# Documentation
# GCap Version 2.5.4


Documentation version: V1

Creation date: December, 2024

# Contents

**Contents** 1

**1 Description** 4
- 1.1 Introduction . . . 4
- 1.2 TAP . . . 5
- 1.3 GCap . . . 5
  - 1.3.1 Different server models . . . 5
  - 1.3.2 Description of the GCap inputs / outputs . . . 5
  - 1.3.3 Electrical connection . . . 8
  - 1.3.4 USB connector and LUKS key . . . 8
- 1.4 GCenter . . . 8
- 1.5 Interconnection of subsets . . . 8
  - 1.5.1 Reminder of the GCap connections . . . 8
  - 1.5.2 Capture and monitoring interfaces `monx` between TAP and GCap: aggregation possibility . . . 9
  - 1.5.3 Transferring rules between GCenter and GCap: single-tenant vs. multi-tenant . . . 11

**2 Operation** 12
- 2.1 GCap . . . 12
  - 2.1.1 GCap functions . . . 12
  - 2.1.2 The Sigflow engine . . . 12
  - 2.1.3 Counters of GCap activity . . . 13
- 2.2 GCap configuration . . . 13
  - 2.2.1 Configuring a GCap and its Sigflow engine . . . 13
  - 2.2.2 Overview of date and time management . . . 14
  - 2.2.3 Overview of `Management` (`gcp1`) and `Tunnel` (`gcp0`) interfaces . . . 14
  - 2.2.4 Overview of managing the monitoring interfaces . . . 15
  - 2.2.5 Capture and monitoring interfaces: single-tenant vs. multi-tenant . . . 16
  - 2.2.6 Capture and monitoring interfaces: aggregation . . . 19
  - 2.2.7 Sigflow detection engine . . . 19
- 2.3 Redundant GCaps: high availability . . . 23

**3 Characteristics** 24
- 3.1 Mechanical characteristics of GCap . . . 24
- 3.2 Electrical characteristics of GCap . . . 24
- 3.3 Functional characteristics of GCap . . . 25
  - 3.3.1 Functional characteristics . . . 25
  - 3.3.2 List of protocols that can be selected for analysis . . . 25
  - 3.3.3 List of selectable protocols for file reconstruction . . . 26

**4 The accounts** 27
- 4.1 List of accounts . . . 27
- 4.2 Related principles . . . 27
  - 4.2.1 Authentication mode . . . 27

4.2.2 Password management . . . 27
4.2.3 Password management policy . . . 28
4.2.4 SSH key . . . 28
4.2.5 Rights associated with each account . . . 28
4.3 gview profile . . . 28
4.4 gviewadm profile . . . 29
4.5 Setup profile . . . 29
4.6 List of functions by level and by theme . . . 31
4.6.1 Configuring the GCap . . . 31
4.6.2 Managing accounts . . . 31
4.6.3 Managing the detection engine . . . 32
4.6.4 Managing network . . . 32
4.6.5 Managing server . . . 32
4.6.6 Monitoring the GCAP . . . 33

**5 Use cases** **34**
5.1 Introduction . . . 34
5.2 How to connect to Gcap? . . . 34
5.2.1 Direct connection and configuration . . . 34
5.2.2 Remote connection to the iDRAC in HTTP (DELL server) . . . 35
5.2.3 Remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode . . . 35
5.2.4 Remote connection to the CLI in SSH via the network interfaces with the `management` role (formerly `gcp0` or `gcp1`) . . . 35
5.3 Remote connection to the GCenter . . . 35
5.4 How to use the procedures . . . 36
5.4.1 Accessing the GCap and GCenter . . . 36
5.4.2 Configuring the GCap . . . 36
5.4.3 Managing accounts . . . 36
5.4.4 Managing networks . . . 37
5.4.5 Managing the detection engine . . . 37
5.4.6 Managing servers . . . 37
5.4.7 Monitoring the GCAP . . . 38
5.5 List of procedures . . . 38
5.5.1 Configuring the GCap for the first connection . . . 38
5.5.2 Starting up a GCap . . . 39
5.5.3 Direct connection to the GCap with keyboard and monitor . . . 40
5.5.4 Remote connection to the iDRAC in HTTP (DELL server) . . . 42
5.5.5 Remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode . . . 43
5.5.6 Remote connection to GCap via an SSH tunnel . . . 45
5.5.7 Connection to the GCenter via a web browser . . . 46
5.5.8 Changing the GCap date and time . . . 47
5.5.9 Managing the network parameters of `Tunnel` and `Management` interfaces . . . 48
5.5.10 Managing capture interface settings `monx` . . . 54
5.5.11 Switching to a single-interface configuration . . . 57
5.5.12 Switching to a dual-interface configuration . . . 59
5.5.13 Managing capture interface aggregation . . . 61
5.5.14 Pairing between a GCap and a GCenter . . . 63
5.5.15 Managing the high availability of GCaps . . . 66
5.5.16 Optimising performance . . . 66

**6 CLI** **69**
6.1 Overview of the CLI . . . 69
6.1.1 Introduction to the CLI . . . 69
6.1.2 Overview of the command prompt . . . 69
6.1.3 Accessible commands grouped by set . . . 69
6.1.4 Directly accessible commands . . . 70

6.1.5 Completion . . . 70
6.1.6 Navigating in the command tree . . . 71
6.1.7 Launching a command . . . 71
6.1.8 Obtaining information on commands via Help . . . 72
6.1.9 Exit . . . 72
6.2 cli . . . 72
6.2.1 show . . . 72
6.2.2 set . . . 105
6.2.3 services . . . 122
6.2.4 system . . . 123
6.2.5 monitoring-engine . . . 126
6.2.6 pairing . . . 128
6.2.7 unpair . . . 129
6.2.8 replay . . . 130
6.2.9 help . . . 132
6.2.10 colour . . . 135
6.2.11 gui . . . 136
6.2.12 exit . . . 136

**7 Metrics** **138**
7.1 List of metrics comparison version 2.5.3.105 vs 2.5.3.104 . . . 138
7.1.1 Internal metrics version 2.5.3.105 vs 2.5.3.104 . . . 139
7.1.2 System information version 2.5.3.105 vs 2.5.3.104 . . . 140
7.1.3 Network information version 2.5.3.105 vs 2.5.3.104 . . . 141
7.1.4 Device and detection information version 2.5.3.105 vs 2.5.3.104 . . . 141
7.2 List of available metrics from version 2.5.3.105 . . . 142
7.2.1 Internal metrics . . . 142
7.2.2 Details of Sigflow counters . . . 142
7.2.3 Details of GCap statistics counters and health information. . . . 144
7.3 Retrieving the metrics . . . 149

**8 Appendices** **150**
8.1 Event files . . . 150
8.1.1 Detection engine events: detection-engine-logs . . . 150
8.1.2 Kernel related events: var-log-kernel . . . 151
8.1.3 GCap authentication information: var-log-auth . . . 151
8.1.4 Information on the activity of the various applications used: var-log-daemon . . . 151
8.1.5 User activity information: var-log-user . . . 152
8.1.6 Debug events: var-log-debug . . . 152
8.1.7 Aggregation of different logs: var-log-messages . . . 153
8.1.8 Scheduled task start information: var-log-cron . . . 153

**9 Glossary** **154**

**Index** **155**

**Index** **155**

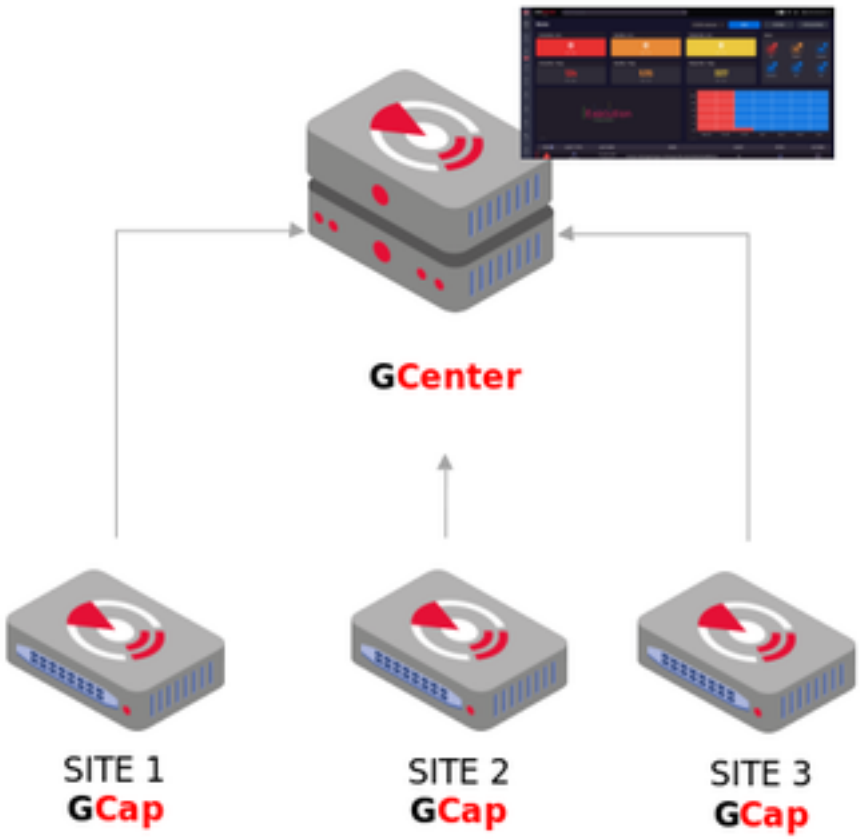
# Chapter 1

# 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



## 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 GCap

GCap is a probe-type component.
It enables:

- Capturing and analysing network traffic from TAPs
- Generating events, alerts, and metadata
- Rebuilding the files contained in the flow
- Communicating with the GCenter

---

### 1.3.1 Different server models

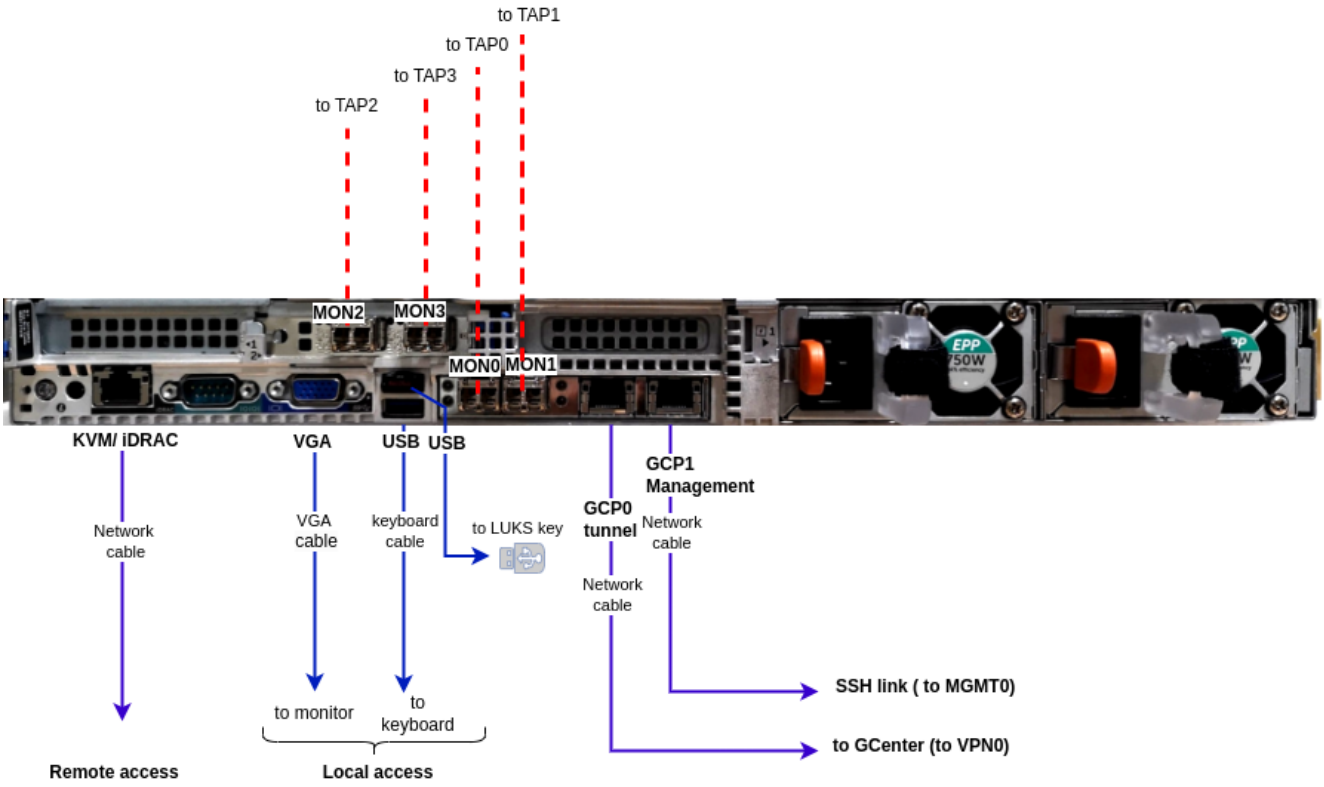
For more information, please refer to the *Characteristics* section.

---

### 1.3.2 Description of the GCap inputs / outputs

The GCap detection probe features:

- A USB and VGA connector to directly access a keyboard and a monitor.
  This connection mode is deprecated in favour of KVM/IDRAC/XCC and should only be used as a last resort
- A USB connector accommodates the USB key enabling disk decryption (standard Linux Unified Key Setup)
- One RJ-45 connector to access the server management and configuration interface (KVM/IDRAC/XCC)
- Two RJ-45 connectors `management` (`gcp1`) and `tunnel` (`gcp0`) roles
- RJ-45 and/or fibre connectors for monitoring `mon0` (`capture` role)
- Two power supplies




#### 1.3.2.1 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.

#### 1.3.2.2 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.

#### 1.3.2.3 Management (gcp1) 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 analysing the monitored flows
  - Report information on the health of the probe to GCenter
  - Control the probe
  - Analysis rules, signatures, and so on
- 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 this interface.
In **dual-interface configuration**, these roles is allocated over to interface (preferably, the two embedded gigabit ethernet network interface, formerly gcp0 and gcp1)

---

##### 1.3.2.3.1 Configuration of the managemement and tunnel network interfaces

For more information on these interfaces and their configuration, refer to the section *Network interfaces management and tunnel*.

---

#### 1.3.2.4 Capture and monitoring interfaces

These interfaces receive:

- The flows from the TAPs on the indicated interfaces (`mon0` and `monx`), which perform the `capture` role.
- 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.

