts	*set passwords* for gviewadm and gview	*set passwords* only for gview
Change the SSH keys	*set ssh-keys* for all accounts	*set ssh-keys* for gviewadm and gview	*set ssh-keys* only for gview
Display the password policy	*show password-policy*	*show password-policy*	*show password-policy*
Unlock blocked accounts	*system unlock* for all accounts	N/A	N/A
Modify the password management policy	*set password-policy* for all accounts	N/A	N/A
Display the protection policy against brute force attacks	*show bruteforce-protection* for all accounts	N/A	N/A
Modify the protection policy against brute force attacks	*set bruteforce-protection* for all accounts	N/A	N/A
Display the duration of inactivity before disconnection	*show session-timeout*	N/A	N/A
Modify the duration of inactivity before disconnection	*set session-timeout*	N/A	N/A

Table 3: Manage the detection engine

Function per level	setup	gviewadm	gview
Display advanced options of the Sigflow configuration	*show monitoring-engine*	N/A	N/A
Apply a Sigflow advanced configuration	*set monitoring-engine*	N/A	N/A
Start the Sigflow detection engine	*monitoring-engine start*	*monitoring-engine start*	N/A
Stop the Sigflow monitor engine	*monitoring-engine stop*	*monitoring-engine stop*	N/A
Display the detection engine status	*monitoring-engine status*	*monitoring-engine status*	N/A
Replay a pcap file of traffic generation	*replay*	*replay*	N/A

Table 4: Manage the network

Function per level	setup	gviewadm	gview
Display the network addressing information of the interfaces	*show network-config*	N/A	N/A
Modify the network interfaces configuration	*set network-config*	N/A	N/A
Display the IP address of the GCenter with which the GCap is paired	*show gcenter-ip*	N/A	N/A
Specify the IP address of the GCenter to which the GCap will be paired	*set gcenter-ip*	N/A	N/A
Display the detailed information of the network interfaces (excluding network addressing)	*show interfaces*	N/A	N/A
Manage the capture interfaces	*set interfaces*	N/A	N/A
Display the MTU value of the network interfaces	*show interfaces*	N/A	N/A
Modify the MTU value of the network interfaces	*set advanced-configuration mtu*	N/A	N/A
Display information on aggregation of capture interfaces	*show interfaces*	N/A	N/A
Configure the aggregation of capture interfaces	*set interfaces*	N/A	N/A

Table 5: Managing server

Function per level	setup	gviewadm	gview
Display help on the commands	*help*	*help*	*help*
Exit the current context	*exit*	*exit*	*exit*
Leave the SSH session	*exit*	N/A	N/A
Shut down the GCap	*system shutdown*	N/A	N/A
Restart the GCap	*system restart*	N/A	N/A

Table 6: Monitoring the GCAP

Function per level	setup	gviewadm	gview
Display the current status of the GCap	*show status*	*show status*	*show status*
Display the statistics of the Sigflow detection engine	*show eve-stats*	*show eve-stats*	*show eve-stats*
Display statistics and health information	*show health*	*show health*	N/A
Extract the information from the GCap as requested by technical support	*show tech-support*	N/A	N/A

9.3 CLI commands

9.3.1 show

9.3.1.1 show bruteforce-protection

A - Introduction

The `bruteforce-protection` command in `show` sub-group enables displaying the system policy for protecting against brute force attacks.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`show bruteforce-protection`

D - Procedure to show the current system policy for protecting against brute force attacks

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show bruteforce-protection
   ```

2. Validate

   The system displays the following information

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

   User accounts are automatically locked for a set period of time (parameter `Lock duration`) after several unsuccessful attempts (parameter `Max tries`).

9.3.1.2 show compatibility-mode

A - Introduction

The `compatibility-mode` command of the `show` sub-group enables displaying the current compatibility mode to interact with GCenter.
The compatibility mode will affect the available functionality of GCap.
Several compatibility modes are available:

- 2.5.3.102 : GCenter 2.5.3.102
- 2.5.3.103 : GCenter 2.5.3.103

The current mode must be selected based on the current GCap and GCenter versions.
For more information, please refer to the table *set compatibility-mode*.

Note:

The compatibility mode for GCenter version 2.5.3.101 and below is deprecated.

B - Prerequisites

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

---

C - Command

`show compatibility-mode`

D - Procedure to display the current compatibility mode

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show compatibility-mode
   ```

2. Validate
   The system displays the current compatibility mode

   ```
   Current compatibility mode: 2.5.3.102
   ```

9.3.1.3 show datetime

A - Introduction

The `datetime` command of the `show` sub-group enables displaying the date and time of the GCap in the format `YYYY-MM-DD HH:MM:SS`.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`show datetime`

D - Procedure to display the date and time of the GCap

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show datetime
   ```

2. Validate
   The system displays the current information

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

9.3.1.4 show eve-stats

A - Introduction

The `eve-stats` command in the `show` sub-group enables displaying the Sigflow (*monitoring-engine*) statistics.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`show eve-stats`

D - Procedure

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show eve-stats
   ```

2. Validate
   The system displays the following information

- counter `Alerts` - Number of Sigflow alerts found
- counters `Files` - Files extracted by Sigflow
- Counters `Codebreaker samples` - Files analyzed by Codebreaker
- Counters `Protocols` - List of protocols seen by Sigflow
- Counters `Detection Engine Stats` - Sigflow statistics (*monitoring-engine*)

E - Details of Counter `Alerts` - Number of Sigflow alerts found

Example :

```
Alerts: 0
```

F - Detail of counters `Files` - Files extracted by Sigflow

- `Observed` - Number of files observed by Sigflow.
- `Extracted` - Number of files extracted by Sigflow.
- `Uploaded` - Data sent to GCenter.
  - `Metadata` - Number of metadata sent to GCenter.
  - `File` - Number of files sent to GCenter.

Example :

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

G - `Codebreaker samples` counter details - Files analysed by Codebreaker

- `Extracted` - Number of extracted files received by Codebreaker.
- `Uploaded` - Data on files received by Codebreaker on GCenter.
  - `Shellcodes` - Data on *shellcodes*.
    - `Plain` - *Shellcodes* detected without encoding.
    - `Encoded` - *Shellcodes* detected with encoding.
  - `Powershell`- Number of malicious *Powershell* scripts detected.

Example :

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

Note:

In version GCenter V102, this engine is called Codebreaker
In version GCenter V103, the engine which detects the shellcodes is called **Shellcode detect engine**
In version GCenter V103, the engine which detects the malicious powershells is called **Malicious Powershell detect engine**.

H - Details of the `Protocols` counters - Lists of protocols seen by Sigflow

- `<protocole>` Number of events observed by Sigflow concerning protocol e.g *HTTP*, *SMB*, and others.
  Example :

```
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:   0source/gcap-cli/6-3-show/eve-stats.rst:97: (WARNING/2) Literal block expected; none found.
```

I - Details of the `Detection Engine Stats` counters - Statistics of Sigflow (*monitoring-engine*)

- `Events` - Data on events observed by Sigflow
  - `Total` - Total number of events
  - `Stats` - Number of statistics generated
- `Capture`
  - `Received` - Number of packets captured
  - `Dropped` - Number of packets ignored
- `Rules` - Sigflow rules data
  - `Loaded` -Number of rules loaded and validated
  - `Invalid` - Number of rules that could not be loaded
- `TCP`
  - `SYN` - Number of SYN observed by Sigflow.
  - `SYN/ACK` - Number of SYN/ACK observed by Sigflow.
  - `Sessions` - Number of *TCP* sessions observed by Sigflow.
- `Flow`
  - `TCP` - Number of TCP sessions observed
  - `UDP` - Number of UDP sessions observed
  - `SCTP` - Number of *SCTP* sessions observed
  - `ICMPv4` - Number of *ICMPv4* messages observed
  - `ICMPv6` - Number of *ICMPv6* messages observed
  - `Timeouts` - Statistics on *TCP* session expirations
    - `New` - Number of new windows *TCP*
    - `Established` - Number of windows established
    - `Closed` - Number of windows closed
    - `Bypassed` - Number of windows ignored

Exemple

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

  Capture:
    Received:   153439718
    Dropped:    60964966

  Rules:
    Loaded:     78
    Invalid:    28

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

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

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

Note:

The TCP sessions counter counts the number of sessions once the connection is established (three-way handshake phase).
The TCP Flows counter counts the number of sessions that have been started (including sessions where the connection is in progress).

9.3.1.5 show gcenter-ip

A - Introduction

The `gcenter-ip` command of the `show` sub-group enables displaying the IP address of the GCenter with which the GCap is paired.