---

##### 1.3.2.4.1 Activating the monitoring monx interfaces

For more information, please refer to the paragraph *Monitoring interfaces: activation*.

---

#### 1.3.2.4.2 Aggregating the monitoring monx interfaces

For more information, see the paragraph *Monitoring interfaces between TAP and GCap: aggregation capability*.

---

### 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 GCenter

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

- The 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 analyses 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 Interconnection of subsets

### 1.5.1 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
- Capture/monitoring interfaces `mon0`, `mon1`, `mon2`, `monx` for connecting TAPs
- The embedded network interfaces formerly `gcp0` and `gcp1`
  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 the *Description of GCap inputs/outputs*.

**Note:**

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

---

### 1.5.2 Capture and monitoring 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 uplink
- A downlink

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

---

#### 1.5.2.1 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.

---

#### 1.5.2.2 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.

---

##### 1.5.2.2.1 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 fibre link handles two links:

- An uplink, i.e. a TX link
- A downlink, i.e. an RX link

The TAP (without aggregation) is connected to the network via 2 physical links called `commutateur X` and `commutateur Y`.
The `commutateur 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 `commutateur 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)

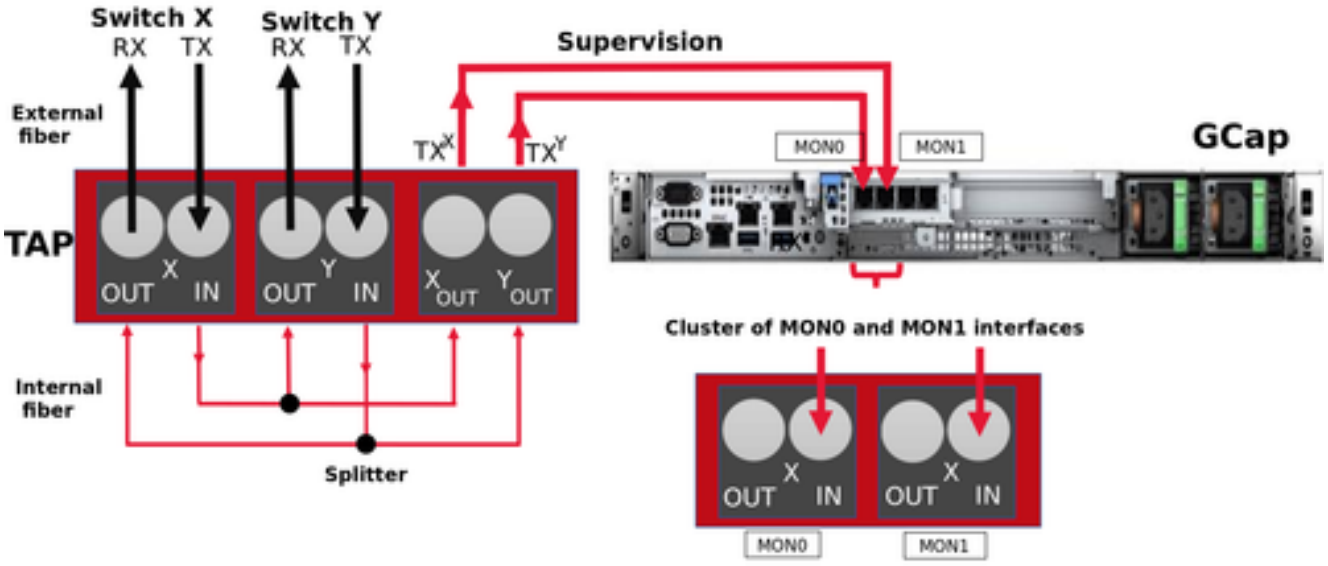
The `commutateur Y` link connects the switch and the **Y** input TAP and enables duplicating the other half the network flow.
The TX link is:

- 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 `commutateur 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)

---

#### 1.5.2.2.2 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.




---

#### 1.5.2.3 Using and configuring interface aggregation

To implement interface aggregation, refer to the *Procedure for managing capture interface aggregation*.

---

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

For more information, please refer to the paragraph *Capture and monitoring 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 and 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 *Managing 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 monopolise 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:**

`show/set advanced-configuration packet-filtering` command has been removed.
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 analysed 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 detection engine*.

---

## 2.2 GCap configuration

### 2.2.1 Configuring a GCap and its Sigflow engine

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

- Synchronise the date and time of the GCap on GCenter: see *Overview of the date and time management*
- Managing Tunnel (`gcp1`) and Management (`gcp0`) interfaces: see *Overview of managing `gcp0` and `gcp1` network interfaces*
- Managing Capture Interfaces: see *Overview of managing capture and monitoring interfaces*
- Manage single-tenant vs. multi-tenant configuration of `monx` interfaces: see *Capture and Monitoring Interfaces: Single-tenant vs. multi-tenant*
- Managing the aggregation of capture interfaces: see *Capture and monitoring 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 the *Procedure for modifying the GCap date and time*.
Thereafter, the GCap date and time are synchronised with the GCenter date and time after the IPsec tunnel is established.

---

### 2.2.3 Overview of `Management` (`gcp1`) and `Tunnel` (`gcp0`) interfaces

**Important:**

Concept of role is introduced in the release 2.5.4.0.

These interfaces perform the following role:

- 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 analysing the monitored flows
  - Report information on the health of the probe to GCenter
  - Control the probe - analysis rules, signatures, and so on
- 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)

---

#### 2.2.3.1 CLI commands

Managing the network interfaces is done using the CLI commands listed in the *Manage the network* table.

---

#### 2.2.3.2 View or configure

To view or configure the network interfaces, refer to the *Procedure for managing the network settings for `Management` and `Tunnel` interface*.

---

##### 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 the *Procedure for switching to 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 (formerly gcp0 and gcp1).

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

---

### 2.2.4 Overview of managing the monitoring 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 labelled:

- `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 the *Capture and monitoring interfaces section*.

**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 monitoring 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 monitoring interfaces is done using the CLI commands listed in the *Manage the network* table.

---

#### 2.2.4.2 Use case procedures

To view or configure the monitoring interfaces, refer to the *Procedure for managing capture interface settings* `monx`.

---

### 2.2.5 Capture and monitoring 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 optimised to reduce false positives.
The set of rules 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.

---

##### 2.2.5.1.1 CLI commands

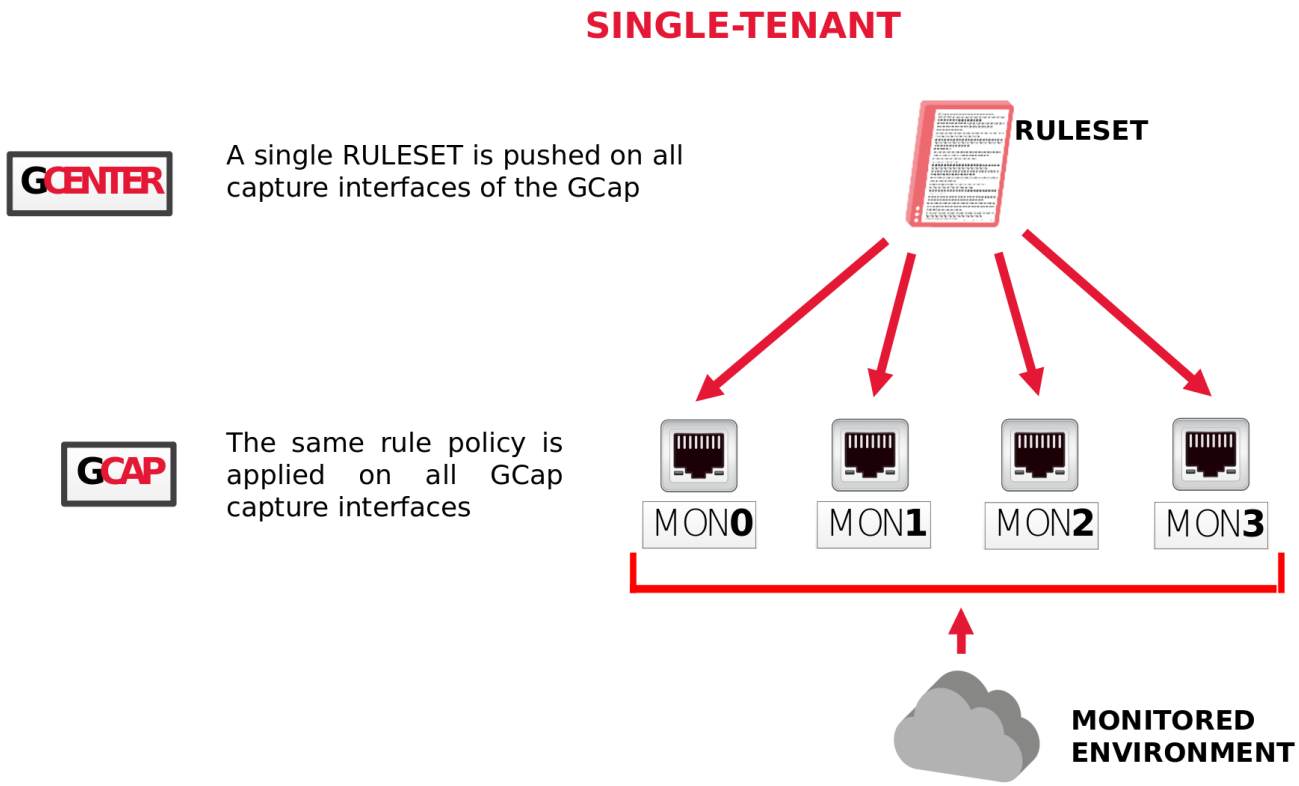
The ability to view and create local rules is handled differently depending on the configuration.
For more information on rules, see the table *Managing the detection engine (advanced functions)*.

---

#### 2.2.5.2 Transferring the rule set in single-tenant mode

##### 2.2.5.2.1 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.




**Sigflow rules in single-tenant**

---

##### 2.2.5.2.2 Configuring the single-tenant mode

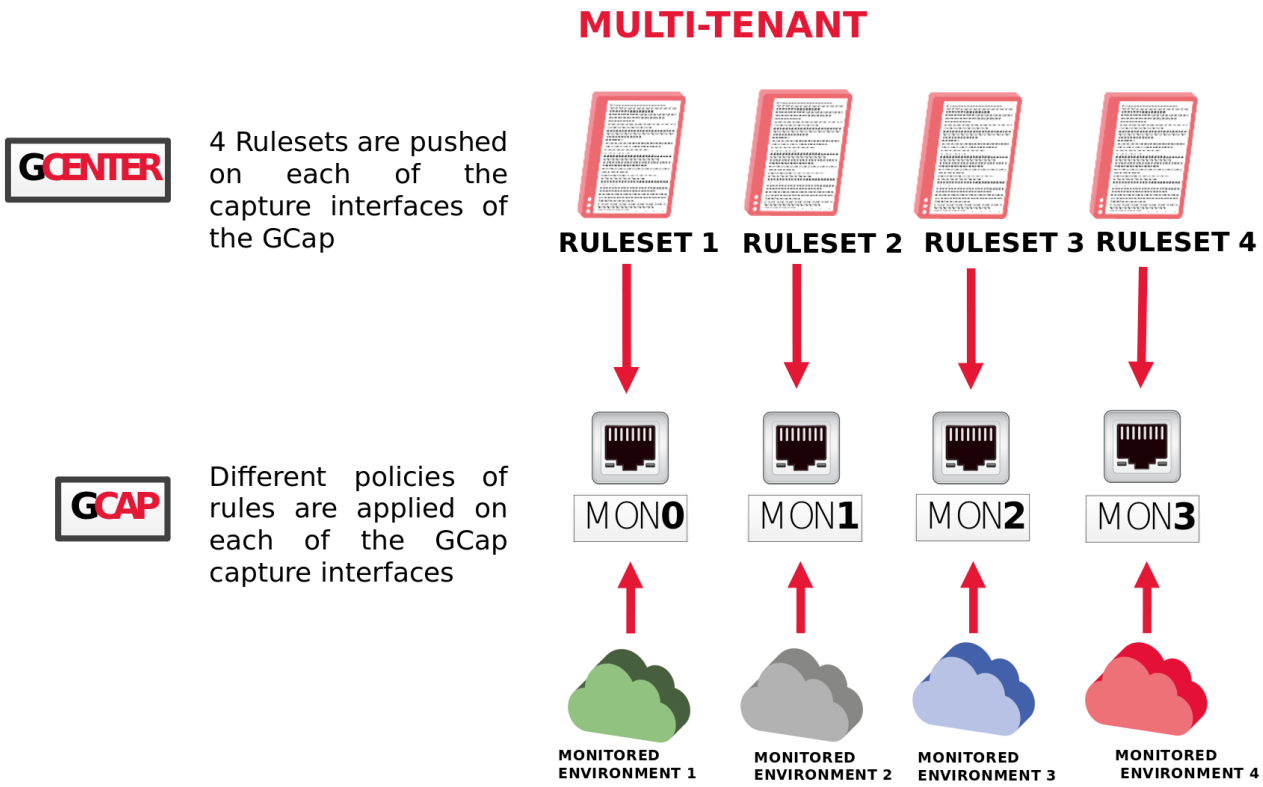
In the GCenter web interface, in the `SIGFLOW - GCaps Profiles > Detection rulesets` part, the default option is single-tenant.

---

#### 2.2.5.3 Transferring the SIGFLOW rule set in multi-tenant mode

##### 2.2.5.3.1 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.




**Sigflow rules in multi-tenant**

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.

---

#### 2.2.5.3.2 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 optimise 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 and monitoring interfaces: aggregation

#### 2.2.6.1 Aggregation principle ("cluster")

For more information, refer to *Capture and monitoring interfaces between TAP and GCap*.

---

#### 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 implementation, refer to the *Procedure for managing capture interface aggregation*.

---

#### 2.2.6.4 Aggregation configuration

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

---

#### 2.2.6.5 Impact on other functionalities

The aggregation functionality of the capture interfaces on the GCap leads to a degradation of some related functions:

- Maximum Transmission Unit (MTU): 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.
- Static rules for filtering flows captured by monitoring interface: XDP (eXpress Data Path) filter function.
  *XDP Filter*: XDP filtering is not applied by default to the aggregation created but rather to the interfaces that comprise it.

---

### 2.2.7 Sigflow detection engine

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

- Activate one or more capture interfaces on the GCap
- Pairing the GCap with GCenter
- Activation of the Sigflow detection engine, by default it is deactivated

---

#### 2.2.7.1 Activate one or more capture and monitoring interfaces on the GCap

##### 2.2.7.1.1 CLI commands

Managing the capture interfaces is done using the CLI commands listed in the *Manage the network* table.

---

##### 2.2.7.1.2 Use case procedures

To view or configure the capture interfaces, refer to the *Procedure for managing capture interface settings* `monx`.

---

#### 2.2.7.2 Aggregating capture and monitoring interfaces `monx`

For more information on this aggregation, see the paragraph *Capture and monitoring interfaces `monx` between TAP and GCap: aggregation capability*.
For more information on how to configure this aggregation, refer to the paragraph Configuring the capture and monitoring 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 the procedure *Pairing between a GCap and 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 monitor engine can be checked with the command `show status`.

---

##### 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:

- Enter the *monitoring-engine start* command
- Validate

```
(gcap-cli) 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.
Detection 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* subgroup 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 start-up 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 analysis 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 via 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:

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

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

```
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 *CLI*.

---

#### 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

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

The system displays the parameter update information.

```
Updating 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.
Please refer to the GCenter documentation for more information.

**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.

## 2.3 Redundant GCaps: high availability

**Note:**

**This feature is deprecated**.
Please contact Gatewatcher if you want to deploy a redundant architecture.

# 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 | CAPTURE PORTS | EXTENSION CAPTURE PORTS | ELECTRIC POWER |
|---|---|---|---|---|
| GCAP1010HWr2 | 256GB | 4 x RJ45 | N/A | 2 x 750W |
| GCAP1020HWr2 | 256GB | 4 x RJ45 | N/A | 2 x 750W |
| GCAP1050HWr2 | 256GB | 4 x RJ45 | N/A | 2 x 750W |
| GCAP1100HWr2 | 2 x 600GB RAID1 | 1 x SFP | N/A | 2 x 750W |
| GCAP1200HWr2 | 2 x 600GB RAID1 | 2 x SFP | N/A | 2 x 750W |
| GCAP1400HWr2 | 2 x 600GB RAID1 | 4 x SFP | N/A | 2 x 750W |
| GCAP2200HWr2 | 4 x 600GB RAID5 | 4 x SFP | 4 x SFP | 2 x 750W |
| GCAP2600HWr2 | 4 x 600GB RAID5 | 4 x SFP | 4 x SFP | 2 x 750W |
| GCAP2800HWr2 | 4 x 600GB RAID5 | 4 x SFP | 4 x SFP | 2 x 750W |
| GCAP5400HWr2 | 8 x 600GB RAID5 | 4 x SFP+ | 4 x SFP+ | 2 x 1100W |
| GCAP5600HWr2 | 8 x 600GB RAID5 | 4 x SFP+ | 4 x SFP+ | 2 x 1100W |
| GCAP5800HWr2 | 8 x 600GB RAID5 | 4 x SFP+ | 4 x SFP+ | 2 x 1100W |

## 3.3 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 | 25 | 200 000 | 10 000 | 3000 |
| GCAP2800HWr2 | 4 GBPS | 25 | 250 000 | 20 000 | 4000 |
| GCAP5400HWr2 | 10 GBPS | 35 | 500 000 | 50 000 | 8000 |
| GCAP5600HWr2 | 20 GBPS | 35 | 750 000 | 75 000 | 8000 |
| GCAP5800HWr2 | 40 GBPS | 35 | 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

| PROTOCOLE | 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 |
| TFTP | 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

| PROTOCOLE | 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 GCap administration interface is protected by a login password.
Three generic accounts are defined with different rights levels:

| Account... | account 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 |
|---|---|
| Number of different characters for a password to be considered as different | 2 |
| Minimum password length | 12 characters |
| Presence of at least one lower case letter | yes |
| Presence of 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 authorised 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

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.

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

- To access the commands of all `show` for:
  - Displaying the keyboard layout (`show keymap`)
  - Displaying the list of users managed by the current level (`show passwords`)
  - Displaying the current GCap status (`show status`)
  - Displaying the statistics of the Sigflow detection engine (`show eve-stats`)
  - Password policy for the accounts (`show password-policy`)
- To access the commands of all `set` for:
  - Changing the password of the current user and the lower level (`set passwords`)
  - Changing the keyboard configuration (`set keymap`)
  - Changing SSH keys for the current user and the lower level (`set ssh-keys`)

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.

---

## 4.4 gviewadm profile

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.

In addition to the common functions of **gview**, the **gviewadm** account has the following supplementary functions:

- Access the commands of all `show` for displaying the statistics and health information of the GCap (`show health`)
- Start, stop and view the status of the detection engine (`monitoring-engine`)

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.

---

## 4.5 Setup profile

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.

In addition to the common functions of **gviewadm**, the **setup** account has the following supplementary functions:

- Access the commands of set `show` to display:
  - Information about the available capture interfaces (`show interfaces`)
  - The compatibility mode used to interact with the GCenter (`show compatibility-mode`)
  - The date and time of the GCap (`show datetime`)
  - The protection system policy (`show bruteforce-protection`)
  - The inactivity time before logging out of a user session (`show session-timeout`)
  - The IP address of the GCenter with which the GCap is paired (`show gcenter-ip`)
  - The advanced options of the detection engine configuration (`show monitoring-engine`)
  - The GCap information requested by technical support (`show tech-support`)
- Access the advanced commands of the `show advanced-configuration` set to display:
  - The static filtering rules of the flow (`show advanced-configuration packet-filtering`)
- Access the commands of the `set` set to:
  - Manage the protection system against brute force attacks (`set bruteforce-protection`)
  - Configure the aggregation on the GCap capture interfaces (`set clusters`)
  - Change the compatibility mode used to interact with the GCenter (`set compatibility-mode`)
  - Adjust the date and time (`set datetime`)
  - Specify the IP address of the GCenter to which the GCap will be paired (`set gcenter-ip`)
  - Administer network capture interfaces (`set interfaces`)
  - Change the keyboard configuration (`set keymap`)
  - Apply advanced configuration for the GCap sensor detection engine (`set monitoring-engine`)
  - Change the network configuration (`set network-config`)
  - Set password policy for accounts (`set password-policy`)
  - Configure inactivity time before logging out (`set session-timeout`)
- Access the advanced commands of the `set advanced-configuration` set to:
  - Modify the MTU value of enabled capture interfaces (`set advanced-configuration mtu`)
- Access the `system` set commands to manage the server:
  - Restart the GCap (`system restart`)
  - Shut down the GCap (`system shutdown`)
  - Reset `gview`, `gviewadm` and `setup` account lockout after unsuccessful authentication attempts (`system unlock`)
- Access the `pairing` commands to associate a GCap to a GCenter:
  - Pair a GCap (`pairing`)
  - Remove an existing pairing (`unpair`)

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.

## 4.6 List of functions by level and by theme

### 4.6.1 Configuring the GCap

Table1: Configuring the GCap

| Function by level | setup | gviewadm | gview |
|---|---|---|---|
| **Keyboard configuration** : display | show keymap | show keymap | show keymap |
| **Keyboard configuration** : modify | set keymap | set keymap | set keymap |
| **Date and time** : display | show datetime | N/A | N/A |
| **Date and time** : modify | set datetime | N/A | N/A |
| **Colours**: enable or disable for the current session | colour | colour | colour |
| **Compatibility mode with the GCenter** : display | show compatibility-mode | N/A | N/A |
| **Compatibility mode with the GCenter** : modify | set compatibility-mode | N/A | N/A |
| **Pairing with the GCenter** | pairing | N/A | N/A |
| **Unpair the GCap** | unpair | N/A | N/A |

### 4.6.2 Managing accounts

Table2: Managing accounts

| Function per level | setup | gviewadm | gview |
|---|---|---|---|
| **Authentication**: display the list of users | show passwords | show passwords | show passwords |
| **Authentication**: change passwords | set passwords | set passwords | set passwords |
| **Authentication**: change SSH keys | set ssh-keys | set ssh-keys | set ssh-keys |
| **Authentication**: display the password policy | show password-policy | show password-policy | N/A |
| **Authentication**: unlocking blocked accounts | system unlock | N/A | N/A |
| **Authentication**: define a password policy | set password-policy | N/A | N/A |
| **Authentication**: display policy for protecting against brute force attacks | show bruteforce-protection | N/A | N/A |
| **Authentication**: modify the policy for protecting against brute force attacks | set bruteforce-protection | N/A | N/A |
| **Session**: display the duration of inactivity before disconnection | show session-timeout | N/A | N/A |
| **Session**: change the duration of inactivity before disconnection | set session-timeout | N/A | N/A |

### 4.6.3 Managing the detection engine

Table3: Managing the detection engine

| Function per level | setup | gviewadm | gview |
|---|---|---|---|
| **Sigflow configuration**: display advanced options | show monitoring-engine | N/A | N/A |
| **Sigflow configuration**: apply an advanced configuration | set monitoring-engine | N/A | N/A |
| **Sigflow configuration**: start the detection engine | monitoring-engine start | monitoring-engine start | N/A |
| **Sigflow configuration**: stop the detection engine | monitoring-engine stop | monitoring-engine stop | N/A |
| **Sigflow configuration**: display status | monitoring-engine status | monitoring-engine status | N/A |
| **Traffic generation**: replaying a pcap file | replay | replay | N/A |

### 4.6.4 Managing network

Table4: Managing network

| Function per level | setup | gviewadm | gview |
|---|---|---|---|
| **Network configuration**: consult the network configuration (IP addresses, name, domain...) | show network-config | N/A | N/A |
| **Network configuration**: change the configuration | set network-config | N/A | N/A |
| **GCenter IP address**: display the IP address of the GCenter with which the GCap is paired | show gcenter-ip | N/A | N/A |
| **GCenter IP address**: specify the IP address of the GCenter to which the GCap will be paired | set gcenter-ip | N/A | N/A |
| **Detection interfaces**: display the information | show interfaces | N/A | N/A |
| **Detection interfaces**: configure | set interfaces | N/A | N/A |
| **Detection interfaces**: display the MTU value | show interfaces | N/A | N/A |
| **Detection interfaces**: change the MTU value | set advanced-configuration mtu | N/A | N/A |
| **Aggregation of detection interfaces**: display the information | show interfaces | N/A | N/A |
| **Aggregation of detection interfaces**: configure | set interfaces | N/A | N/A |

### 4.6.5 Managing server

Table5: Managing server

| Function per level | setup | gviewadm | gview |
|---|---|---|---|
| Display help on the commands | help | help | help |
| Exit the current session or leave the SSH session | exit | system restart | system restart |
| **System**: shut down the GCap | system shutdown | N/A | N/A |

### 4.6.6 Monitoring the GCAP

Table6: Monitoring the GCAP

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

# Chapter 5

# Use cases

## 5.1 Introduction

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 *Procedure list* section enable a general overview of the most common actions.

---

## 5.2 How to connect to Gcap?

Access to the GCap can be made:

- 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
- Or by a remote connection to the CLI in SSH via the network interface with the role `management` (formerly `gcp0` or `gcp1`)

Access to the operating system and CLI for managing the GCap can be done remotely via an SSH or HTTP connection.

**Note:**

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

---

### 5.2.1 Direct connection and configuration

There is no specific configuration required other than knowing the iDRAC login name and password.
This access can be done to configure the network connection of the iDRAC among other things.
For implementation, refer to the *Procedure for direct connection to the GCap*.

**Note:**

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

---

### 5.2.2 Remote connection to the iDRAC in HTTP (DELL server)

The remote access can be made:

- Via the network connection to the iDRAC port of the GCap
- Using 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)

This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
For its implementation, refer to the *Procedure for remote HTTP connection to iDRAC*.

---

### 5.2.3 Remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode

The remote access can be made:

- Via the network connection to the iDRAC port of the GCap
- By using 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)

This connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
For the implementation, refer to the *Procedure for remote connection to the CLI by SSH via the iDRAC interface in serial port forwarding mode*.

---

### 5.2.4 Remote connection to the CLI in SSH via the network interfaces with the `management` role (formerly `gcp0` or `gcp1`)

Remote access to the GCap CLI is achieved via the network connection to the port:

- with the `management` role (dual-interface configuration - formerly gcp1)
- with the `management-tunnel` role (single interface configuration - formerly gcp0)

This connection is the nominal way to access the GCap.
For more information, see *Procedure for connecting to the GCap via SSH*.

---

## 5.3 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.
- Or via a web browser in order to pair the GCap.
  For more information, see *Procedure for connecting to the GCenter via a web browser*.

---

## 5.4 How to use the procedures

### 5.4.1 Accessing the GCap and GCenter

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| First connection to the GCap by a direct connection | 1 | *Direct connection to GCap with keyboard and monitor* |
| Remote connection to iDRAC via HTTP | 1 | *Remote connection to iDRAC via HTTP* |
| Remote SSH connection in serial port forwarding mode | 1 | *Remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode* |
| Connection to the GCenter via a web browser | 1 | *Connection to the GCenter via a web browser* |

### 5.4.2 Configuring the GCap

| To perform the following task | Perform the following procedures in sequence | |
|---|---|---|
| The first installation to GCap | 1 | *Configuring the GCap on first login* |
| | 2 | *Putting a GCap into operation* |
| Keyboard configuration | 1 | Display: use the command *show keymap* |
| | 2 | Modify: use the command *set keymap* |
| Configuring the Gcap interface: (GUI or CLI) | 1 | Display: use the command *show setup-mode* |
| | 2 | Modify: use the command *set setup-mode* |
| Date and time | 1 | Display: use the command *show datetime* |
| | 2 | Modify: use the procedure *Change GCap date and time* |
| Colours in the display | 1 | Enable or disable: use the command *colour* |
| Compatibility mode with the GCenter | 1 | Show: use the command *show compatibility-mode* |
| | 2 | Modify: use the command *set compatibility-mode* |
| Pairing with GCenter | 1 | Use the procedure *Pairing between a GCap and a GCenter* |

### 5.4.3 Managing accounts

| To perform the following task | Perform the following procedures in sequence | |
|---|---|---|
| Authentication: the list of users | 1 | Display the list: use the command *show passwords* |
| | 2 | Change passwords: use the command *set passwords* |
| Authentication: modify the SSH keys | 1 | Use the command *set ssh-keys* |
| Authentication: display the password policy | 1 | Use the command *show password-policy* |
| Authentication: unlock blocked accounts | 1 | Use the command *system unlock* |
| Authentication: define a password policy | 1 | Use the command *set password-policy* |
| Authentication: display the protection policy against brute force attacks | 1 | Use the command *show bruteforce-protection* |
| Authentication: modify the protection policy against brute force attacks | 1 | Use the command *set bruteforce-protection* |
| Session: display the duration of inactivity before disconnection | 1 | Use the command *show session-timeout* |
| Session: modify the duration of inactivity before disconnection | 1 | Use the command *set session-timeout* |

### 5.4.4 Managing networks

| To perform the following task | Perform the following procedures in sequence | |
|---|---|---|
| Managing Tunnel (gcp0) and Management (gcp1) interfaces | 1 | Use the procedure *Managing network settings for Tunnel and Management interfaces* |
| IP address of the GCenter: display the GCenter IP address | 1 | Use the command *show gcenter-ip* |
| IP address of the GCenter: modify the GCenter IP address | 1 | Use the command *set gcenter-ip* |
| Manage the capture interfaces monx | 1 | Use the procedure *Manage monx capture interface settings* |
| Manage interface aggregation of capture | 1 | Use the procedure *Manage capture interface aggregation* |
| Switch to the configuration single-interface | 1 | Use the procedure *Flip to single-interface configuration* |
| Switching to the configuration dual-interface | 1 | Use the procedure *Flip to dual-interface configuration* |

### 5.4.5 Managing the detection engine

Table1: Basic functions

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Display advanced options | 1 | Use the command *show monitoring-engine* |
| Apply an advanced configuration | 1 | Use the command *set monitoring-engine* |
| Start the detection engine | 1 | Use the command *monitoring-engine start* |
| Stop the detection engine | 1 | Use the command *monitoring-engine stop* |
| Display the detection engine status | 1 | Use the command *monitoring-engine status* |
| Traffic generation: replaying a pcap file | 1 | Use the command *replay* |

### 5.4.6 Managing servers

| To perform the following task | # | Carry out the following procedures in succession |
|---|---|---|
| Exit the current session or leave the SSH session | 1 | Use the command *exit* |
| System: restart the GCap | 1 | Use the command *system restart* |
| System: shut down the GCap | 1 | Use the command *system shutdown* |

### 5.4.7 Monitoring the GCAP

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

## 5.5 List of procedures

### 5.5.1 Configuring the GCap for the first connection

#### 5.5.1.1 Introduction

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

#### 5.5.1.2 Prerequisites

- **User:** setup

#### 5.5.1.3 Preliminary operations

- 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

- Connect to the GCap.
- Depending on the situation:
  - Either connect directly to the GCap via keyboard and screen (see *Procedure for connecting directly to the GCap*)
  - Or connect to the GCap via the iDRAC (see *Procedure for connecting to the GCap via the iDRAC*)
- 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).

---

#### 5.5.1.4 Procedure

- Manage passwords (passwords, SSH keys, and the like): see the *Manage accounts* table.
- Manage network interfaces with `Tunnel` (`gcp0`) and `Management` (`gcp1`) roles: see the *Manage network* table.
  - Configure the IP addressing
  - Enter the GCap name and the domain name
  - Configure the MTU value if necessary
    To do this, see the *Procedure for managing the network parameters of the `Tunnel` and `Management` interfaces*.
- Connect to the GCap via a remote connection through an SSH tunnel (see *Procedure for remote connection to GCap via an SSH tunnel*).
- Set the operating mode for the SSH link to single-interface or dual-interface
  To do this, see the *Procedure for switching to single-interface configuration* or the *Procedure for switching to dual-interface configuration*.
- Manage the GCap date and time, refer to the *Procedure for changing the GCap date and time*.
- Manage the capture interfaces: see the *Manage network* table.
  - Activate the desired interfaces
  - Configure the MTU value
    To do this, see the *Procedure for managing capture interface settings `monx`*.
- If needed, manage the aggregation of detection interfaces: see the *Procedure for managing the aggregation of capture interfaces*.
- If needed, manage the high availability of GCaps: see *Procedure for managing the high availability of GCaps*.
- Pairing the GCap with the GCenter: see the *Procedure for pairing a GCap with a GCenter*.
  - On the GCenter,
    - Connect via an SSH
    - Know the GCenter IP address
  - 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
- Put the GCap into operation: see the *Procedure for putting a GCap into operation*.

---

### 5.5.2 Starting up a GCap

#### 5.5.2.1 Introduction

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

---

#### 5.5.2.2 Prerequisites

- **User:** setup

---

#### 5.5.2.3 Preliminary operations

- Perform the *Procedure for connecting to the GCap for the first time*.
- Activate the required `monx` capture interfaces: see *Procedure for managing `monx` capture interface settings*.

---

#### 5.5.2.4 Procedure to be followed on the GCap

- Starting the detection engine: see the *Managing 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.
- Enter the following command.

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

- Validate.
- Wait for the engine to be up and running.
- 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 running.

---

#### 5.5.2.5 Procedure to be carried out on the GCenter

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

---

### 5.5.3 Direct connection to the GCap with keyboard and monitor

#### 5.5.3.1 Introduction

The first connection to the GCap can be done by a direct connection with a keyboard and monitor.
This is necessary if the network configuration is not yet completed on the GCap or if the network address is not known.

---

#### 5.5.3.2 Preliminary operations

- Connect the GCap power cables.
- Connect the network cables of the GCap (*see section Description / The GCap*).

---

#### 5.5.3.3 Procedure for connecting the screen and keyboard

- Connect the screen to the VGA connector of the GCap.
- Connect the keyboard to the USB connector of the GCap.
- Switch on the server.

---

#### 5.5.3.4 Procedure for obtaining the network settings via the BIOS

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

---

#### 5.5.3.5 Procedure for accessing the CLI

The command prompt is displayed:

```
gcap-protor login:
```

- Enter the login and the corresponding password.
  The following 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 **Enter** to display all available commands along with a short explanation.

**Astuce:**

- 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.

### 5.5.4 Remote connection to the iDRAC in HTTP (DELL server)

#### 5.5.4.1 Introduction

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 connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password of iDRAC

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

**Astuce:**

- 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.

#### 5.5.4.2 Preliminary operations

- Perform the network configuration (IP address of the iDRAC): otherwise, use the *Procedure for direct connection to the GCap* to connect to the GCap.

#### 5.5.4.3 Procedure

- On the remote PC, open a web browser.
- Enter the IP address of the GCap iDRAC interface and confirm.
  The `Login` window is displayed.
- Enter the requested parameters:
  - `Username`: login name
  - `Password`: password of the entered login
  - `Domain`: select `This IDRA`
- Click on the `Submit` button.
- Launch the virtual console (`Virtual console Preview` zone, `Lanch` button).
  Following this action, a new page will open. It will be possible to interact with the GCap.
- 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 **Enter** to display all available commands along with a short explanation.

---

#### 5.5.4.4 Special cases

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

- Enter the command

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

- Validate
  The system:
  - Opens the SSH connection
  - Executes the command (here `show status`)
  - 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 x.x.x.x closed
```

---

### 5.5.5 Remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode

#### 5.5.5.1 Introduction

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 connection is not the normal way to access the GCap but enables access to the GCap in the event of problems.
To carry out this procedure, it is necessary:

- That the iDRAC has an accessible IP in order to be able to connect to it
- To know the login name and password of iDRAC

From the interface, it is possible to:

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

**Astuce:**

- 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.

---

#### 5.5.5.2 Preliminary operations

- Perform the network configuration (IP address of the iDRAC).
  Otherwise, use the *Procedure for direct connection to the GCap* to connect to the GCap.

---

#### 5.5.5.3 Procedure

- On the remote PC running Linux:
  - Open a command prompt
  - Enter the `ssh identifiant@adresse_ip` command
    For example, `ssh setup@x.x.x.x` where
    - `setup` is the ID and
    - x.x.x.x is the IP address of the GCap's iDRAC port.
  - Validate the command
  - Enter password of the entered login
  - Press **Enter** to display all available commands and a short explanation
- On a Windows PC:
  - Open an SSH client software, such as Putty
  - Enter the IP address of the iDRAC interface of the GCap then validate
- Enter the following command `racadm>>console com2`.
- 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.
- 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 **Enter** to display all available commands along with a short explanation.

---

#### 5.5.5.4 Special cases

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

- Enter the command

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

- Validate
  The system:
  - Opens the SSH connection
  - Executes the command (here `show status`)
  - 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 x.x.x.x closed.
```

---

### 5.5.6 Remote connection to GCap via an SSH tunnel

#### 5.5.6.1 Introduction

This procedure describes how to connect from a remote PC securely using an SSH tunnel.

**Astuce:**

- 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.

---

#### 5.5.6.2 Preliminary operations

- Make an initial connection to the GCap (see *Procedure for direct connection to GCap*).
- Learn the name of the GCap or its IP address (see *Procedure for viewing network Tunneland Management interface settings* ).

---

#### 5.5.6.3 Procedure

- On the remote PC running Linux:
  - Open a command prompt
  - Enter the `ssh identifiant@adresse_ip_GCap` or `ssh identifiant@FQDN_GCap` command
    For example, `ssh setup@gcap` where:
    - The identifier is `setup` and
    - The FQDN is `gcap`
  - Validate the command
  - Enter password of the entered login
- On a Windows PC:
  - Open an SSH client software, such as Putty
  - Enter the IP address of the interface 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 along with a short explanation.

---

### 5.5.7 Connection to the GCenter via a web browser

#### 5.5.7.1 Introduction

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

---

#### 5.5.7.2 Preliminary operations

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

---

#### 5.5.7.3 Procedure

On the remote PC:

- Open a web browser.
- 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`*
- Validate.
  The GCenter login window is displayed.
  - Enter the login name.
  - Enter the password.
  - Validate.

  The GCenter graphical interface is displayed.

**Note:**

Refer to the GCenter documentation for its use.

### 5.5.8 Changing the GCap date and time

#### 5.5.8.1 Introduction

Before pairing the GCap and GCenter, it is important to ensure that both systems are in sync in terms of time.
Once the pairing is complete, the GCenter acts as an NTP server for the GCap to ensure that the equipment clocks are synchronised.
When connecting for the first time, these items must be set via the *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, it is the time of the GCap that must be changed.

---

#### 5.5.8.2 Prerequisites

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

---

#### 5.5.8.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
- Connect as a **setup**.

---

#### 5.5.8.4 Procedure for viewing the date and time on the GCap and GCenter

- Enter the `show datetime` command then validate.
  The `datetime` command of the `show` subgroup enables displaying the date and time of the GCap in the format YYYY-MM-DD HH:MM:SS.

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

- Log in to the GCenter.
- 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.

---

#### 5.5.8.5 Procedure for changing the date and time of the GCap

- Enter the command *set datetime* 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)

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

- Validate.
  A confirmation window is displayed.

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

---

### 5.5.9 Managing the network parameters of Tunnel and Management interfaces

#### 5.5.9.1 Introduction

This procedure describes:

- Viewing the network settings
- Modifying these parameters.

| To... | Use the command | described in the procedure |
|---|---|---|
| obtain an overview of the information on all network interfaces | *show network-config configuration* | Procedure A |
| display for each interface: MAC address, carrier presence, speed, and type of connection | *show interfaces* | Procedure B |
| display or change the domain name | *show network-config domain* or *set network-config domain* | Procedure C |
| display or change the system name | *show network-config hostname* or *set network-config hostname* | Procedure D |
| display or modify the interface used in SSH for administering the GCap and the GCap GCenter link | *show interfaces* or *set interfaces assign-role* | Procedure E |
| display or modify the MTU value of the interfaces | *show interfaces* or *set advanced-configuration mtu* | Procedure F |
| display or modify the TCP/IP settings of the Management / Tunnel interfaces | *show network-config gcp0* | Procedure G |

#### 5.5.9.2 Prerequisites

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

#### 5.5.9.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
- Stop the detection engine (see *monitoring-engine*).

#### 5.5.9.4 Procedure A: Display the network configuration

- Enter the `show network-config configuration` command then 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 the `monx` capture interfaces, refer to the *Procedure for managing 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

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

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

**Note:**

The configuration in the above example is dual interface.

---

#### 5.5.9.5 Procedure B: display the status of the GCap network interfaces

- Enter the following command.

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

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

---

#### 5.5.9.6 Procedure C : display/change the GCap domain name

- To display the current name:
  - Enter the following command.

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

  - Validate.
    The system displays the domain name.

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

- To change the current name:
  - Enter the following command.

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

  - 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)
```

  - Press **y** and then confirm.

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

- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the domain name.

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

---

#### 5.5.9.7 Procedure D: display or change the GCap name

- To display the current name:
  - Enter the following command.

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

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

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

- To change the current name:
  - Enter the following command.

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

  - Validate.

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

  - Press **y** and then confirm

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

- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the host name of the GCap.

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

---

#### 5.5.9.8 Procedure E: display or modify the interface used to manage the GCap in SSH

- To display the current configuration:
  - Enter the following command.

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

  - Validate.
    The system displays the role of the different interface of GCap (for SSH connection `management`, for IPSec tunnel: `tunnel`, for both: `management-tunnel` ).
    * 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 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 |

- To configure the `enpXXXX` interface for SSH and the `enpYYYY` interface for IPSec:
  - Enter the following command.

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

  - Validate.
    * Enter the following command.

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

  - Validate.
  - Enter the following command.

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

  - Validate.
  - Enter the following command.

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

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

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

  - Enter the following command.

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

  - Validate.
  - Enter the following command.

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

  - Validate.

#### 5.5.9.9 Procedure F: display or change the MTU value

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

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

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

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

  - Validate.
    The system displays the result.

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

---

#### 5.5.9.10 Procedure G: display or modify the TCP/IP settings of a `management` and/or `tunnel` interface

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

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

  - Validate.

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

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

- To change the configuration of the `management` interface address:
  - Enter the following command.

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

  - Validate.
    The system displaying the `management` interface configuration.

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

– Press **y** and then confirm.

---

## 5.5.10 Managing capture interface settings `monx`

### 5.5.10.1 Introduction

This procedure describes:

- Viewing the network settings
- Modifying these parameters

| To... | Use the command | described in the procedure |
|---|---|---|
| obtain an overview of the information on all network interfaces | *show interfaces* | Procedure A |
| display the MTU value of the interfaces | *show interfaces* | Procedure B |
| modify the MTU value of the interfaces | *set advanced-configuration mtu* | Procedure B |
| display the available detection interfaces | *show interfaces* | Procedure C |
| manage the available detection interfaces | *set interfaces* | Procedure C |

---

### 5.5.10.2 Prerequisites

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

---

### 5.5.10.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
- Stop the detection engine (see *monitoring-engine*).

---

#### 5.5.10.4 Procedure A: Display the network configuration

- Enter the following command.

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

- 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** ).

---

#### 5.5.10.5 Procedure B: display or change the MTU value

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

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

  - 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 )
```

- In our example, to change the current configuration of enabled interfaces: e.g. to change the MTU value of the `mon0` interface
  - Enter the following command.

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

  - Validate.
    The system displays the result.

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

---

#### 5.5.10.6 Procedure C: display or change the available detection interfaces

- To display the information on the detection interfaces:
  - Enter the following command.

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

  - Validate.
    The system displays the available detection 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 Device ID of the network card
- `PCI bus`: PCI bus number used by the network card
- In our example, mon0, mon1 and mon2 are enabled ( field: **role**, value : **capture** ).
- To activate an interface (here enp27s0 for example):
  - Enter the following command.

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

  - Validate.
  - then to check the new configuration

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

  - Validate.
    The system displays the available detection 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
```

- To deactivate an interface (here mon0 for example):
  - Enter the following command.