B - Prerequisites

- **User:** setup
- **Dépendances :**
  - the detection engine must be switched off
  - A GCenter must be paired

C - Command

`show gcenter-ip`

D - Exemple

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show gcenter-ip
   ```

2. Validate
   The system displays the IP address of the paired GCenter

   ```
   Current GCenter IP:
   ```

   If there is no paired Gcenter then the following message is displayed :

   ```
   Current GCenter IP: None
   ```

9.3.1.6 show health

A - Introduction

The `health` command of the `show` sub-group enables displaying statistics and the health information of the GCap.

B - Prerequisites

- **User:** setup, gviewadm
- **Dependencies:** N/A

C - Command

`show health`

D - Procedure

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show health
   ```

2. Validate
   The system displays the following information

- `block` counters - Mass storage statistics
- `cpu_stats` counters - Processor statistics
- `disks` counters - Mount point occupancy statistics
- `emergency` counters - GCap emergency mode information
- `gcenter` counters - Paired GCenter information
- `high_availability` counters - High Availability (HA) information
- `interfaces` counters - Statistics on network interfaces
- `loadavg` counters - Statistics on the average load of the GCap
- `meminfo` counters - Statistics on the RAM
- `numastat` counters - Non Uniform Memory Access (NUMA) node
- `quotas` counters - Quota Information
- `sofnet` counters – Statistics on received packets according to processor cores
- `suricata` counters - Sigflow (*monitoring-engine*) information
- `systemd` counters - System initialization information
- `uptime` counters - Uptime
- `virtualmemory` counters - Swap space information (*swap*)

E - Details of `block` counters - Mass storage statistics

- `sdN` - Disk statistics N where N is a letter of the alphabet
  - `read_bytes` - Bytes read since startup
  - `written_bytes` - Bytes written since startup

Example :


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

F - Details of `cpu_stats` counter - CPU statistics

- `cpus` - CPU usage statistics
  - `cpu` - Overall core usage statistics
  - **`cpuX` - CPU X core statistics**
    - `idle` - Elapsed time doing nothing in milliseconds
    - `iowait` - Elapsed time waiting for disk operations in milliseconds
    - `irq` - Elapsed time on material IRQs
    - `nice` - Time elapsed in user space on low priority processes in milliseconds
    - `softirq` - Elapsed time on hardware IRQs in milliseconds
    - `system` - Elapsed time in kernel space in milliseconds
    - `user` - Elapsed time in user space in milliseconds
    - `interrupts` - Number of interrupts since startup
    - `processes_blocked` - Number of blocked or *dead* processes
    - `processes_running` - Number of running processes

Example :


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


G- Details of `disks` counters - Mount point occupancy statistics

- `/mountpoint/path` - Mount point path
  - `block_free` - Number of free *blocks*
  - `block_total` - Total number of *blocks*
  - `inode_free` - Number of remaining inodes
  - `inode_total` - Total number of *inodes*

Example :


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


(continues on next page)

(continued from previous page)

```
        "inode_total": 1827840
    },
}
```

H - Details of `emergency` counters - GCap emergency mode information

- `emergency_active` - Active or inactive status of the **emergency mode**

Example :

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

I - Details of `GCenter` counters - Paired GCenter information

- `chronyc_sync` - Status of the NTP synchronization with the GCenter
- `Reachable` - GCenter reachable (true) or not (false)

Example :

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

J - Details of `high_availability` counters - High Availability (*HA*) information

This feature is deprecated.
These counters are not significant.

- `healthy` - *HA* health status
- `last_status` - Last known *HA* status
- `last_transition` - Date of last known *HA* status change in *ISO8601* format
- `leader` - True for a GCap leader, false for a GCap *follower*
- `Status` - Active or inactive (false) status of the *HA*

Example :

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

K - Details of `interfaces` counters - Statistics on network interfaces

- `mon0`: network interface name
  - `rx_bytes` - Number of bytes received
  - `rx_drop` - Number of bytes lost in reception
  - `rx_errs` - Number of invalid bytes received
  - `rx_packets` - Total number of packets received from this interface
  - `tx_bytes` - Number of bytes sent
  - `tx_drop` - Number of bytes lost while sending
  - `tx_errs` - Number of invalid bytes sent
  - `tx_packets` - Total number of packets sent from this interface

Example :

```
"interfaces": {
    "mon0": {
        "rx_bytes": 0,
        "rx_drops": 0,
        "rx_errs": 0,
        "rx_packets": 0,
        "tx_bytes": 0,
```

(continues on next page)

(continued from previous page)


```
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    },
    "tunnel": {
        "rx_bytes": 138433006,
        "rx_drops": 82901,
        "rx_errs": 0,
        "rx_packets": 2143236,
        "tx_bytes": 796294,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 3635
    },
    "management": {
        "rx_bytes": 137642525,
        "rx_drops": 82902,
        "rx_errs": 0,
        "rx_packets": 2135060,
        "tx_bytes": 0,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    }
}
```


Note:

Here the interfaces are named with the labels (`mon0`, `tunnel`, `management`).
Reminder: in role management-tunnel, the interface displayed is called `management`.

L - Details of `loadavg` counters - Statistics on the average load of the GCap

- `active_processes` - Number of processes started
- `load_average_15_mins` - Average load over the last fifteen minutes
- `load_average_1_min` - Average load over the last minute
- `load_average_5_mins` - Average load over the last five minutes
- `running_processes` - Number of running processes

Example :


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

M - Details of `meminfo` counters - Statistics on the RAM

- `available` - Total physical memory in kilo-Bytes
- `buffers` - Memory used by disk operations in kilo-Bytes
- `cached` - Memory used by the cache in kilo-Bytes
- `dirty` - Memory used by pending write operations in kilo-Bytes
- `free` - Unused memory in kilo-Bytes
- `hugepages_anonymous` - Number of anonymous transparent huge pages used
- `hugepages_free` - Number of available transparent huge pages
- `hugepages_reserved` - Number of reserved transparent huge pages
- `hugepages_shmem` - Number of shared transparent huge pages
- `hugepages_surplus` - Number of extra transparent huge pages
- `hugepages_total` - Total number of huge pages
- `kernel_stack` - Memory used by kernel stack allocations in kilo-Bytes
- `page_tables` - Memory used for page management in kilo-Bytes
- `s_reclaimable` - Cache memory that can be reallocated in case of memory shortage in kilo-Bytes
- `Shmem` - Memory used by shared pages in kilo-Bytes
- `slab` - Memory used by kernel data structures in kilo-Bytes
- `swap_cached` - Memory used by the swap cache in kilo-Bytes
- `swap_free` - Available memory in swap in kilo-Bytes

- `swap_total` - Total swap memory in kilo-Bytes.
- `Total` - Total memory in kilo-Bytes
- `v_malloc_used` - Memory used by large memory areas allocated by the kernel
  For more information, please refer to this documentation‘meminfo
  <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s2-proc-meminfo.html>‘_

  Example :


```
"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
},
```

N - Details of `numastat` counters - Non Uniform Memory Access (NUMA) node

- `nodes` - List of NUMA nodes
  - `nodeX` - NUMA X node statistics
    - `interleave_hit` - Interleaved memory successfully allocated in this node
    - `local_node` - Memory allocated in this node while a process was running on it
    - `numa_foreign` - Memory planned for this node, but currently allocated in a different node
    - `numa_hit` - Memory successfully allocated in this node as expected
    - `numa_miss` - Memory allocated in this node despite process preferences.
      Each numa_miss has a numa_foreign in another node
    - `other_node` - Memory allocated in this node while a process was running in another node

Example :


```
"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
        }
    }
},
```

O - Details of `quotas` counters - Quota statistics by category

- `quotas` - Quota list
  - `by_gid` - Statistics sorted by group (gid identifier)
  - `by_prj` - Statistics sorted by project (prj identifier)
  - `by_uid` - Statistics sorted by user (uid identifier)

In each category, the following counters are displayed:

- `block_grace` - Grace time for blocks
- `block_hard_limit` - Hardware limit of blocks.
  Sets an absolute limit for the use of space.
  The user cannot exceed this limit.
  Beyond this limit, writing to this file system is forbidden.
- `block_soft_limit` - Software block limit
  Specifies the maximum amount of space a user can occupy on the file system.
  If this limit is reached, the user receives warning messages that the quota assigned to them has been exceeded.
  If its use is combined with the timeframes (or grace period), when the user continues to exceed the software limit after the grace period has elapsed, then he finds himself in the same situation as in the reaching of a hard limit.
- `block_used` - Number of blocks used
- `file_grace` - Grace time for files
- `file_hard_limit` - Hardware file limit
  Sets an absolute limit for the use of space.
  The user cannot exceed this limit.
  Beyond this limit, writing to this file system is forbidden.
- `file_soft_limit` - Software file limit
  Specifies the maximum amount of space a user can occupy on the file system.
  If this limit is reached, the user receives warning messages that the quota assigned to them has been exceeded.
  If its use is combined with the timeframes (or grace period), when the user continues to exceed the software limit after the grace period has elapsed, then he finds himself in the same situation as in the reaching of a hard limit.
- `file_used` - Number of files used

Example :


```
"quotas": {
    "by_gid": {
        "0": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "2148952",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "177"
        },
        "10012": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "5216",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "295"
        },
        }
    },
    "by_prj": {
        "0": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "51600",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "225"
        },
        "1": {
            "block_grace": "0",
            "block_hard_limit": "7980499",
            "block_soft_limit": "7980499",
            "block_used": "2101904",
            "file_grace": "0",
```


(continues on next page)

(continued from previous page)


```
            "file_hard_limit": "1000",
            "file_soft_limit": "1000",
            "file_used": "43"
        },
        }
    },
    "by_uid": {
        "0": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "2153356",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "269"
        },
        "10012": {
            "block_grace": "0",
            "block_hard_limit": "0",
            "block_soft_limit": "0",
            "block_used": "1032",
            "file_grace": "0",
            "file_hard_limit": "0",
            "file_soft_limit": "0",
            "file_used": "258"
        },
    }
}
```


Example below is without defined limit: the value ”0” indicates that there is no defined value for limits and grace times.


```
"10012": {
    "block_grace": "0",
    "block_hard_limit": "0",
    "block_soft_limit": "0",
    "block_used": "1032",
    "file_grace": "0",
    "file_hard_limit": "0",
    "file_soft_limit": "0",
    "file_used": "258"
},
```


P - Details of `sofnet` counters – Statistics on received packets according to processor cores

- `cpus` - Usage statistics per CPU
  - `CpuX` - CPU X core statistics
    - `backlog_len` -
    - `dropped` - Number of packets dropped
    - `flow_limit_count` - Number of times the throughput limit was reached
    - `processed` - Number of packets processed
    - `received_rps` - Number of times the CPU was woken up
    - `time_squeeze` - Number of times the thread could not process all the packets in its backlog within the allocated budget
  - `summed` - Overall core usage statistics
    - `backlog_len` -
    - `dropped` - Number of packets dropped
    - `flow_limit_count` - Number of times the throughput limit was reached
    - `processed` - Number of packets processed
    - `received_rps` - Number of times the CPU was woken up
    - `time_squeeze` - Number of times the thread could not process all the packets in its backlog within the allocated budget

Example :


```
"softnet": {
    "cpus": {
        "cpu0": {
```


(continues on next page)

(continued from previous page)


```
            "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
    }
},
```

Q - Details of `Sigflow` counters - Sigflow (*monitoring-engine*) information

`detailed_status` - Sigflow container status

- `up` - Status of Sigflow and the detection engine

detailed_status + status `up`	signification
status `Container down` + `up` false	status engine off
status `Container down` + `up` true	impossible status: device cannot be rotated in a disabled container
status `Container UP` + `up` false	unstable status: call GATEWATCHER support
status `Container UP` + `up` true	status engine on

Example :


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

R - Details of `systemd` counters - System initialization information

- `failed_services` - List of failed services reported by `systemctl failed`.