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

  - Validate.
- To change the interface start-up delay by five seconds for example
  - Enter the following command.

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

– Validate.

---

### 5.5.11 Switching to a single-interface configuration

#### 5.5.11.1 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

---

#### 5.5.11.2 Prerequisites

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

---

#### 5.5.11.3 Preliminary operations

- As appropriate, refer to:
  - The *Procedure for direct connection to the GCap*
  - The *Procedure for remote HTTP connection to iDRAC*
  - The *Procedure for remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
- Stop the detection engine (see *monitoring-engine*)

---

#### 5.5.11.4 Procedure for displaying the current configuration

- To display the `management` and ```tunnel``` interfaces configuration:
  - Enter the following command.

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

  - Validate.
    The system displaying the `management` and `tunnel` interfaces configuration.
    * **Single-interface configuration**
      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.
    * **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.

---

#### 5.5.11.5 Procedure for switching from dual to single interface configuration

- First of all, use the following command to unpair the GCap:

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

- If you want to use the same IP configuration as the interface with `management` role:
  - Enter the following command to disable the configuration of current `tunnel` interface:

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

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

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

  - Validate.
- If you want to use another IP configuration than the interface with `management` role:
  - Enter the following command to reconfigure the management interface:

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

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

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

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

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

– Validate.

**Note:**

If you want to apply the IP configuration of current tunnel interface to current management interface, you need to configure current tunnel interface with another network configuration before configuring the management interface.

- 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.

---

## 5.5.12 Switching to a dual-interface configuration

### 5.5.12.1 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

---

#### 5.5.12.2 Prerequisites

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

---

#### 5.5.12.3 Preliminary operations

- As appropriate, refer to:
  - The *Procedure for direct connection to the GCap*
  - The *Procedure for remote HTTP connection to iDRAC*
  - The *Procedure for remote connection to the CLI using SSH via the iDRAC interface in serial port forwarding mode*
- Stop the detection engine (see *monitoring-engine*).

---

#### 5.5.12.4 Procedure for displaying the current configuration

- To display the `management` and ```tunnel``` interfaces configuration:
  - Enter the following command.

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

  - Validate.
    The system displaying the `management` and ```tunnel``` interfaces configuration.
    - **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.
    - **Single-interface configuration**
      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 this example, the current configuration is single-interface ( field: role, value : management-tunnel )**
      In this case, continue with the following procedure.

---

#### 5.5.12.5 Procedure for switching from single to dual interface configuration

- Use the following command to unpair the GCap:

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

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

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

- Validate.
- Enter the following command to configure the selected interface with the role `tunnel` :

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

- Validate.
- Enter the following command the IP configuration of tunnel interface:

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

- Validate.
- Rewire the GCap network cables if necessary.

---

### 5.5.13 Managing capture interface aggregation

#### 5.5.13.1 Introduction

This procedure describes the aggregation of capture interfaces.
For more information on aggregation, see the paragraph *Capture and monitoring interfaces monx between TAP and GCap: aggregation possibility*.
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.
  *MTU*: uses the largest value of the interfaces making 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: When enabling interface aggregation and multi-tenant detection, file rebuild rules are not generated.

To create an aggregation of two interfaces, use the *set interfaces assign-role* command.

---

#### 5.5.13.2 Prerequisites

- **User:** setup
- **Commands used in this procedure:**
  - *show interfaces*
  - *set interfaces assign-role*

---

#### 5.5.13.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
- Stop the detection engine (see *monitoring-engine*).

---

#### 5.5.13.4 Procedure for displaying the aggregation of capture interfaces

- Enter the `show interfaces` command then 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.

---

#### 5.5.13.5 Procedure to create an interface aggregation

- In our case, we are going to create a cluster with `enp4s0` and `enp12s0`.
- Enter the following commands.

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

- Validate.

---

#### 5.5.13.6 Procedure for displaying the created aggregation

- Enter the following command.

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

- Validate.
  The system displays the following information:

```
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`.

---

## 5.5.14 Pairing between a GCap and a GCenter

### 5.5.14.1 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

---

### 5.5.14.2 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*

---

### 5.5.14.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
- Know the FQDN of the GCap and its IP address.
- Know the FQDN of the GCenter and its IP address.
- Check that the date and time of the GCenter and the GCap match: refer to the *Procedure for modifying the GCap date and time*.

---

#### 5.5.14.4 Procedure for displaying the IP address of the GCenter

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

---

#### 5.5.14.5 Procedure for setting the compatibility mode on the GCap

- 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).
- To display the current compatibility mode between the GCap and the GCenter:
  - Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
  - Enter the following command.

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

  - Validate.
    The system displays the current compatibility mode.

```
Current compatibility mode: 2.5.3.101
```

  - Compare the version between the one displayed on the GCap and the one on the GCenter.
    In this example:
    - 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.
- To change the GCap compatibility mode:
  - Enter the following command (for example for version 2.5.3.102).

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

  - Validate.

---

#### 5.5.14.6 Procedure for setting the GCenter IP on the GCap

- To display the current version of the GCenter IP:
  - Connect to the GCap (see *Procedure for connecting to the GCap via SSH*).
  - Enter the following command.

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

  - 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: X.X.X.X
```

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

```
Current GCenter IP: None
```

  - Check that the IP address displayed is that of the GCenter to be paired. If there is a change, continue this procedure.
- To change the current version of the GCenter IP:
  - Enter the *set gcenter-ip* command followed by the GCenter IP setting.
    Example: set gcenter-ip 10.2.10.234

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

```
Setting GCenter IP to 10.2.19.218
```

---

#### 5.5.14.7 Procedure for declaring the GCap in the GCenter

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

---

#### 5.5.14.8 Procedure for pairing the GCap and the GCenter

- Log on to the GCap CLI.
- Enter the following command.

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

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

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

- 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
e655bc02553e2291a486a32bdce3943a315f830de70b2c627c39884e80
0f08b2. Is it correct? (y/N)
```

- 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, answer **Y** and validate.

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

- 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.
On the GCap, this information is visible with the `show status` command.

```
(gcap-cli) show status

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

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

  © Copyright GATEWATCHER 2024
```

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

---

#### 5.5.14.9 Procedure for remove the pairing between a GCap and the GCenter

- Log on to the GCap CLI.
- Enter the following command.

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

- Validate.

---

### 5.5.15 Managing the high availability of GCaps

**Note:**

**This feature is deprecated**
Please contact Gatewatcher if you want to deploy a redundant architecture.

---

### 5.5.16 Optimising performance

#### 5.5.16.1 Introduction

Performance optimisation 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 the Procedure for adjusting the size of the captured packet.
  - 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 datasheets.

- **Subject 2: optimising 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 using a TAP aggregator is preferable because it requires the least amount of GCap resources for the same flow.
- **Subject 3: optimising the network flow to be analysed**
  - One or more CPUs are being overloaded because there are too many packets being analysed.
    - To reduce the size of the captured network, it is possible to suppress the unnecessarily analysed 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, another rule can be defined or, more likely, an existing rule can be modified.
      A flow was defined but it was too large. It must therefore be subdivided so that each part is analysed by several CPUs.
    - To modify the rules, see the procedure for defining static packet filtering rules.
  - Change the analysed protocols.
    - To modify this list, this action must be performed on the paired GCenter.
      See the GCenter documentation for more information.
- **Subject 4: optimising the detection engine rules**
  The rules define:
  - Detection rules
  - File rebuilding rules
  - Rules defining thresholds or limits under the threshold heading

  See 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'.

---

#### 5.5.16.2 Prerequisites

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

---

#### 5.5.16.3 Preliminary operations

- Connect to the GCap (see *Procedure for connecting to the GCap via SSH*)
- Stop the detection engine (see *monitoring-engine*)

---

#### 5.5.16.4 Procedure for adjusting 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.

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

---

#### 5.5.16.5 Procedure for defining flow filtering rules

**Astuce:**

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

- To view the number of dropped packets per CPU core, use the *show health* command, sofnet-Statistics counter details on received packets by CPU core.

  Certain parts of the captured flow cannot be detected or reconstructed: for example, encrypted flows.
- If nothing is done, the system will monopolise resources to achieve a result known in advance.

  To avoid this, it is possible to create rules to filter the flow to be captured.

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

---

# Chapter 6

# CLI

## 6.1 Overview of the CLI

### 6.1.1 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.

---

### 6.1.2 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` set

---

### 6.1.3 Accessible commands grouped by set

The commands are grouped by set (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 commands depends on:

- The current user type
- 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

... then the command is not recognised and the message `` `Command `X` is not recognised` `` is displayed.

**Note:**

User type or context elements are specified where necessary.

---

### 6.1.4 Directly accessible commands

The commands below are directly accessible:

| Use the command... | to... |
|---|---|
| *monitoring engine* | manage the detection engine |
| *pairing* | pairing the GCap and GCenter |
| *unpair* | pairing the GCap and GCenter |
| *help* | obtain help with the available commands |
| *colour* | enable or disable colours for the current CLI session |
| *exit* | return to the root of the CLI or exit the CLI |

---

### 6.1.5 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`:

```
(gcap-cli) set keymap

fr us
```

---

### 6.1.6 Navigating in the command tree

#### 6.1.6.1 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)
```

- Enter the `show` command.

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

The prompt changes to inform the user that the set has changed.
Now the commands of set `show` 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 set `show`.

---

#### 6.1.6.2 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 set are accessible.

- Enter 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 sets are accessible.
  The **CTRL** + **D** shortcut enables calling the `exit`command.

---

### 6.1.7 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

---

#### 6.1.7.1 Example of launching from the root for the `show interfaces` command

```
(gcap-cli)
```

- Enter the `show interfaces` command then validate.

---

#### 6.1.7.2 Example of launching the `show interfaces` command from the `show` set

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

- Enter the `interfaces` command then validate.

---

### 6.1.8 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*.

---

### 6.1.9 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 command, see the paragraph on *exit*.

---

## 6.2 cli

### 6.2.1 show

#### 6.2.1.1 alerts

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.2 bruteforce-protection

##### 6.2.1.2.1 Introduction

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

---

##### 6.2.1.2.2 Prerequisites

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

---

#### 6.2.1.2.3 Command

```
show bruteforce-protection
```

---

#### 6.2.1.2.4 Example for showing the current system policy for protecting against brute force attacks

- Enter the following command.

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

- 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`).

---

### 6.2.1.3 bypassed-flows

This command has been removed since version 2.5.3.105.

---

### 6.2.1.4 clusters

This command has been removed since version 2.5.4.0.

---

### 6.2.1.5 compatibility-mode

#### 6.2.1.5.1 Introduction

The `compatibility-mode` command of the `show` subgroup 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, refer to the *compatibility table*.

**Note:**

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

---

#### 6.2.1.5.2 Prerequisites

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

---

#### 6.2.1.5.3 Command

```
show compatibility-mode
```

---

#### 6.2.1.5.4 Example for displaying the current compatibility mode

- Enter the following command.

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

- Validate.
  The system displays the current compatibility mode.

```
Current compatibility mode: 2.5.3.102
```

---

### 6.2.1.6 config-files

This command has been removed since version 2.5.4.0.

---

### 6.2.1.7 datetime

#### 6.2.1.7.1 Introduction

The `datetime` command of the `show` subgroup enables the date and time of the GCap to be displayed in `YYYY-MM-DD HH:MM:SS` format.

---

#### 6.2.1.7.2 Prerequisites

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

---

#### 6.2.1.7.3 Command

`show datetime`

---

#### 6.2.1.7.4 Example of displaying the date and time of the GCap

- Enter the following command.

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

- Validate.
  The system displays the current information.

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

---

### 6.2.1.8 eve-stats

#### 6.2.1.8.1 Introduction

The `eve-stats` command of the `show` subgroup enables displaying the Sigflow (*monitoring-engine*) statistics.

---

#### 6.2.1.8.2 Prerequisites

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

---

#### 6.2.1.8.3 Command

`show eve-stats`

---

#### 6.2.1.8.4 Example

- Enter the following command.

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

- Validate.
  The system displays the following information:
  - counter `Alerts` - Number of Sigflow alerts found
  - counters `Files` - Files extracted by Sigflow
  - counters `Codebreaker samples` - Files analysed by the motor which detects shellcodes or powershells
  - counters `Protocols` - List of protocols seen by Sigflow
  - counters `Detection Engine Stats` - Sigflow statistics (*monitoring-engine*)

---

#### 6.2.1.8.4.1 Counter `Alerts` details - Number of Sigflow alerts found

Example:

```
Alerts: 0
```

---

#### 6.2.1.8.4.2 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
```

---

#### 6.2.1.8.4.3 Counter `Codebreaker samples` 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**

---

#### 6.2.1.8.4.4 Detail of counters `Protocols` - List 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:  0
```

#### 6.2.1.8.4.5 Detail of counters `Detection Engine Stats` - Sigflow statistics (*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

  Example :

```
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).

---

#### 6.2.1.9 gcenter-ip

##### 6.2.1.9.1 Introduction

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

---

#### 6.2.1.9.2 Prerequisites

- **User:** setup
- **Dependencies:**
  - The detection engine must be switched off
  - A GCenter must be paired

---

#### 6.2.1.9.3 Command

```
show gcenter-ip
```

---

#### 6.2.1.9.4 Example

- Enter the following command.

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

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

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

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

```
Current GCenter IP: None
```

---

### 6.2.1.10 health

#### 6.2.1.10.1 Introduction

The `health` command of the `show` subgroup enables displaying statistics and the health information of the GCap.

---

#### 6.2.1.10.2 Prerequisites

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

---

#### 6.2.1.10.3 Command

```
show health
```

---

#### 6.2.1.10.4 Example

- Enter the following command.

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

- 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 statistics
  - `quotas` counters - Quota Information
  - `sofnet` counters - Statistics on received packets according to processor cores
  - `suricata` counters - Sigflow (*monitoring-engine*) information
  - `systemd` counters - System initialisation information
  - `uptime` counters - Uptime
  - `virtualmemory` counters - Swap space information (*swap*)

---

##### 6.2.1.10.4.1 `block` counters details - 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
    }
},
```


---

#### 6.2.1.10.4.2 `cpu_stats` counter details - 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
},
```

#### 6.2.1.10.4.3 `disks` counters details - 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,
        "inode_total": 1827840
    },
},
```

---

#### 6.2.1.10.4.4 `emergency` Counters details - GCap emergency mode information

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

Example:

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

---

#### 6.2.1.10.4.5 `gcenter` Counters details - Paired GCenter information

- `chronyc_sync` - Status of the NTP synchronisation with the GCenter
- `reachable` - GCenter reachable or not (false)

Example:

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

---

#### 6.2.1.10.4.6 `high_availability` counters details - 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
},
```

---

#### 6.2.1.10.4.7 `interfaces` counter details - Statistics on network interfaces

- `bond0` - Name of the network interface
  - `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": {
    "bond0": {
        "rx_bytes": 0,
        "rx_drops": 0,
        "rx_errs": 0,
        "rx_packets": 0,
        "tx_bytes": 0,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    },
    "gcp0": {
        "rx_bytes": 138433006,
        "rx_drops": 82901,
        "rx_errs": 0,
        "rx_packets": 2143236,
        "tx_bytes": 796294,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 3635
    },
    "gcp1": {
```

(suite sur la page suivante)

(suite de la page précédente)

```
        "rx_bytes": 137642525,
        "rx_drops": 82902,
        "rx_errs": 0,
        "rx_packets": 2135060,
        "tx_bytes": 0,
        "tx_drops": 0,
        "tx_errs": 0,
        "tx_packets": 0
    }
},
```

#### 6.2.1.10.4.8 `loadavg` counter details - 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
},
```

#### 6.2.1.10.4.9 `meminfo` counter details - Statistics on the RAM

- `available` - Total physical memory in kilobytes
- `buffers` - Memory used by disk operations in kilobytes
- `cached` - Memory used by the cache in kilobytes
- `dirty` - Memory used by pending write operations in kilobytes
- `free` - Unused memory in kilobytes
- `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 kilobytes
- `page_tables` - Memory used for page management in kilobytes
- `s_reclaimable` - Cache memory that can be reallocated in case of memory shortage in kilobytes
- `shmem` - Memory used by shared pages in kilobytes
- `slab` - Memory used by kernel data structures in kilobytes
- `swap_cached` - Memory used by the swap cache in kilobytes
- `swap_free` - Available memory in swap in kilobytes
- `swap_total` - Total swap memory in kilobytes
- `total` - Total memory in kilobytes

- `v_malloc_used` - Memory used by large memory areas allocated by the kernel
  For more information, please refer to this documentation `meminfo`.

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
},
```


#### 6.2.1.10.4.10 `numastat` counter details- Non Uniform Memory Access (NUMA) node statistics

- `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,
```


(suite sur la page suivante)

(suite de la page précédente)

```
            "numa_foreign": 0,
            "numa_hit": 4224964539,
            "numa_miss": 0,
            "other_node": 21531
        }
    }
},
```

#### 6.2.1.10.4.11 quotas counter details- 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

Exemple :

```
"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"
```

(suite sur la page suivante)

(suite de la page précédente)


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


(suite sur la page suivante)

(suite de la page précédente)

```
            },
        }
    }
```

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"
    },
```

#### 6.2.1.10.4.12 `sofnet` counter details - 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 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 budget

Example:

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

(suite sur la page suivante)

(suite de la page précédente)


```
            "processed": 36250,
            "received_rps": 0,
            "time_squeeze": 0
        }
    },
    "summed": {
        "backlog_len": 0,
        "dropped": 0,
        "flow_limit_count": 0,
        "processed": 5239450,
        "received_rps": 0,
        "time_squeeze": 27
    }
},
```


#### 6.2.1.10.4.13 `Sigflow` counter details - 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
    },
```


#### 6.2.1.10.4.14 `systemd` counter details - System initialisation information

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

Example:


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

#### 6.2.1.10.4.15 `uptime` counter details - Uptime

- `up_seconds` - Number of seconds since start-up.

Example:

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

---

#### 6.2.1.10.4.16 `virtualmemory` counter details - Swap space information (*swap*)

- `disk_in`: Number of pages saved to disk since start-up.
- `disk_out` - Number of pages out of disk since start-up.
- `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 kilobytes the system swapped from disk to RAM per second.
- `swap_out` - Number of kilobytes 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
}
```

---

### 6.2.1.11 interfaces

#### 6.2.1.11.1 Introduction

The `interfaces` command of the `show` subgroup enables displaying the GCap network interfaces:

- The management interfaces ( formerly `gcp0` and `gcp1`)
- The detection 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 monitoring 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 monitoring interfaces, **tunnel** for IPSec connections, **management** for SSH connections, **management-tunnel** for SSH and IPSec connections, **capture-cluster** for monitoring interfaces in cluster mode, **inactive** for disable 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 Device ID of the network card

- **PCI bus**: PCI bus number used by the network card

---

#### 6.2.1.11.2 Prerequisites

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

---

#### 6.2.1.11.3 Commands

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

---

#### 6.2.1.11.4 Example of displaying the available capture interfaces

- Enter the following command.

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

- 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.

---

#### 6.2.1.11.5 Example of displaying the grace period given to start up the interfaces

- Enter the following command.

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

- Validate.
  The system displays the grace period for starting up the interfaces.

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

---

#### 6.2.1.12 keymap

##### 6.2.1.12.1 Introduction

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

---

##### 6.2.1.12.2 Prerequisites

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

---

##### 6.2.1.12.3 Command

```
show keymap
```

---

##### 6.2.1.12.4 Example of displaying the current keyboard language

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

- Validate.
  The system displays the current information.
  Example :

  ```
  Current keymap is fr
  ```

---

#### 6.2.1.13 logs

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.14 monitoring-engine

##### 6.2.1.14.1 Introduction

The `monitoring-engine` command of the `show` subgroup 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

---

#### 6.2.1.14.2 Prerequisites

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

---

#### 6.2.1.14.3 Command

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

---

#### 6.2.1.14.4 Example of displaying the default value of the start-timeout

- Enter the following command.

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

- Validate.
  The system displays the current value.

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

---

#### 6.2.1.14.5 Example of displaying the default value of the stop-timeout

- Enter the following command.

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

- Validate.
  The system displays the current value.

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

---

#### 6.2.1.14.6 Example of displaying the status of the verification check

- Enter the following command.

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

- 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.

---

#### 6.2.1.15 network-config

##### 6.2.1.15.1 Introduction

The GCap includes:

- Capture and monitoring interfaces.
- Network interfaces for managing the probe via SSH and for pairing with the GCenter.

Two cases are possible:

- **Single-interface configuration**
  SSH connection for GCap management and VPN communication are managed through one interface (formerly `gcp0`).
- **dual-interface configuration**
  The VPN communication is controlled by the one interface (formerly `gcp0`).
  The SSH connection for GCap management is handled by another interface (formerly `gcp1`).

For more information on network interfaces, refer to the *GCap input / output description* section.
The `network-config` command of the `show` subgroup enables displaying:

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

---

##### 6.2.1.15.2 Prerequisites

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

---

##### 6.2.1.15.3 Commands

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

---

##### 6.2.1.15.4 Example of displaying the GCap configuration

- Enter the following command.

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

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

---

#### 6.2.1.15.4.1 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
    },
    "enp27s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "monvirt": {
        "filtering_rules": {},
        "mtu": 1500
    }
}
```

#### 6.2.1.15.4.2 Dual-interface configuration

In this case, the system displays the configuration information.

```
(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": {
```

(suite sur la page suivante)

(suite de la page précédente)


```
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp20s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "enp27s0": {
        "filtering_rules": {},
        "mtu": 1500
    },
    "monvirt": {
        "filtering_rules": {},
        "mtu": 1500
    }
}
```


#### 6.2.1.15.5 Example of displaying the GCap domain

- Enter the following command.

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

- Validate.
  The system displays the domain name.

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

#### 6.2.1.15.6 Example of displaying the `management` interface configuration

- Enter the following command.

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

- Validate.
  The system displaying the `management` interface configuration.
  For example:

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

#### 6.2.1.15.7 Example of displaying the `tunnel` interface configuration

- Enter the following command.

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

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

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

---

#### 6.2.1.15.8 Example of displaying the host name of the GCap

- Enter the following command.

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

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

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

---

### 6.2.1.16 password-policy

#### 6.2.1.16.1 Introduction

The `password-policy` command in subgroup `show` 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.

---

#### 6.2.1.16.2 Prerequisites

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

---

#### 6.2.1.16.3 Command

```
show password-policy
```

---

#### 6.2.1.16.4 Example of displaying the default password policy

- Enter the following command.

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

- 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 | At least x different characters are required 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 |

---

### 6.2.1.17 passwords

#### 6.2.1.17.1 Introduction

The `passwords` command of the `show` subgroup enables:

- Displaying the list of users managed by the current level. This is accessible for setup, gviewadm, and gview users.
- Retrieving the root token as a text or QR code.
  This is available to setup users only.

**Note:**

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

---

#### 6.2.1.17.2 Prerequisites

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

---

#### 6.2.1.17.3 Command

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

---

#### 6.2.1.17.4 Example of displaying the list of users managed by the current level

- Enter the following command.

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

- 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
    ```

---

#### 6.2.1.17.5 Example of displaying the root token in text

- Enter the following command.

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

- Validate.
  The system displays the root token in text.

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

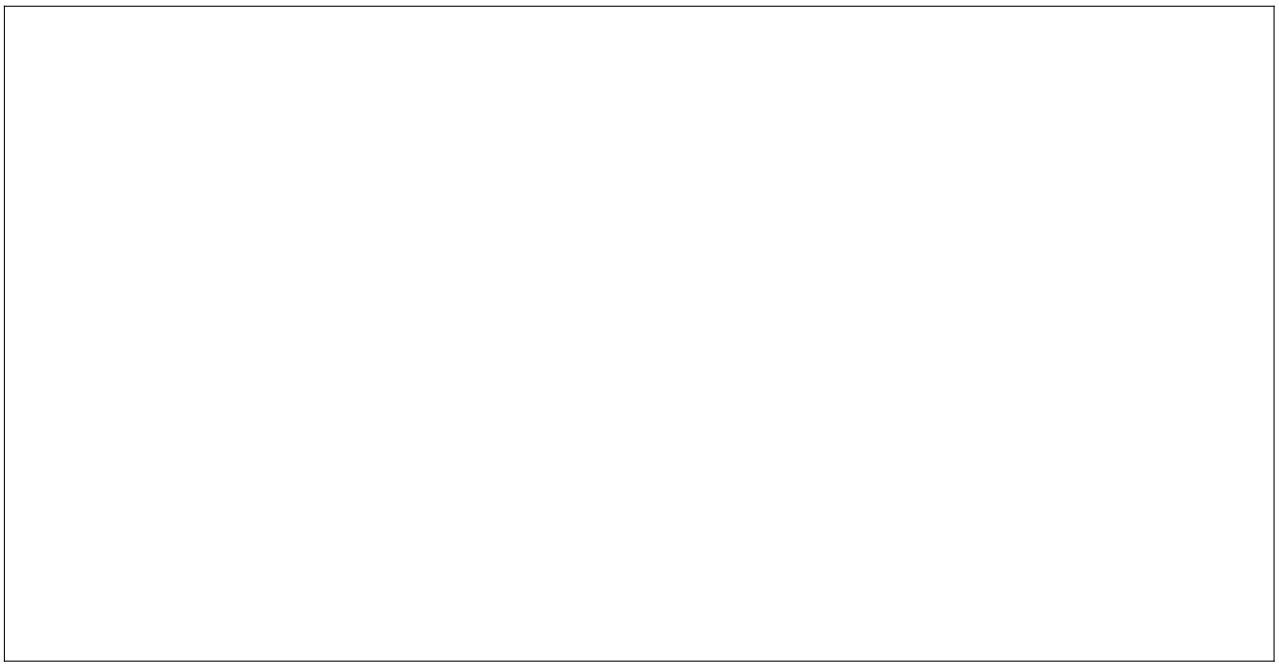
---

#### 6.2.1.17.6 Example of displaying the root token as a QR code

- Enter the following command.

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

- Validate.
  The system displays the root token as a QR code.



#### 6.2.1.18 protocols-selector

This command has been removed since version 2.5.3.105.

#### 6.2.1.19 session-timeout

##### 6.2.1.19.1 Introduction

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

##### 6.2.1.19.2 Prerequisites

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

##### 6.2.1.19.3 Command

```
show session-timeout
```

#### 6.2.1.19.4 Example of displaying the session-timeout value

- Enter the following command.

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

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

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

---

### 6.2.1.20 setup-mode

This command has been removed since version 2.5.4.0.

---

### 6.2.1.21 status

#### 6.2.1.21.1 Introduction

The `status` command of the `show` subgroup enables displaying the current GCap status.

---

#### 6.2.1.21.2 Prerequisites

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

---

#### 6.2.1.21.3 Command

```
show status
```

---

#### 6.2.1.21.4 Example of displaying the GCap information

- Enter the following command.

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

- 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 monitoring interfaces, here **mon0, mon2, mon4, monvirt**

---

#### 6.2.1.22 tech-support

##### 6.2.1.22.1 Introduction

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

**Note:**

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

---

#### 6.2.1.22.2 Prerequisites

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

---

#### 6.2.1.22.3 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..

---

##### 6.2.1.22.3.1 Command for extracting light tech-support

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

---

##### 6.2.1.22.3.2 Command for extracting standard tech-support

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

---

##### 6.2.1.22.3.3 Command for extracting heavy tech-support

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

---

### 6.2.1.23 advanced-configuration

#### 6.2.1.23.1 high availability by redundancy of 2 GCaps

This feature has been removed since version 2.5.4.0.

---

#### 6.2.1.23.2 interface-names

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.23.3 local-rules

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.23.4 memory-settings

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.23.5 MTU

This command has been removed since version 2.5.4.0.

---

#### 6.2.1.23.6 packet-filtering

##### 6.2.1.23.6.1 Introduction

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

**Note:**

Packet filtering is not supported when the MTU > 3000.

---

##### 6.2.1.23.6.2 Prerequisites

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

---

##### 6.2.1.23.6.3 Command

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

---

#### 6.2.1.23.6.4 Example of displaying the flow filtering rules

- Enter the following command.

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

- 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
```

---

## 6.2.2 set

### 6.2.2.1 bruteforce-protection

#### 6.2.2.1.1 Introduction

The `bruteforce-protection` command of the `set` subgroup 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.

---

#### 6.2.2.1.2 Prerequisites

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

---

#### 6.2.2.1.3 Commands

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

---

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

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

---

##### 6.2.2.1.3.2 Command used to set an account lockout duration in seconds (0 to deactivate)

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

---

##### 6.2.2.1.3.3 Command to restore the default configuration

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

---

#### 6.2.2.1.4 Example to change the lockout duration to 360 seconds

- Enter the following command.

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

- Validate.
  The system indicates the setting has been changed.

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

---

### 6.2.2.2 Clusters

This command has been removed since version 2.5.4.0.
For implementation, refer to the *Procedure for managing capture interface aggregation*.