Example :


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

S - Details of `uptime` counters - Uptime

- `up_seconds` - Number of seconds since startup.

Example :


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

T - Details of `virtualmemory` counters - Swap space information (*swap*)

- `disk_in` - Number of pages saved to disk since startup.
- `disk_out` - Number of pages out of disk since startup.
- `pagefaults_major` - Number of page faults per second.
- `pagefaults_minor` - Number of page faults per second to load a memory page from disk to RAM.
- `swap_in` - Number of kilo-Bytes the system swapped from disk to RAM per second.
- `swap_out` - Number of kilo-Bytes the system swapped from RAM to disk per second.

  Example :

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

9.3.1.7 show interfaces

A - Introduction

The `interfaces` command of the `show` sub-group enables displaying the GCap network interfaces:

- The management and tunnel interfaces
- The capture interfaces available physically `mon0` to `monx` or virtually `monvirt`

This command can take the keyword `delay` as a parameter to display the grace period granted to the interfaces.
The following information is available with the `show interfaces` command:

- `Label`: The label name of the interface, `monX` for capture interfaces, `tunnel` for IPSec connections, `management` for SSH connections or SSH and IPSec connections if the interface role is `management-tunnel`, `clusterX` for interfaces in cluster mode.
- `Name`: the system name of the interface
- `Role`: The role assigned to the interface, `capture` for capture interfaces,“‘tunnel“‘ for IPSec connections, `management` for SSH connections, `management-tunnel` for SSH and IPSec connections, `capture-cluster` for capture interfaces in cluster mode, `inactive` for deactivated interfaces.
- `Capture capability`: if the interface can capture traffic
- `MTU`: the MTU of the interface
- `Physical Address`: the MAC address of the interface
- `Speed`: the interface speed
- `Type`: the type of cable/sfp connected to the physical port
- `Vendor ID`: the Vendor ID of the network card
- `Device ID`: the ID of the network card
- `PCI bus`: PCI bus number used by the network card

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`show interfaces{ |delay|}`

D - Procedure to display the available network interfaces

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show interfaces
   ```

2. Validate

   The system displays the available capture interfaces

```
(gcap-cli) show interfaces

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

Note:

All existing interfaces are displayed, even those making up an aggregation of interfaces.

E - Procedure to display the grace period given to start up the interfaces

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show interfaces delay
   ```

2. Validate

   The system displays the grace period for starting up the interfaces

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

9.3.1.8 show keymap

A - Introduction

The `keymap` command of the `show` sub-group enables displaying the keyboard layout between azerty (choice fr) and qwerty (choice en) used on physical interfaces (KVM, iDRAC, physical).

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`show keymap`

D - Procedure to display the current keyboard language

The command prompt is displayed.

```
(gcap-cli)
```

```
show keymap
```

1. Validate
   The system displays the current information
   Example :

```
Current keymap is fr
```

9.3.1.9 show monitoring-engine

A - Introduction

The `monitoring-engine` command of the `show` sub-group enables displaying the advanced options of the GCap detection engine configuration:

- The start-timeout grace period
- The grace period when the engine is stopped (stop-timeout)
- The status of the sanity checks

B - Prerequisites

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

---

C - Command

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

D - Procedure to display the default value of the start-timeout

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show monitoring-engine start-timeout
   ```

2. Validate
   The system displays the current value

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

E - Procedure to display the default value of the stop-timeout

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show monitoring-engine stop-timeout
   ```

2. Validate
   The system displays the current value

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

F - Procedure to display the status of the verification check

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show monitoring-engine sanity-checks
   ```

2. Validate
   The system displays the current value

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

   The system reports that the control system is active.
   The detection engine will only start after it verifies that at least one `monx` capture interface is activated and a cable is connected.

9.3.1.10 show network-config

A - Introduction

The GCap includes:

- the capture interfaces
- Network interfaces for managing the probe via SSH and for pairing with the GCenter

Two cases are possible:

- The **single interface configuration**
  SSH connection for GCap management and VPN communication are managed through the interface tunnel- management.
- **dual-interface configuration**
  The VPN communication for the connection with the GCenter is managed by the tunnel interface.
  The SSH connection for GCap management is handled by another management interface.

For more information on network interfaces, refer to *Description of the GCap inputs / outputs* section.
The `network-config` command of the `show` sub-group enables displaying:

- The status of all GCap interfaces: `show network-config configuration` command
- The status for each interface: `show network-config tunnel` or `show network-config management` command
- The domain name: `show network-config domain` command
- The host name: `show network-config hostname` command

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`show network-config {configuration|tunnel|management|hostname|domain}`

D - Procedure to display the GCap configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show network-config configuration
   ```

2. Validate
   Depending on the single or dual interface configuration, the information is different
   The two cases are listed below
   Example of single-interface configuration

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

(continues on next page)

(continued from previous page)


```
   "enp27s0": {
      "filtering_rules": {},
      "mtu": 1500
   },
   "monvirt": {
      "filtering_rules": {},
      "mtu": 1500
   }
}
```


The `ip_address` values of the `tunnel` and `management` interfaces are identical.

Example of dual-interface configuration


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


The `ip_address` values of the `tunnel` and `management` interfaces are different.

E - Procedure to display the GCap domain name

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show network-config domain
   ```

2. Validate

   The system displays the domain name

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

F - Procedure to display the `management` interface configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show network-config management
   ```

2. Validate

The system displays the `management` interface configuration
For example:

```
Interface management configuration
 - IP Address:
 - Mask:
 - Gateway:
```

I - Procedure to display the `tunnel` interface configuration

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show network-config tunnel
   ```

2. Validate
   The system displaying the `tunnel` interface configuration
   For example:

   ```
   Interface tunnel configuration
    - IP Address:
    - Mask:
    - Gateway:
   ```

J - Procedure to display the GCap hostname

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show network-config hostname
   ```

2. Validate
   The system displays the interface the host name of the GCap

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

9.3.1.11 show password-policy

A - Introduction

The `password-policy` command in `show` sub-group enables displaying the password policy for the accounts `setup`, `gviewadm` and `gview`.
The possibility of modifying this policy is enabled by the *set password-policy* command.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`show password-policy`

D - Procedure to display the default password policy

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show password-policy
   ```

2. Validate
   The system displays the rules to be followed for defining a password

```
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
```

Parameter...	Signification...
Minimum different characters between old and new passwords : x	It takes at least x different characters for a password to be considered different
Minimum length	minimum password length: here 12 characters
Lowercase character required:	yes: means that the password must contain at least 1 lower case letter
Uppercase character required:	yes: means that the password must contain at least 1 capital letter
Digits required:	yes: means that the password must contain at least 1 digit 0 to 9
Symbols required:	yes: means that the password must contain at least 1 symbol, not a number or a letter

9.3.1.12 show passwords

A - Introduction

The `passwords` command of the `show` sub-group enables:

- to display the list of users managed by the current level, accessible for setup, gviewadm, gview users
- to retrieve the root token in the form of a text or QR code, accessible for **setup** user only.

Note:

The "retrieve root token" feature must be used in consultation with GATEWATCHER customer support.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`show passwords {list|text|qrcode}`

D - Procedure to display the list of users managed by the current level

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show passwords list
   ```

2. Validate
   The system displays the list of users managed by the current level
   - Example for the gview level:

     ```
     Allowed users: gview
     ```

   - Example for the setup level:

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

E - Procedure to display the root token in text

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show passwords root text
   ```

2. Validate
   The system displays the root token in text

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

F - Procedure to display the root token as a QR code

The command prompt is displayed.

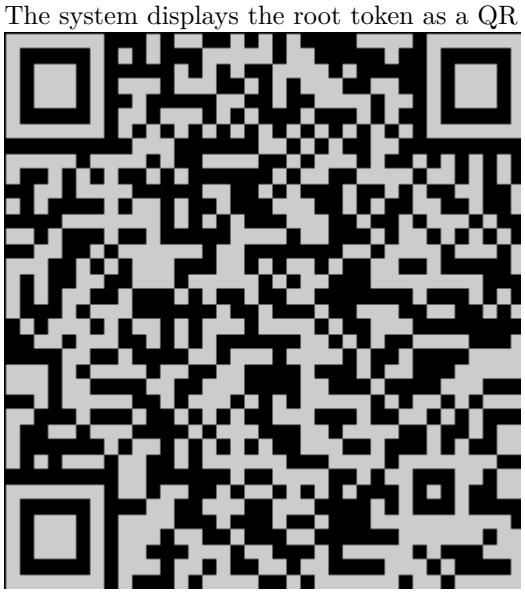
```
(gcap-cli)
```

1. Enter the command

   ```
   show passwords root qrcode
   ```

2. Validate

The system displays the root token as a QR code



9.3.1.13 show session-timeout

A - Introduction

The `session-timeout` command of the `show` sub-group enables displaying the time of inactivity before logging out of a user session.
This figure is expressed in minutes and the default value is 5 minutes.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`show session-timeout`

D - Procedure to display the session-timeout value

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show session-timeout
   ```

2. Validate
   The system displays the current session-timeout value
   For example:

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

9.3.1.14 show status

A - Introduction

The `status` command of the `show` sub-group enables displaying the current GCap status.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`show status`

D - Procedure to display the GCap information

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   show status
   ```

2. Validate
   For example:

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

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

     © Copyright GATEWATCHER ...
   ```

   The system displays the following information

- `GCAP FQDN`: Fully Qualified Domain Name of the GCap, here `gcap.gatewatcher.com`.
- `Version`: current software version, here `2.5.4.0`.
- `Overall status` : current global status of the GCap, here `Running`.
- `Tunnel`: status of the tunnel between GCap and GCenter, here `up`.
- `Detection Engine`: status of the detection engine container, here not started `Up and running`.
- `Configuration`: status of the configuration, here `Complete`.
- `Gcap name` hostname of the GCap, here `gcap`.
- `Domain name`: Domain name of the GCap, here `gatewatcher.com`.
- `Tunnel interface`: IP address of the tunnel interface, here `192.168.2.2`.
- `Management interface` : IP address of the management interface, here `192.168.1.2`.
- `Gcenter version`: version of the remote GCenter, here `2.5.3.103`.
- `Gcenter IP`: IP address of the remote GCenter, `192.168.2.3`.
- `Paired on Gcenter`: Status of the pairing with GCenter, `Yes`.
- `Monitoring interfaces` : enabled capture interfaces, here `mon0, mon2, mon4, monvirt`.

9.3.1.15 show tech-support

A - Introduction

The `tech-support` command of the `show` sub-group enables extracting the GCap information requested by technical support.

Note:

Tech-support is not encrypted and may contain confidential information.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

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

Note:

GCapX should be replaced with the IP address of GCap.

D - Command to extract light tech-support

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

E - Command to extract standard tech-support

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

F - Command to extract heavy tech-support

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

9.3.1.16 show advanced-configuration packet-filtering

A - Introduction

The `packet-filtering` command of the `show advanced-configuration` sub-group enables displaying the static packet filtering rules.

Note:

Packet filtering is not supported when the MTU > 3000.

B - Prerequisites

- **User:** setup
- **Dépendances :**
  - the detection engine must be switched off
  - A network capture interface must be enabled

C - Command

`show advanced-configuration packet-filtering`

D - Procedure to display the flow filtering rules

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

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

2. Validate
   The system displays the result

```
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
```

9.3.2 set

9.3.2.1 set bruteforce-protection

A - Introduction

The `bruteforce-protection` command of the `set` sub-group enables the system to protect against brute force attacks when a user logs in. User accounts are automatically locked for a set period of time after several unsuccessful attempts.
The default value is 3.
To view the current values for the number of attempts and the account lockout duration, use the *show bruteforce-protection* command.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

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

D - Command used to set a maximum number of authentication attempts for an account (0 to deactivate)

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

E - Command used to set an account lockout duration in seconds (0 to deactivate)

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

F - Command to restore the default configuration

`set bruteforce-protection restore-default`

G - Procedure to change the lockout duration to 360 seconds

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set bruteforce-protection lock-duration 360
   ```

2. Validate
   The system indicates the setting has been changed

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

9.3.2.2 set compatibility-mode

A - Introduction

The `compatibility-mode` command of the `set` sub-group enables modifying the compatibility mode used to interact with GCenter.
The compatibility mode will affect the available functionality of GCap.

Several compatibility modes are available:

- 2.5.3.102 : GCenter 2.5.3.102
- 2.5.3.103 : GCenter 2.5.3.103

For a GCap	Version GCenter	supported	Action or Command to be executed
2.5.4.1	2.5.3.101 HF4	unsupported	GCenter to migrate to a newer version
2.5.4.1	2.5.3.102 HF3	supported	set compatibility-mode 2.5.3.102
2.5.4.1	2.5.3.103	supported	set compatibility-mode 2.5.3.103

Important:

The above table is given as an example. Please refer to the GCap Release Note.

Note:

The compatibility mode for GCenter version 2.5.3.101 and below is deprecated.

B - Prerequisites

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

---

C - Command

`set compatibility-mode {2.5.3.102|2.5.3.103}`

D - Procedure to configure the compatibility between a GCap version V2.5.4.0 with a GCenter 2.5.3.102

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set compatibility-mode 2.5.3.102
   ```

2. Validate

9.3.2.3 set datetime

A - Introduction

The `datetime` command of the `set` sub-group enables the date and time of the GCap to be adjusted.
This enables avoiding clock problems that could lead to the impossibility of establishing an IPSec tunnel with GCenter.

Note:

This clock must always be adjusted so that the GCap and the associated GCenter are on the same time (e.g. for the timestamping of events).

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

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

D - Procedure to change the GCap date and time

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set datetime 2022-01-26T16:00:00Z
   ```

2. Validate
   The system displays the result

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

9.3.2.4 set gcenter-ip

A - Introduction

The `gcenter-ip` command of the `set` sub-group enables specifying the IP address of the GCenter to which the GCap will be paired.

Note:

The GCap uses this IP address during pairing to connect to the GCenter via SSH and retrieve the GCenter fingerprint.

B - Prerequisites

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

---

C - Command

`set gcenter-ip {GCenter-IP}`

D - Procedure

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set gcenter-ip 192.168.1.1
   ```

2. Validate
   The system displays the result

   ```
   Setting GCenter IP to 192.168.1.1
   ```

9.3.2.5 set interfaces

A - Introduction

The `interfaces` command of the `set` sub-group allows assigning roles to capture interfaces.
Interfaces can be physical or virtual.

Note:

The management of network parameters is done by the show network-config / set network-config commands

---

B - Prerequisites

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

---

C - Command

To change the delay before starting up the interfaces: `set interfaces delay SECOND`
To assign a specific role to an interface `set interfaces assign-role {management|tunnel|management-tunnel|capture|capture-cluster|inactive}`

- **Role**: the role assigned to the interface are the following:
  - **capture** for capture interfaces
  - **tunnel** for IPSec connections
  - **management** for SSH connections
  - **management-tunnel** for SSH and IPSec connections
  - **capture-cluster** for capture interfaces in cluster mode
  - **inactive** for disable interfaces

D - Procedure to change the interface startup delay by five seconds

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set interfaces delay 5
   ```

2. Validate

F - Procedure to assign a capture role to interface specific interface

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set interfaces assign-role enp4s0 capture
   ```

2. Validate

Note:

If the system displays the following message, *Failed to assign role: network configuration cannot be changed now*, check if the monitoring-engine is up.

9.3.2.6 set keymap

A - Introduction

The `keymap` command of the `set` sub-group enables choosing the keyboard layout between azerty (choice fr) and qwerty (choice en) used on physical interfaces (KVM, iDRAC, physical).

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`set keymap {fr|en}`

D - Procedure to change the keyboard language to French

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set keymap fr
   ```

2. Validate
   The system displays the result

   ```
   Setting keymap to fr
   ```

E - Procedure to change the keyboard language to English us

1. Enter the command

   ```
   set keymap en
   ```

2. Validate
   The system displays the result

   ```
   Setting keymap to en
   ```

9.3.2.7 set monitoring-engine

A - Introduction

The `monitoring-engine` command of the `set` sub-group enables applying an advanced configuration for the GCap sensor detection engine.

Note:

If the number of signatures loaded by Sigflow is too large, the timeout value must be adjusted.

B - Prerequisites

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

---

C - Command

To change the grace period when starting the engine: `set monitoring-engine start-timeout SECOND`.
To change the grace period when the engine is stopped: `set monitoring-engine stop-timeout SECOND`.
To enable or disable the check of the controls: `set monitoring-engine {disable-sanity-checks|enable-sanity-checks}`.
If the `sanity-checks` option is set to `enable`, the detection engine starts only after verifying that at least one `monx` capture interface has been activated and that a cable is connected.