---

#### 6.2.2.3 compatibility-mode

##### 6.2.2.3.1 Introduction

The `compatibility-mode` command of the `set` subgroup 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 | GCenter version | supported | Action or Order to be executed |
|---|---|---|---|
| 2.5.4.0 | 2.5.3.101 HF4 | unsupported | GCenter to migrate to a newer version |
| 2.5.4.0 | 2.5.3.102 HF3 | supported | set compatibility-mode 2.5.3.102 |
| 2.5.4.0 | 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.

---

##### 6.2.2.3.2 Prerequisites

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

---

##### 6.2.2.3.3 Command

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

---

#### 6.2.2.3.4 Example of configuring compatibility between a GCap version V2.5.4.0 with a GCenter 2.5.3.102

- Enter the following command.

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

- Validate.

---

### 6.2.2.4 datetime

#### 6.2.2.4.1 Introduction

The `datetime` command of the `set` subgroup 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, for example.

**Note:**

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

---

#### 6.2.2.4.2 Prerequisites

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

---

#### 6.2.2.4.3 Command

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

---

#### 6.2.2.4.4 Examples for changing the GCap time

- Enter the following command.

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

- Validate.
  The system displays the result.

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

---

#### 6.2.2.5 gcenter-ip

##### 6.2.2.5.1 Introduction

The `gcenter-ip` command of the `set` subgroup 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.

---

##### 6.2.2.5.2 Prerequisites

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

---

##### 6.2.2.5.3 Command

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

---

##### 6.2.2.5.4 Example

- Enter the following command.

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

- Validate.
  The system displays the result.

```
Setting GCenter IP to 192.168.1.1
```

---

#### 6.2.2.6 interfaces

##### 6.2.2.6.1 Introduction

The `interfaces` command of the `set` subgroup enables the administration of monitoring and management interfaces.
Interfaces can be physical or virtual.
Virtual interfaces enable replaying *.pcap* files directly on the GCap.

---

#### 6.2.2.6.2 Prerequisites

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

---

#### 6.2.2.6.3 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 monitoring interfaces
  - **tunnel** for IPSec connections
  - **management** for SSH connections
  - **management-tunnel** for SSH and IPSec connections
  - **capture-cluster** for monitoring interfaces in cluster mode
  - **inactive** for disable interfaces

---

#### 6.2.2.6.4 Example to change the interface start-up delay by five seconds

- Enter the following command.

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

- Validate.

---

#### 6.2.2.6.5 Example of assigning capture role to interface specific interface

- Enter the following command.

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

- 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.

---

#### 6.2.2.7 keymap

##### 6.2.2.7.1 Introduction

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

---

##### 6.2.2.7.2 Prerequisites

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

---

##### 6.2.2.7.3 Command

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

---

##### 6.2.2.7.4 Example of a French keyboard

- Enter the following command.

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

- Validate.
  The system displays the result.

```
Setting keymap to fr
```

---

##### 6.2.2.7.5 Example of an English US keyboard

- Enter the following command.

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

- Validate.
  The system displays the result.

```
Setting keymap to en
```

---

#### 6.2.2.8 monitoring-engine

##### 6.2.2.8.1 Introduction

The `monitoring-engine` command of the `set` subgroup 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.

---

##### 6.2.2.8.2 Prerequisites

- **User:** setup
- **Dependencies:** the detection engine is switched off

---

##### 6.2.2.8.3 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.

---

##### 6.2.2.8.4 Example of changing the grace period to 600 seconds when starting the engine

- To change the grace period to 600 seconds when starting the engine:
  - Enter the following command.

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

  - Validate.
- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the current value.

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

---

#### 6.2.2.8.5 Example of changing the grace period on engine shutdown to 600 seconds

- To change the grace period to 600 seconds when the engine is stopped:
  - Enter the following command.

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

  - Validate.
- To check the value modification:
  - Enter the following command.

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

- Validate.
  The system displays the current value.

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

---

#### 6.2.2.8.6 Example of disabling the capture interface verification

- To disable the capture interface verification:
  - Enter the following command.

```
(gcap-cli) set monitoring-engine disable-sanity-checks
```

  - Validate.
- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the current value.

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

---

#### 6.2.2.8.7 Example of enabling the capture interface verification

- To enable the capture interface verification:
  - Enter the following command.

```
(gcap-cli) set monitoring-engine enable-sanity-checks
```

  - Validate.
- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the current value.

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

---

#### 6.2.2.9 network-config

##### 6.2.2.9.1 Introduction

For more information on the management interfaces (formerly `gcp0`/`gcp1`) and monitoring interfaces (`mon0` to `monx`), refer to the *show network-config* command.
The `network-config` command of the `set` subgroup enables modifying the network configuration of the GCap.
The `network-config` command of the `set` subgroup 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

---

##### 6.2.2.9.2 Prerequisites

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

---

##### 6.2.2.9.3 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.

---

##### 6.2.2.9.4 Example of configuring the `tunnel` and `management` interface

- Enter the following command.

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

- Validate.
- Enter the following command.

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

- Validate.

---

#### 6.2.2.9.5 Example of configuring the Gcap in gatewatcher.com

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

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

  - 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)
```

  - Press **y** and then confirm.
- To check the value modification:
  - Enter the following command

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

  - Validate.
    The system displays the domain name.

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

---

### 6.2.2.10 password-policy

#### 6.2.2.10.1 Introduction

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

---

#### 6.2.2.10.2 Prerequisites

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

---

#### 6.2.2.10.3 Command

To set the password complexity options: `(gcap-cli) set password-policy {lowercase-optional|lowercase-required|uppercase-optional|uppercase-required|digits-optional|digits-requ`

To enable or disable the password control policy: `(gcap-cli) set password-policy {disable|enable}`

To restore the default password control policy: `(gcap-cli) set password-policy restore-default`

To specify the minimum password length: `(gcap-cli) set password-policy password-length {8-100}`

To set the length of time a password is valid: `(gcap-cli) set password-policy validity-duration {0|1-3650}`

To disallow previously used passwords: `(gcap-cli) set password-policy previous-check {0|1-1000}`

---

#### 6.2.2.10.4 Example of removing the restriction on numbers

- Enter the following command.

```
(gcap-cli) set password-policy digits-optional
```

- 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.

---

#### 6.2.2.10.5 Example of disabling the default password control policy

- To disable the default password control policy:
  - Enter the following command.

```
(gcap-cli) set password-policy disable
```

  - Validate.
    The system displays the result.

```
Rules successfully updated
```

- To check the value modification:
  - Enter the following command.

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

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

```
No active password policy
```

---

### 6.2.2.11 passwords

#### 6.2.2.11.1 Introduction

The `passwords` command of the `set` subgroup 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).

---

#### 6.2.2.11.2 Prerequisites

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

---

#### 6.2.2.11.3 Command

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

---

#### 6.2.2.11.4 Example of changing the password of the current user (here setup)

- Enter the following command.

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

- Validate.

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

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

```
New password:
```

- Enter the new password and confirm.
  The system asks you to re-enter the new password.

```
Retype new password:
```

- 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
```

---

#### 6.2.2.11.5 Example of changing the password of another user

- Enter the following command.

```
(gcap-cli) set passwords gviewadm
```

- 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:
```

- Enter the new password for the account (here gviewadm) then validate.
  The system asks you to re-enter the new password.

```
Retype new password:
```

- 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
```

---

#### 6.2.2.12 protocols-selector

This command has been removed since version 2.5.3.105.

---

#### 6.2.2.13 session-timeout

##### 6.2.2.13.1 Introduction

The `session-timeout` command of the `set` subgroup 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.

---

##### 6.2.2.13.2 Prerequisites

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

---

#### 6.2.2.13.3 Command

```
set session-timeout MINUTES
```

---

#### 6.2.2.13.4 Example of changing the default value for automatic logoff via the user setup

- To change the default value for automatic logoff via user setup:
  - Enter the following command.

```
(gcap-cli) set session-timeout 1200
```

  - Validate.
    The system displays the result.

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

- To check the value modification:
  - Enter the following command.

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

  - Validate.
    The system displays the current session-timeout value.

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

---

### 6.2.2.14 setup-mode

This command has been removed since version 2.5.4.0.

---

### 6.2.2.15 ssh-keys

#### 6.2.2.15.1 Introduction

The `ssh-keys` command of the `set` subgroup 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 or 4096
- ssh-ed25519
- ecdsa-sha2-nistp256.

---

#### 6.2.2.15.2 Prerequisites

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

---

#### 6.2.2.15.3 Command

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

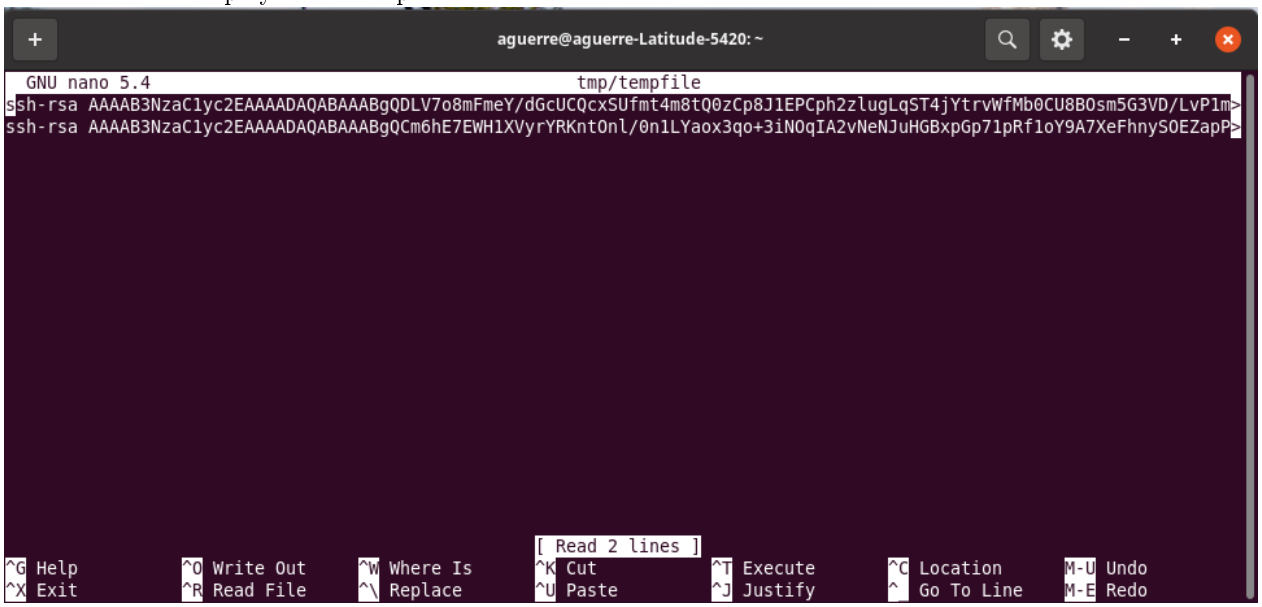
---

#### 6.2.2.15.4 Example of using the text editor

- Enter the following command.

```
(gcap-cli) set ssh-keys gview
```

- Validate.
  The text editor displays the SSH password file.




  Each line in the file is an SSH key starting with ssh-rsa.
- To delete a key, delete the line.
  To change a key, edit a line.
  To add a key, add a line starting with ssh-rsa.
- To exit, press **CTRL** + **X**.
- Save the changes if necessary.

---

#### 6.2.2.15.5 Example of adding an SSH key to the setup user from a connection with the setup user

- Enter the following command.

```
(gcap-cli) set ssh-keys setup "ssh-rsa ..."
```

- Validate.

---

### 6.2.2.16 advanced-configuration

#### 6.2.2.16.1 high-availability

This command has been removed since version 2.5.4.0.

---

#### 6.2.2.16.2 interface-names

This command has been removed since version 2.5.4.0.

---

#### 6.2.2.16.3 local-rules

This command has been removed since version 2.5.4.0.

---

#### 6.2.2.16.4 mtu (Maximum Transfert Unit)

##### 6.2.2.16.4.1 Introduction

The `mtu` command in subgroup `set advanced-configuration` enables displaying changing the MTU byte value of enabled network interfaces (`mon0`, `mon1`, ... `monx`, `gcp0`, `gcp1`, clusters).
This value must be between `1280` and `9000` bytes.

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

---

##### 6.2.2.16.4.2 Prerequisites

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

---

#### 6.2.2.16.4.3 Command

```
set advanced-configuration mtu {interface-name}
```

---

#### 6.2.2.16.4.4 Example of changing the MTU value of the ensp04 interface

- Enter the following command.

```
(gcap-cli) set advanced-configuration mtu ensp04 1500
```

- Validate.
  The system displays the result.

```
Updating Network MTU configuration to:
      - mon1: 1500
```

---

#### 6.2.2.16.5 packet-filtering

This command has been removed since version 2.5.4.0.

---

#### 6.2.2.16.6 rescan-interfaces

This command has been removed since version 2.5.4.0.

---

### 6.2.3 services

#### 6.2.3.1 Service commands

These commands have been removed since version 2.5.4.0.

---

#### 6.2.3.2 show

This command has been removed since version 2.5.4.0.

---

#### 6.2.3.3 start

This command has been removed since version 2.5.4.0.

---

#### 6.2.3.4 status

This command has been removed since version 2.5.4.0.

---

#### 6.2.3.5 stop

This command has been removed since version 2.5.4.0.

---

### 6.2.4 system

#### 6.2.4.1 delete-data

##### 6.2.4.1.1 Introduction

The `delete-data` command of the `system` subgroup enables deleting all data generated by the monitoring engine which are stored on the filesystem.

---

##### 6.2.4.1.2 Prerequisites

- **User:** setup
- **Dependencies:**

---

##### 6.2.4.1.3 Command

`system delete-data`

---

##### 6.2.4.1.4 Example of deleting data

- Enter the following command.

```
(gcap-cli) system delete-data confirm
```

- Validate.
  **all data will be deleted and the GCap will reboot**
  The SSH connection will be interrupted.

---

#### 6.2.4.2 reload-drivers

This command has been removed since version 2.5.4.0.

---

#### 6.2.4.3 restart

##### 6.2.4.3.1 Introduction

The `restart` command of the `system` subgroup enables restarting the GCap.
If before start-up the detection engine is activated (**UP** status), it will be activated after start-up.
If the GCap is paired with the GCenter before start-up, it will be paired after start-up.

---

##### 6.2.4.3.2 Prerequisites

- **User:** setup
- **Dependencies:** None

---

##### 6.2.4.3.3 Command

```
system restart
```

---

##### 6.2.4.3.4 Example of restarting a GCap

- Enter the following command.

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

- Validate.
  The SSH connection will be interrupted.