D - Procedure to change the grace period to 600 seconds when starting the engine

The command prompt is displayed.

```
(gcap-cli)
```

1. To change the grace period to 600 seconds when starting the engine:
    1. Enter the command
    ```
    set monitoring-engine start-timeout 600
    ```
    2. Validate
2. To check the value modification:
    1. Enter the command
    ```
    show monitoring-engine start-timeout
    ```
    2. Validate
    The system displays the current value
    ```
    Monitoring Engine Options:
    start timeout: 600s
    ```

E - Procedure to modify the grace period to 600 seconds when starting the engine

The command prompt is displayed.

```
(gcap-cli)
```

1. To change the grace period to 600 seconds when stopping the engine:
    1. Enter the command
    ```
    set monitoring-engine stop-timeout 600
    ```
    2. Validate
2. To check the value modification:
    1. Enter the command
    ```
    show monitoring-engine stop-timeout
    ```
    2. Validate
    The system displays the current value
    ```
    Monitoring Engine Options:
    Stop timeout: 600s
    ```

E - Procedure to disable the capture interface verification

The command prompt is displayed.

```
(gcap-cli)
```

1. To disable the capture interface verification:
   1. Enter the command

      ```
      set monitoring-engine disable-sanity-checks
      ```

   2. Validate
2. To check the value modification:
   1. Enter the command

      ```
      show monitoring-engine sanity-checks
      ```

   2. Validate

      The system displays the current value

      ```
      Monitoring Engine Options:
      Sanity checks disabled
      ```

E - Procedure to enable the capture interface verification

The command prompt is displayed.

```
(gcap-cli)
```

1. To enable the capture interface verification:
   1. Enter the command

      ```
      set monitoring-engine enable-sanity-checks
      ```

   2. Validate
2. To check the value modification:
   1. Enter the command

      ```
      show monitoring-engine sanity-checks
      ```

   2. Validate

      The system displays the current value

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

9.3.2.8 set network-config

A - Introduction

The `network-config` command of the `set` sub-group enables modifying the network configuration of the GCap management and tunnel interfaces.
The `network-config` command of the `set` sub-group enables configuring:

- Each interface with the network parameters: `set network-config {management|tunnel}} [ip-address IP_value] [gateway GATEWAY_value] [mask MASK_value]` command
- The domain name: `set network-config domain NAME_value` command
- The host name: `set network-config hostname HOSTNAME_value` command

For more information on the network interfaces (management, tunnel) and the capture interfaces (`mon0` to `monx`), refer to the *show network-config* command.

B - Prerequisites

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

---

C - Command

`set network-config {management|tunnel} [ip-address IP_value] [gateway GATEWAY_value] [mask MASK_value] [confirm] [no-reload]` `set network-config [domain-name NAME_value|hostname HOSTNAME_value] [confirm]`

Note:

The *no-reload* option enables not reloading network services.

D - Procedure to configure the `management` interface and the `tunnel` interface

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set network-config tunnel ip-address x.y.z.w gateway Z.Z.Z.Z mask Z.Z.Z.Z
   ```
2. Validate
3. Enter the command

   ```
   set network-config management ip-address x.y.z.w gateway Z.Z.Z.Z mask Z.Z.Z.Z confirm
   ```
4. Validate

E - Procedure to modify the GCap domain name

The command prompt is displayed.

```
(gcap-cli)
```

1. To change the GCap domain in gatewatcher.com:
   1. Enter the command

      ```
      set network-config domain-name gatewatcher.com
      ```
   2. Validate

      ```
      Setting hostname/domain name to:
         - Hostname: gcap-int-129-dag
         - Domain name: gatewatcher.com
      Do you want to apply this new configuration? (y/N)
      ```
   3. Press <y> and then confirm
2. To check the value modification:
   1. Enter the following command

```
show network-config domain
```

2. Validate

   The system displays the domain name

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

9.3.2.9 set password-policy

A - Introduction

The `password-policy` command in `set` sub-group enables defining a password policy for the `setup`, `gviewadm` and `gview` accounts. This policy applies to all users.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

To set the password complexity options: `set password-policy {lowercase-optional|lowercase-required|uppercase-optional|uppercase-required|digits-optional|digits-required|symbols-optional|sym`
To enable or disable the password control policy: `set password-policy {disable|enable}`
To restore the default password control policy: `set password-policy restore-default`
To set the minimum password length: `set password-policy password-length {8-100}`
To set the length of time a password is valid: `set password-policy validity-duration {0|1-3650}`
To disallow previously used passwords: `set password-policy previous-check {0|1-1000}`

D - Procedure to remove the restriction on numbers

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set password-policy digits-optional
   ```

2. Validate
   The system displays the result

   ```
   Rules successfully updated
   ```

> **Note:**
> To avoid having an end of validity, put 0 in the `Validity duration` field.
> To prevent verification of old passwords, put 0 in the `Verify last 0 passwords` field.

E - Procedure to disable the default password control policy

The command prompt is displayed.

```
(gcap-cli)
```

1. To disable the default password control policy:
   1. Enter the command

      ```
      set password-policy disable
      ```

   2. Validate
      The system displays the result

      ```
      Rules successfully updated
      ```

2. To check the value modification:
   1. Enter the command

      ```
      show password-policy
      ```

   2. Validate
      The system displays the disabled status of the control

```
No active password policy
```

9.3.2.10 set passwords

A - Introduction

The `passwords` command of the `set` sub-group enables modifying the passwords of the setup, gviewadm and gview users.

User	can change the password		
	setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

Passwords must match predefined rules.
For more information on these rules, use the *show password-policy* command.

Important:

Check the keyboard configuration before changing the password (`show keymap` command).

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`set passwords {setup|gviewadm|gview}`

D - Procedure to change the password of the current user (here setup)

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set passwords setup
   ```

2. Validate

   ```
   (current) LDAP Password:
   ```

3. Enter the LDAP password and confirm
   The system asks for the new password of the account (here setup)

   ```
   New password:
   ```

4. Enter the new password and confirm
   The system asks you to reenter the new password

   ```
   Retype new password:
   ```

5. Enter the new password again and confirm
   The system announces that the password has been changed

   ```
   passwd: password updated successfully
   Password changed for user setup
   ```

E - Procedure to change the password of another user

1. Enter the command

   ```
   set passwords gviewadm
   ```

2. Validate

```
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:
```

3. Enter the new password for the account (here gviewadm) then validate
   The system asks you to reenter the new password

```
Retype new password:
```

4. Enter the new password again and confirm
   The system announces that the password has been changed

```
passwd: password updated successfully
Password changed for user gviewadm
```

9.3.2.11 set session-timeout

A - Introduction

The `session-timeout` command of the `set` sub-group enables configuring the time of inactivity before logging out of a user session.

Below are the configuration options:

- The default value is `5min`
- The value `0` enables deactivating the automatic disconnection
- The maximum value is `1440min`

Modifying this configuration is possible at any time. It has no impact on the overall operation of the GCap.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`set session-timeout MINUTES`

D - Procedure to change the default value for automatic log out via the user setup

The command prompt is displayed.

```
(gcap-cli)
```

1. To change the default value for automatic log out via the **user** setup:
   1. Enter the command

      ```
      set session-timeout 1200
      ```

   2. Validate

      The system displays the result

      ```
      Setting session timeout to 1200 mins
      Session timeout successfully changed.
      ```

2. To check the value modification:
   1. Enter the command

      ```
      show session-timeout
      ```

   2. Validate

      The system displays the current session-timeout value

      ```
      Current session timeout is 1200 mins
      ```

9.3.2.12 set ssh-keys

A - Introduction

The `ssh-keys` command of the `set` sub-group enables adding or changing the SSH keys.
Depending on the account, it is possible to change only the current level and the lower level.
The addition or modification can be carried out either on the command line or via the Nano text editor.
Changing SSH keys overwrites the old keys. You must specify the old keys followed by the new ones in the command.

User	can change the password		
	setup	gviewadm	gview
setup	X	X	X
gviewadm		X	X
gview			X

The GCap enables up to 50 different users with different key sizes:

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

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

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

D - Procedure to use the text editor

The command prompt is displayed.

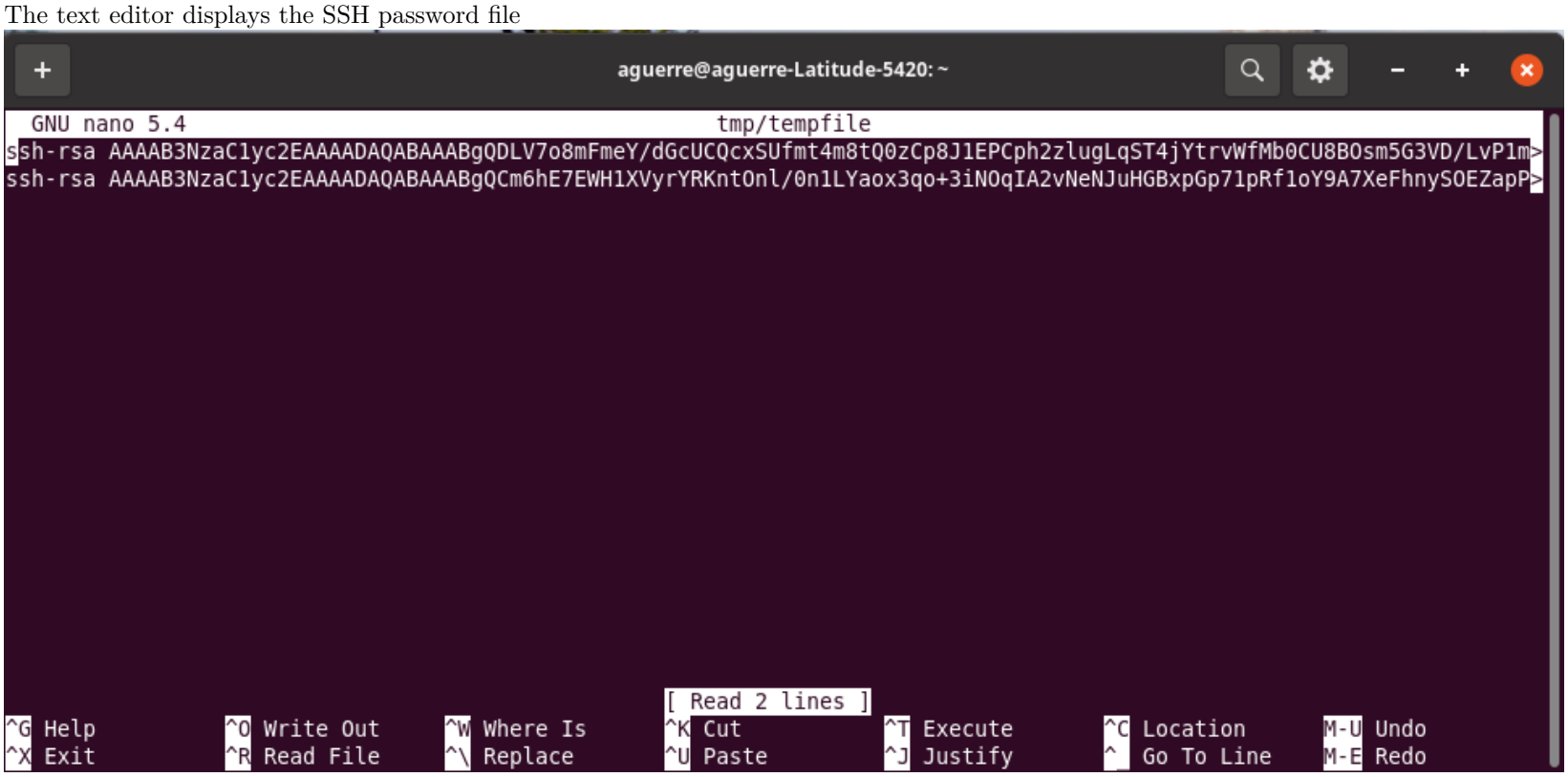
```
(gcap-cli)
```

1. Enter the command

   ```
   set ssh-keys gview
   ```

2. Validate

   The text editor displays the SSH password file



   Each line in the file is an SSH key starting with ssh-rsa.

3. To delete a key, delete the line
   To change a key, edit a line
   To add a key, add a line starting with sshrsa
4. To exit, press <CTRL> + <X>
5. Save the changes if necessary

E - Procedure to add an SSH key to the setup user from a connection with the setup user

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set ssh-keys setup "ssh-rsa ..."
   ```

2. Validate

9.3.2.13 set advanced-configuration mtu

A - Introduction

The `mtu` command in `set advanced-configuration` sub-group enables displaying changing the MTU byte value of enabled network interfaces (`mon0`, `mon1`, … `monx`, `tunnel`, `management`, clusters).
This value must be between 1280 and 9000 bytes.

Note:

XDP Filtering features is not supported if the MTU > 3000.

B - Prerequisites

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

---

C - Command

`set advanced-configuration mtu {interface-name}`

D - Procedure to change the MTU value of the `ensp04` interface

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   set advanced-configuration mtu mon1 1500
   ```

2. Validate
   The system displays the result

   ```
   Updating Network MTU configuration to:
          - mon1: 1500
   ```

9.3.2.14 set advanced-configuration rescan-interfaces

A - Introduction

The `rescan-interfaces` command of the `set advanced-configuration` sub-group enables:

- scanning network interfaces
- synchronizing the detected network interfaces with the predefined names in the system

This command is particularly useful if the interfaces are misnamed or out of order. This can happen in some cases with old or unrecognized material.

B - Prerequisites

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

---

C - Procedure to scan the GCap interfaces without rebooting

Note:

Interfaces being potentially unassigned, access via the SSH connection may not work.
So only physical access or via the management console (iDrac) access are possible.

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

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

2. Validate

   ```
   Operation successful
   ```

9.3.3 system

9.3.3.1 system delete-data

A - Introduction

The `delete-data` command of the `system` sub-group enables deleting all data generated by the monitoring engine which are stored on the filesystem.

B - Prerequisites

- **User:** setup
- **Dépendances :**

C - Command

`system delete-data`

D - Procedure to delete data

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   system delete-data confirm
   ```

2. Validate
   All data will be deleted and the GCap will reboot
   The SSH connection will be interrupted

9.3.3.2 system restart

A - Introduction

The `restart` command of the `system` sub-group enables restarting the GCap.
If before startup the detection engine is activated (**UP** status), it will be activated after startup.
If the GCap is paired with the GCenter before startup, it will be paired after startup.

B - Prerequisites

- **User:** setup
- **Dependencies:** none

C - Command

`system restart`

D - Procedure to restart a GCap

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   system restart
   ```

2. Validate
   The SSH connection will be interrupted

9.3.3.3 system shutdown

A - Introduction

The `shutdown` command of the `system` sub-group enables shutting down the GCap.

Important:

Once the Gcap is turned off, it will need to be turned back on via remote access through the iDRAC.

B - Prerequisites

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

---

C - Command

`system shutdown`

D - Procedure to shut down the GCap

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   system shutdown
   ```

2. Validate

9.3.3.4 system unlock

A - Introduction

The `unlock` command of the `system` sub-group enables resetting the lock of the `gview`, `gviewadm` and `setup` accounts after unsuccessful authentication attempts.

B - Prerequisites

- **User:** setup
- **Dependencies:** N/A

C - Command

`system unlock {setup|gview|gviewadm}`

D - Procedure to unlock the setup account

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   system unlock setup
   ```

2. Validate
   The system displays the result

   ```
   User setup successfully unlocked
   ```

9.3.3.5 system upgrade

A - Introduction

The `upgrade` command of the `system` sub-group enables upgrading the sensor to a new version.

B - Prerequisites

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

C - Command

`system upgrade`

D - Procedure to put a GCap into operation

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the following command to list available packages on GCenter.

   ```
   system upgrade list
   ```

2. Validate
3. Enter the following command to upgrade the sensor

   ```
   system upgrade apply '[package_name]' confirm
   ```

4. Validate

   At the end of the operation sensor will restart

   The SSH connection will be interrupted

9.3.4 monitoring-engine

A - Introduction

The GCap detection engine captures network traffic and analyses it to generate security events such as alerts and metadata.
The `monitoring-engine` command enables:

- Start the detection engine
- Stop the detection engine
- Check the status of the monitor engine

Note:

For this command, there are advanced options (see the *set monitoring-engine* section).
Once the capture engine is enabled, some GCap configuration commands are no longer accessible.
This information is indicated by the "Dependencies" field in the description of each command.
The capture engine must be disabled to make them accessible again.
If the GCap configuration is changed via the GCenter, the detection engine is reloaded automatically.
If the GCap device is restarted, there is no impact on the detection engine status.

B - Prerequisites

- **User:** setup, gviewadm
- **Dependencies**:
  - Add the IP of the GCenter (`set gcenter-ip`).
  - Pair the GCap and the GCenter.
  - Choose the GCenter compatibility version.
  - Activate at least one capture interface.

Note:

If the `sanity-checks` option is set to `enable`, the detection engine starts only after verifying that at least one `monx` capture interface has been activated and that a cable is connected.

C - Command

`monitoring-engine {status|start|stop}`

9.3.4.1 Example of displaying the status of the detection engine

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

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

2. Validate
   The system displays the engine status.

   ```
   Detection engine is down
   ```

   Meaning:
   - Detection engine `down`: means that the engine status is inactive
   - Detection engine `up`: means that the engine status is active

---

9.3.4.2 Example to start the detection engine

The system displays the following command prompt:

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

The command prompt indicates the status of the detection engine : here it is stopped.

1. Enter the command

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

2. Validate
3. Check the status of the detection engine
   The system displays the following command prompt:

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

   The command prompt indicates the status of the detection engine : here it is started.

9.3.4.3 Example of stopping the detection engine

The system displays the following command prompt:

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

The command prompt indicates the status of the detection engine : here it is started.

1. Enter the command

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

2. Validate
3. Check the status of the detection engine

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

   The command prompt indicates the status of the detection engine : here it is stopped.

9.3.5 pairing

A - Introduction

The `pairing` command enables configuring the IPsec pairing with the GCenter.

B - Prerequisites

- **User:** setup
- **Dépendances :**
  - the detection engine must be switched off
  - the network interfaces must be correctly configured
  - the IP address of the GCenter must be entered via the `set gcenter-ip` command
  - the compatibility of the GCenter must be entered via the `set compatibility-mode` command

---

C - Command

```
pairing {fingerprint FINGERPRINT otp OTP|reload-tunnel}
```

D - Procedure to pair a GCap version 2.5.4.0 with a GCenter

For more information on this procedure, see *Procedure to pair a GCap with the GCenter*.

9.3.6 unpair

A - Introduction

The `unpair` command enables deleting configuration related to the pairing (IPSec configuration).

B - Prerequisites

- **User:** setup

C - Command

`unpair`

D - Procedure of unparing

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the following command

   ```
   unpair
   ```

2. Validate
   The system displays **Operation successful**
   For more information on pairing, refer to *Procedure to pair a GCap with the GCenter*

9.3.7 replay

A - Introduction

A file with the pcap extension is one in which raw network traffic has been captured.
The `replay` command enables:

- List the available pcap files
- Asking the detection engine to analyze this network traffic to rebuild the packets contained in this flow
- Replaying it with the possibility of modifying the speed compared to that of the initial capture

Below are the configuration options:

- **List the available pcap files**
  - `list`
- **Choose the name of the pcap file**
  - `pcap`
- **Choose the replay speed**
  - `speed`
- **Choose a loop replay**
  - `forever`

> **Note:**
>
> Adding pcap is only possible with supported versions of the GCenter software.
> Adding pcap is only possible via the command line with the *root* account, otherwise contact Gatewatcher support.

B - Prerequisites

- **User:** setup, gviewadm
- **Dépendances :**
  - The detection engine is started (`UP`)
  - The `monvirt` interface is activated
  - At least one pcap file must be present in the pcap directory

---

C - Command

`replay pcap name.pcap {speed FACTOR} {forever}`

`replay list`

Available commands:

- `forever`: means to replay the pcap file until **CTRL** + **C** is pressed
- `speed x`: x is a number specifying the replay speed of the pcap file (X times the nominal speed)

D - Procedure to display the list of available pcap files

The command prompt is displayed.

```
[Monitoring UP] GCap-lab (gcap-cli)
```

1. Enter the command

   ```
   replay list
   ```

2. Validate

   ```
   Available pcaps are:

   test-dga-v#.pcap
   test-malcore-v1.pcap
   test-powershell-v1.pcap
   test-shellcode-v1.pcap
   test-sigflow-v1.pcap
   ```

   The list of the pcap files present is displayed.
   The files listed above were installed during a new installation or an update if no other pcap file is present on the GCap.

Each of these files allows you to test a different engine.

Note:

For the testsigflowv1.pcap file, it is possible to replay this pcap file but:

- If one of the following 2 signatures is present in the ruleset applied to the GCap then the alerts at the GCenter level are visible:
  - sid:2020716 => ET POLICY Possible External IP Lookup ipinfo.io
  - sid:2013028 ==> ET POLICY curl User-Agent Outbound
- If none of these signatures is present in the ruleset then there is no GCenter alert so it will not be known if the Sigflow engine is working correctly

---

E - Procedure to replay a pcap file with the capture speed

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   replay pcap name.pcap speed 4
   ```

2. Validate

   ```
   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
   ```

The system displays the counters approximately every five seconds:

- Throughput in Bps
- Throughput in Mbps
- Throughput in pps (packets)

then the final counters.

9.3.8 help

9.3.8.1 Introduction

To obtain help with the available commands, it is possible to:

- Prefix it with `` `help` `` (example `` `help show status` ``)
- Suffix the command with `` `?` `` (example `` `show status ?` ``)

Help enables displaying the available commands and a description of the command in the current context.

9.3.8.2 Command `` `?` ``

A - Prerequisites for `` `?` ``

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

B - Command `` `?` ``

- `` `?` `` to display the list of available commands
- `` `show status ?` `` to display the help for the `` `status` `` command of the `` `show` `` sub-group

---

C - Using of `` `?` ``

The `` `?` `` command can be used :

- Alone : in this case, it has the same function as the `` `help` `` command
- After the command for which help is to be displayed : suffixing

---

D - Using the `` `?` `` of suffixing

To list the configuration files accessible via the CLI:

The command prompt is displayed.

```
(gcap-cli)
```

1. Use the `` `show network` `` command followed by `` `?` ``

   ```
   show network ?
   ```

2. Validate
   The system displays the following information

   ```
   Show current network configuration
   ==================================

   Available commands:
      - configuration: Show current network configuration in JSON format
      - tunnel: Show current configuration for tunnel interface
      - management: Show current configuration for management interface
      - hostname: Show current configuration for hostname
      - domain: Show current configuration for domain
   ```

9.3.8.3 Command `` `help` ``

A - Prerequisites for `` `help` ``

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

B - Command `` `help` ``

- `` `help` `` to display the list of available commands
- `` `show status --help` `` to display the help for the `` `status` `` command of the `` `show` `` sub-group
- `` `help show status` `` to display the help for the `` `status` `` command of the `` `show` `` sub-group

---

C - Using the `help` command

The `help` command can be used:

- Alone: in this case, the system displays the commands available in the current level
- Before the command for which the help is to be displayed: prefixing
- After the command for which the help is to be displayed, but `--help` or `-h` must be entered

---

D - Using `help` alone

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   help
   ```

2. Validate
   The system displays the following information

   ```
   CLI entrypoint
   ==============

   Available commands:
    - show: Show system configuration
    - set: Modify system configuration
    - services: Manage service
    - system: Handle system operations
    - monitoring-engine: Handle Monitoring Engine
    - help: Display command help message
    - colour: Handle colour support for current CLI session
    - exit: Exit configuration tool
   ```

E - Procedure of prefixing: display the commands available in the monitoring-engine context from the root of gcap-cli

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   help monitoring-engine
   ```

2. Validate
   The system displays the following information
   - **case 1**

     ```
     Available commands:
         - start: Start the Monitoring Engine
         - status: View current Monitoring Engine status
     ```

     In this case, the engine can be started.

or

- **case 2**

  ```
  Available commands:
   - status: View current Monitoring Engine status
  ```

  In this case, the prerequisites to start the engine are not met.

E - Procedure of suffixing : displaying the information of a command

1. Enter the command

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

2. Validate
   The system displays the following information

   ```
   Shutdown GCap
   ```

9.3.9 color

A - Introduction

The `colour` command enables or disables colors in the output of the current instance of gcap-cli.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`colour {disable|enable}`

D - Procedure to display service statuses with color

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   colour enable
   ```

2. Validate
   The system then displays the information in color

   ```
   <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>
   ```

E - Procedure to display service reports without color

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   colour disable
   ```

2. Validate
   The system then displays the information without color (see example below)

   ```
   <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>
   ```

9.3.10 exit

A - Introduction

The `exit` command enables:

- Returning to the root (gcap cli) if the prompt is elsewhere in the tree structure
- Leave the SSH session if the prompt is already at the root (gcap-cli)

The **CTRL** + **D** shortcut enables calling the `exit` command.

B - Prerequisites

- **User:** setup, gviewadm, gview
- **Dependencies:** N/A

C - Command

`exit`

D - Procedure to exit the current context

1. Enter the command

   ```
   (gcap-cli ...) exit
   ```

2. Validate

   The prompt changed and shows the root context

   ```
   (gcap-cli)
   ```

E - Procedure to exit the CLI

The command prompt is displayed.

```
(gcap-cli)
```

1. Enter the command

   ```
   exit
   ```

2. Validate

Chapter 10

Metrics

10.1 List of available metrics from version 2.5.3.105

10.1.1 Internal metrics

Name	Unit Dimensions	Comments
netdata.runtime_proc_net_dev	run time ms	Execution time of the script for collecting information on the interfaces
netdata.runtime_xdp_filter	run time ms	Execution time of the script for collecting information on XDP filters
netdata.runtime_disk_usage	run time ms	Execution time of the script for collecting information on disk usage
netdata.runtime_proc_meminfo	run time ms	Execution time of the script for collecting information on memory usage
netdata.runtime_proc_loadavg	run time ms	Execution time of the script for collecting information on the GCap load
netdata.runtime_proc_uptime	run time ms	Execution time of the script for collecting information on the uptime
netdata.runtime_proc_vmstat	run time ms	Execution time of the script for collecting information on the virtual memory
netdata.runtime_proc_stat	run time ms	Execution time of the script for collecting information on CPU usage details
netdata.runtime_high_availability	run time ms	Execution time of the script for collecting information on the high availability
netdata.runtime_sys_block	run time ms	Execution time of the script for collecting information on the I/O disks
netdata.runtime_proc_net_softnet_stat	run time ms	Execution time of the script for collecting information on the network stack
netdata.runtime_suricata	run time ms	Execution time of the script for collecting information on Sigflow
netdata.runtime_codebreaker	run time ms	Execution time of the script for collecting information on Codebreaker
netdata.web_thread[1-6]_cpu	user system ms/s	CPU usage time of netdata threads
netdata.plugin_diskspace_dt	duration ms/run	Execution time of the script for collecting information on disk space
netdata.plugin_diskspace	user system ms/s	CPU usage time of the disk space information collection plugin

10.1.2 Details of Sigflow counters

10.1.2.1 Details of Counter Alerts - Number of Sigflow alerts found

Name	Dimensions	Comments
suricata.alert	Alerts.value	Number of Sigflow alerts found

10.1.2.2 Details of Codebreaker samples counters - Files analysed by Codebreaker

Name	Dimensions	Comments
codebreaker.shellcode_samples	plain encoded	Shellcodes detected without encoding / Shellcodes detected with encoding
codebreaker.powershell_samples	Powershell.value	Number of malicious Powershell scripts detected

10.1.2.3 Details of the Protocols counters - Lists of protocols seen by Sigflow

The following counters display the number of events observed by Sigflow about each protocol.

Name	Dimensions	Unit	Comments
suricata.dhcp	DHCP.value	number	protocole DHCP
suricata.dnp3	DNP3.value	number	DNP3 protocol
suricata.dns	DNS.value	number	DNS protocol
suricata.ftp	FTP.value	number	FTP protocol
suricata.http	HTTP.value	number	HTTP protocol
suricata.http2	HTTP2.value	number	HTTP2 protocol
suricata.ikev2	IKEv2.value	number	IKEv2 protocol
suricata.krb5	krb5.value	number	KRB5 protocol
suricata.mqtt	MQTT.value	number	MQTT protocol
suricata.netflow	NETFLOW.value	number	NETFLOW Protocol
suricata.nfs	NFS.value	number	NFS protocol
suricata.rdp	RDP.value	number	RDP protocol
suricata.rfb	RFB.value	number	RFB protocol
suricata.sip	SIP.value	number	SIP protocol
suricata.smb	SMB.value	number	SMB protocol
suricata.smtp	SMTP.value	number	SMTP protoco
suricata.snmp	SNMP.value	number	SNMP protocol
suricata.ssh	SSH.value	number	SSH protocol
suricata.tftp	TFTP.value	number	TFTP protocol
suricata.tls	TLS.value	number	TLS protocol
suricata.tunnel	tunnel.value	number	tunnel protocol

10.1.2.4 Details of the Detection Engine Stats counters - Statistics of Sigflow (monitoring-engine)

Name	Dimensions	Comments
suricata.Status	alive.value	Status of the Sigflow container and the detection engine (boolean)
suricata.total	total.value	Total number of events observed
suricata.fileinfo	• extracted • sent • duplicated	• Number of files extracted • Number of files sent • Number of files duplicated
suricata.received_packets	• ReceivedPackets.value • DroppedPackets.value	• Number of packages captured • Number of packets dropped
suricata.rules	• RulesLoaded.value • RulesFailed.value	• Number of rules loaded and validated • Number of rules that could not be loaded
suricata.tcp_sessions	TcpSessions.value	Number of TCP sessions observed by Sigflow
suricata.tcp_pkt_on_wrong_thread	TcpPktOnWrongThread.value	Misrouted packets par Sigflow
suricata.flows	• FlowTCP.value • FlowUDP.value	• Number of TCP sessions observed • Number of UDP sessions observed

10.1.3 Details of GCap statistics counters and health information.

10.1.3.1 Details of quota counters

Name	Dimensions	Comments
quotas.uid.block	• block.used • block.soft_limit • block.hard_limit	• Number of blocks used • Software limit • Hardware limit
quotas.uid.file	• file.used • file.soft_limit • file.hard_limit	• Number of files used • Software limit • Hardware limit
quotas.uid.grace	• grace.block • grace.file	• Grace time for the blocks • Grace time for the files

10.1.3.2 Details of cpu_stats counters - CPU statistics

Name	Dimensions	Unit	Comments
proc_stat.interrupts	• interrupts	intr/s	Number of interruptions per second
proc_stat.processes	- running blocked	processes	Status of the processes
proc_stat.cpu.cpu(0n)	- softirq irq - user - system - nice iowait - idle	percentage	Percentage of CPU usage

10.1.3.3 System information

Name	Dimensions	Unit	Comments
sys_block.blocks.<disque>	read written	bytes	I/O on the disk **<disque>**
proc_uptime.uptime	uptime.uptime	seconds	System uptime
disk_inodes.<partition>	avail used reserved for root	inodes	Use of the partition's inodes <partition>
xdp_filter.dropped_bytes	dropped_bytes	bytes	Volume dropped per XDP
xdp_filter.dropped_packets	dropped_packets	pkts	Packets dropped per XDP
xdp_filter.bypassed_half_flows	bypassed_half_flows	half flows	Number of half flows dropped per XDP

10.1.3.4 Details of high_availability counters - High availability (HA) information

Name	Dimensions	Unit	Comments
high_availability.ha_status	ha.status	boolean	HA enabled (1) or not (0) (1) ou non (0)
high_availability.leader_status	ha.health_status	boolean	Node status (0: slave or not configured / 1: leader)
high_availability.health_status	ha.health_status	boolean	Ability of the node to become a leader (0: no or not configured / 1: OK)
high_availability.last_received_status	ha.last_status	seconds	Duration since change of status

10.1.3.5 Details of interface counters - Statistics on network interfaces

Name	Dimensions	Unit	Comments
proc_net_dev.net.**<iface>**	• received • sent	bytes	Traffic on the interface **<iface>**
proc_net_dev.net_drops.**<iface>**	• rx drops • tx drops	pkts	Number of packets lost on the interface **<iface>**
proc_net_dev.net_errors.**<iface>**	• rx errors • tx errors	pkts	Number of packets in error on the interface **<iface>**
proc_net_dev.net_pkts.**<iface>**	• received • sent	pkts	Number of packets on the interface **<iface>**

10.1.3.6 Details of meminfo counters - Statistics on RAM

Name	Dimensions	Comments
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 • buffers	• Unused memory in kilo-Bytes • Memory used • Memory used by the cache • Memory used by operations
proc_meminfo.available	available	Total physical memory in kilo-Bytes
proc_meminfo.swap	• swap_free • swap_used • swap_cached	• swap file available • swap file used • swap file used for caching
proc_meminfo.kernel	• kernel.slab • kernel.kernel_stack • kernel.page_tables • kernel.v_malloc_used	• Memory used by kernel data structures • Memory used by kernel stack allocations • Memory used for page management • Memory used by large memory areas allocated by the kernel
proc_meminfo.hugepages	• hugepages_free • hugepages_used • hugepages.surplus • hugepages.reserved	• Number of huge transparent pages available • Number of huge transparent pages used • Number of extra huge transparent pages • Number of huge transparent pages reserved

10.1.3.7 Details of numastat counters - Statistics on NUMA nodes

Name	Dimensions	Unit	Comments
numa_stat	numa_hit	MiB	Memory successfully allocated in this node as expected
	numa_stat	MiB	• Memory allocated in this node despite process preferences • Each numa_miss has a numa_foreign in another node
	numa_foreign	MiB	Memory intended for this node, but currently allocated in a different node
	other_node	MiB	Memory allocated in this node while a process was running in another node
	interleave_hit	MiB	Interleaved memory successfully allocated in this node
	local_node	MiB	Memory allocated in this node while a process was running on it

10.1.3.8 Details of softnet counters - Statistics on received packets according to processor cores

Name	Dimensions	Unit	Comments
proc_net_softnet_stat.cpu[0-n].packets	• Processed • Dropped • Flow limit count • Process queue lengths	pkts	Packets processed on the relevant cpu
proc_net_softnet_stat.cpu[0n].sched	• Received RPS (IPI schedules) • Time squeeze	events	network stack events on the relevant cpu
proc_net_softnet_stat.summed.packets	• Processed • Dropped • Flow limit count • Input/Process queue lengths	pkts	Packets processed by the network stack

10.1.3.9 Details of `virtualmemory` counters - Swap space information (*swap*)

Name	Dimensions	Unit	Comments
proc_vmstat.swapio	• in • out	pkts	I/O swap
proc_vmstat.pagefaults	• minor • major	faults/s	Memory Page Faults /s

10.2 Retrieving the metrics

The GCap metrics are retrieved through the Netdata session hosted on the GCenter.
To find out about the different access methods, please refer to the *Supervision* section of the GCenter documentation.
Metrics are collected at a steady interval:

- Every 10 seconds for system related metrics
- Every minute for detection related metrics

Chapter 11

Appendices

11.1 The log files

It is possible to consult the event files.

To display...	file name...
detection engine events	detection-engine-logs
kernel events	var-log-kernel
the aggregation of different logs	var-log-messages
GCap authentication information	var-log-auth
the launch information of scheduled tasks	var-log-cron
information about the activity of the various applications used	var-log-daemon
information on the activity of the GCap users	var-log-user
debugging events	var-log-debug

11.1.1 Detection engine events: detection-engine-logs

This log contains debug events of the monitoring engine.
They enable obtaining additional information on the status or errors of the detection engine.
Some examples of useful lines:

- End of startup

```
[97] <Info> -- All AFP capture threads are running.
```

- End of rule reload

```
[76] <Info> -- cleaning up signature grouping structure... complete
[76] <Notice> -- rule reload complete
```

- Rule loading error

```
[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
```

11.1.2 Kernel related events: var-log-kernel

This log contains information about kernel events.
Some examples of useful information:

- Change of link status

```
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
```

11.1.3 GCap authentication information: var-log-auth

This log contains the GCap authentication information.
Some examples of useful lines:

- SSH authentication error

```
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]
```

- IPSec events

```
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.gatewatcher.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]
```

11.1.4 Information on the activity of the various applications used: var-log-daemon

This log contains information about the activity of the different applications used.
Some examples of useful lines:

- Configuration synchronization with the 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
```

11.1.5 User activity information: var-log-user

This log contains information about the activity of the GCap users.
Some examples of useful lines:

- Detection engine startup

```
2022-02-03T14:18:26.428461+00:00 GCap.domain.tld root: [GCap_suricata_tools.suricata-INFO] Detection Engine successfully␣
↪started!
```

- Actions performed via the `gcap-cli` command

```
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
```

11.1.6 Debug events: var-log-debug

This log contains debug events.
This entry is mainly used by support during advanced troubleshooting.

11.1.7 Aggregation of different logs: var-log-messages

This log contains the aggregation of the different logs listed above.

11.1.8 Scheduled task start information: var-log-cron

This log contains the launch information of scheduled tasks.

Chapter 12

Glossary

CLI
The Command Line Interface (CLI) is the means used to administer and configure the GCap. It is the set of commands in text mode.

FQDN
The Fully Qualified Domain Name (FQDN) refers to the host.domain name.

GCap
GCap is the detection probe for the Trackwatch/Aioniq solution. It retrieves the network flow from the TAP and reconstructs the files it sends to the GCenter.

GCenter
The GCenter is the component that administers the GCap and performs the analysis of files sent by the GCap.

gview
Account name intended for an operator

gviewadm
Account name intended for a manager

MTU
The Maximum Transfer Unit (MTU) is the largest packet size that can be transmitted at one time, without fragmentation, over a network interface.

OTP
The One Time Password (OTP) is a single-use password defined on the GCenter.

RAID1
RAID 1 consists of using n redundant disks. Each disk in the cluster contains exactly the same data at all times, hence the use of the word "mirroring".

RAID5
RAID 5 uses several hard disks (at least 3) grouped together in a cluster to form a single logical unit. The data is duplicated and allocated to two different disks.

setup
Account name intended for a system administrator

SIGFLOW
The detection engine, also called Sigflow, is responsible for rebuilding the files and is also one of the engines for intrusion detection.

TAP
The Test Access Point (TAP) is a passive device enabling a network flow to be duplicated.

`PDF documentation`