---

#### 6.2.4.4 shutdown

##### 6.2.4.4.1 Introduction

The `shutdown` command of the `system` subgroup 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.

---

#### 6.2.4.4.2 Prerequisites

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

---

#### 6.2.4.4.3 Command

```
system shutdown
```

---

#### 6.2.4.4.4 Example of shutting down the GCap.

- Enter the following command.

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

- Validate.

---

### 6.2.4.5 unlock

#### 6.2.4.5.1 Introduction

The `unlock` command of the `system` subgroup enables resetting the lock of the `gview`, `gviewadm` and `setup` accounts after unsuccessful authentication attempts.

---

#### 6.2.4.5.2 Prerequisites

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

---

#### 6.2.4.5.3 Command

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

---

#### 6.2.4.5.4 Example of unlocking the setup account

- Enter the following command.

```
(gcap-cli) system unlock setup
```

- Validate.
  The system displays the result.

```
User setup successfully unlocked
```

---

#### 6.2.4.6 upgrade

##### 6.2.4.6.1 Introduction

The `upgrade` command of the `system` subgroup enables upgrading the sensor to a new version.

---

##### 6.2.4.6.2 Prerequisites

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

---

##### 6.2.4.6.3 Command

`system upgrade`

---

##### 6.2.4.6.4 Example of upgrading a GCap

- Enter the following command to list available packages on GCenter.

```
(gcap-cli) system upgrade list
```

- Validate.
- Enter the following command to upgrade the sensor.

```
(gcap-cli) system upgrade apply [package_name] confirm
```

- Validate.
  **At the end of the operation sensor will restart**
  The SSH connection will be interrupted.

---

### 6.2.5 monitoring-engine

#### 6.2.5.1 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:

- Starting the detection engine
- Stopping the detection engine
- Visualising the status of the detection 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.

---

#### 6.2.5.2 Prerequisites

- **Users:** setup, gviewadm
- **Dependencies:**
  - Add the IP of the GCenter (`set gcenter-ip`).
  - Pair the GCap and 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.

---

#### 6.2.5.3 Command

```
monitoring-engine {status|start|stop}
```

---

#### 6.2.5.4 Example of displaying the status of the detection engine

- Enter the following command.

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

- 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

---

#### 6.2.5.5 Example of starting 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.

- Enter the following command.

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

- Validate.
- 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 running.

---

#### 6.2.5.6 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 running.

- Enter the following command.

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

- Validate.
- 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.

---

### 6.2.6 pairing

#### 6.2.6.1 Introduction

The `pairing` command enables configuring the IPsec pairing with the GCenter.

---

#### 6.2.6.2 Prerequisites

- **User:** setup
- **Dependencies:**
  - 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

---

#### 6.2.6.3 Command

`pairing fingerprint FINGERPRINT otp OTP`

---

#### 6.2.6.4 Example of pairing a GCap version 2.5.4.0 with a GCenter

- Retrieve the FQDN (hostname + domain) of the GCap via the `show status` command.

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

- Go to the GCenter WEB interface to add the full FQDN (Fully Qualified Domain Name) of the probe
  For more information, please refer to the GCenter documentation.
- Enter the SSH fingerprint of the GCenter in the `pairing` command.
- Enter the generated OTP in the `pairing` command.

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

- Validate the pairing with the `show status` command.

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

  For more information on this procedure, refer to the *Pairing procedure between a GCap and a GCenter*.

---

### 6.2.7 unpair

#### 6.2.7.1 Introduction

The `unpair` command enables deleting configuration related to the pairing (IPSec configuration).

---

#### 6.2.7.2 Prerequisites

- **User:** setup

---

#### 6.2.7.3 Command

`unpair`

---

#### 6.2.7.4 Example of unparing

- Enter the following command.

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

- Validate.
  The system displays **Operation successful**.
  For more information on the pairing, refer to the *Pairing procedure between a GCap and a GCenter*.

---

### 6.2.8 replay

#### 6.2.8.1 Introduction

A file with the pcap extension is one in which raw network traffic has been captured.
The `replay` command enables:

- Listing the available pcap files
- Asking the detection engine to analyse 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.

---

#### 6.2.8.2 Prerequisites

- **Users:** setup, gviewadm
- **Dependencies:**
  - The detection engine is started (`UP`)
  - The `monvirt` interface is activated
  - At least one pcap file must be present in the pcap directory

---

#### 6.2.8.3 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)

---

#### 6.2.8.4 Example of displaying the list of available pcap files

- Enter the following command.

```
[Monitoring UP] GCap-lab (gcap-cli) replay list
```

- Validate.

```
Available pcaps are:

test-dga-v1.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 test-sigflow-v1.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

---

#### 6.2.8.5 Example of replaying a pcap file with the capture speed

- Enter the following command.

```
(gcap-cli) replay pcap name.pcap speed 4
```

- 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
```

(suite sur la page suivante)

(suite de la page précédente)

```
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.

---

### 6.2.9 help

To obtain help with the available commands, it is possible to:

- Prefix it with `help` (example `help show config-files`)
- Suffix the command with `?` (example `show config-files ?`)

Help enables displaying the available commands and a description of the command in the current context.

---

#### 6.2.9.1 Use 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

---

##### 6.2.9.1.1 Prerequisites for ?

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

---

#### 6.2.9.1.2 Command `?`

- `(gcap-cli) ?` to display the list of available commands
- `(gcap-cli) show status ?` to display the help for the `status` command of the `show` set

---

#### 6.2.9.1.3 Using the `?` of suffixing

To list the configuration files accessible via the CLI:

- Use the `show network` command followed by `?`

```
(gcap-cli) show network ?
```

- 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
```

---

### 6.2.9.2 Use of `help`

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

---

#### 6.2.9.2.1 Prerequisites for `help`

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

---

#### 6.2.9.2.2 Command `help`

- `(gcap-cli) help` to display the list of available commands
- `(gcap-cli) show status --help` to display the help for the command `status` of the set `show`
- `(gcap-cli) help show status` to display the help for the command `status` of the set `show`

---

#### 6.2.9.2.3 Using `help` alone

- Enter the following command.

```
(gcap-cli) help
```

- Validate.
  The system displays the following information:

```
CLI entrypoint
==============

Available commands:
       - show: Show system configuration
   - set: Modify system configuration
   - system: Handle system operations
   - monitoring-engine: Handle Monitoring Engine
   - unpair: Unpair from the current GCenter
   - help: Display command help message
   - colour: Handle colour support for current CLI session
   - exit: Exit configuration tool
```

---

#### 6.2.9.2.4 Example of prefixing: display the commands available in the monitoring-engine context from the root of gcap-cli

- Enter the following command.

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

- Validate.
  The system displays the following information depends on the GCap configuration:
  **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.

---

#### 6.2.9.2.5 Example of suffixing: displaying the information of a command

- Enter the following command.

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

- Validate.
  The system displays the following information:

```
Shutdown GCap
```

---

## 6.2.10 colour

### 6.2.10.1 Prerequisites

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

The `colour` command enables or disables colours in the output of the current instance of gcap-cli.

---

### 6.2.10.2 Command

`colour {disable|enable}`

---

### 6.2.10.3 Example to display service statuses with colour.

- Enter the following command.

```
(gcap-cli) colour enable
```

- Validate.
  The system then displays the information in colour.

```
    <pre>
    <span style="color:green;">[Monitoring UP]</span> <span style="color:red;">GCap</
↪span><span style="color:blue;"> (gcap-cli)</span> service status
    <span style="color:green;">up</span> - Service eve-generation
    <span style="color:green;">up</span> - Service eve-upload
    <span style="color:green;">up</span> - Service file-extraction
    <span style="color:green;">up</span> - Service file-upload
    <span style="color:red;">down</span> - Service filter-fileinfo
    <span style="color:red;">down</span> - Service eve-compress

    <span style="color:green;">[Monitoring UP]</span> <span style="color:red;">GCap</
↪span><span style="color:blue;"> (gcap-cli)</span> colour disable
    </pre>
```

---

#### 6.2.10.4 Example for displaying service reports without colour

- Enter the following command.

```
(gcap-cli) colour disable
```

- Validate.
  The system then displays the information without colour(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>
```

---

### 6.2.11 gui

This command has been removed since version 2.5.4.0.

---

### 6.2.12 exit

#### 6.2.12.1 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.

---

#### 6.2.12.2 Prerequisites

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

---

#### 6.2.12.3 Command

```
exit
```

---

#### 6.2.12.4 Example of exiting the "set protocols-selector logging" context

- Enter the following command.

```
(gcap-cli set protocols-selector logging) exit
```

- Validate.
  The prompt changed and shows the root context:

```
(gcap-cli)
```

---

#### 6.2.12.5 Example of exiting the CLI

- Enter the following command.

```
(gcap-cli) exit
```

- Validate.

---

# Chapter 7

# Metrics

## 7.1 List of metrics comparison version 2.5.3.105 vs 2.5.3.104

Version 2.5.3.105 uses new counters and renames others.
The tables below provide a comparison between version 2.5.3.105 vs. 2.5.3.104 counters.

### 7.1.1 Internal metrics version 2.5.3.105 vs 2.5.3.104

| Name on V105 version | Name on V104 version | Difference between versions |
|---|---|---|
| netdata.runtime_proc_net_dev | | counter added with V105 |
| netdata.runtime_xdp_filter | netdata.runtime_xdp_filter_local | counter renamed with V105 |
| netdata.runtime_disk_usage | netdata.runtime_disk_usage_local | counter renamed with V105 |
| netdata.runtime_proc_meminfo | | counter added with V105 |
| netdata.runtime_proc_loadavg | | counter added with V105 |
| netdata.runtime_proc_uptime | | counter added with V105 |
| netdata.runtime_proc_vmstat | | counter added with V105 |
| netdata.runtime_proc_stat | | counter added with V105 |
| netdata.runtime_high_availability | | counter added with V105 |
| netdata.runtime_sys_block | | counter added with V105 |
| netdata.runtime_proc_net_softnet_stat | | counter added with V105 |
| netdata.runtime_suricata | netdata.runtime_suricata_local | counter renamed with V105 |
| netdata.runtime_codebreaker | netdata.runtime_codebreaker_local | counter renamed with V105 |
| netdata.web_thread[1-6]_cpu | | counter renamed with V105 |
| netdata.plugin_diskspace_dt | | counter renamed with V105 |
| netdata.plugin_diskspace | | counter renamed with V105 |
| | netdata.plugin_proc_cpu | counter renamed with V105 |
| | netdata.plugin_proc_modules | counter renamed with V105 |

### 7.1.2 System information version 2.5.3.105 vs 2.5.3.104

| Name on V105 version | Name on V104 version | Difference between versions |
|---|---|---|
| disk_space.**<partition>** | | counter added with V105 |
| disk_inodes.**<partition>** | | counter added with V105 |
| disk_usage.mountpoint.**<mount>** | | counter added with V105 |
| sys_block.blocks.**<disque>** | | counter added with V105 |
| proc_stat.processes | system.processes | counter renamed with V105 |
| proc_stat.interrupts | system.intr | counter renamed with V105 |
| proc_stat.cpu.cpu(0-n) | system.cpu.cpu(0-n) | counter renamed with V105 |
| proc_vmstat.swapio | system.swapio | counter renamed with V105 |
| proc_vmstat.pgpio | system.pgpgio | counter renamed with V105 |
| proc_vmstat.pagefaults | mem.pgfaults | counter renamed with V105 |
| proc_uptime.uptime | system.uptime | counter renamed with V105 |
| proc_loadavg.Load_average | system.load | counter renamed with V105 |
| proc_loadavg.Active_processes | system.active_processes | counter renamed with V105 |
| proc_meminfo.RAM | system.ram | counter renamed with V105 |
| proc_meminfo.available | mem.available | counter renamed with V105 |
| proc_meminfo.swap | system.swap | counter renamed with V105 |
| proc_meminfo.kernel | mem.kernel | counter renamed with V105 |
| proc_meminfo.hugepages | mem.transparent_hugepages | counter renamed with V105 |
| | system.io | counter deleted with V105 |
| | system.net | counter deleted with V105 |

### 7.1.3 Network information version 2.5.3.105 vs 2.5.3.104

| Name on V105 version | Name on V104 version | Difference between versions |
|---|---|---|
| proc_net_dev.net_drops.**<iface>** | proc_net_dev_local.net_drops.**<iface>** | counter renamed with V105 |
| proc_net_dev.net_drops.**<iface>** | proc_net_dev_local.net_errors.**<iface>** | counter renamed with V105 |
| proc_net_dev.net_pkts.**<iface>** | proc_net_dev_local.net_pkts.**<iface>** | counter renamed with V105 |
| proc_net_dev.net.**<iface>** | proc_net_dev_local.net.**<iface>** | counter renamed with V105 |
| proc_net_softnet_stat.cpu[0-n].sched | | counter added with V105 |
| proc_net_softnet_stat.cpu[0-n].packets | | counter added with V105 |
| proc_net_softnet_stat.summed.sched | | counter added with V105 |
| proc_net_softnet_stat.summed.packets | | counter added with V105 |

### 7.1.4 Device and detection information version 2.5.3.105 vs 2.5.3.104

| Name on V105 version | Name on V104 version | Difference between versions |
|---|---|---|
| high_availability.ha_status | | counter added with V105 |
| high_availability.leader_status | | counter added with V105 |
| high_availability.last_status | | counter added with V105 |
| high_availability.health_status | | counter renamed with V105 |
| xdp_filter.dropped_bytes | | counter added with V105 |
| xdp_filter.dropped_packets | | counter added with V105 |
| xdp_filter.bypassed_half_flows | | counter added with V105 |
| codebreaker.shellcode_samples | codebreaker_local.shellcode_samples | counter renamed with V105 |

## 7.2 List of available metrics from version 2.5.3.105

### 7.2.1 Internal metrics

| Name | Unit<br>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<br>ms/s | CPU usage time of netdata threads |
| netdata.plugin_diskspace_dt | duration<br>ms/run | Execution time of the script for collecting information on disk space |
| netdata.plugin_diskspace | user system<br>ms/s | CPU usage time of the disk space information collection plugin |

### 7.2.2 Details of Sigflow counters

#### 7.2.2.1 Alerts counter details - Number of Sigflow alerts found

| Name | Dimensions | Comments |
|---|---|---|
| suricata.alert | Alerts.value | Number of Sigflow alerts found |

#### 7.2.2.2 Codebreaker samples counter details - 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 |

#### 7.2.2.3 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 | Units | Comments |
|---|---|---|---|
| suricata.dhcp | DHCP.value | number | DHCP protocol |
| 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 protocol |
| 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 |

#### 7.2.2.4 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<br>• sent<br>• duplicated | • Number of files extracted<br>• Number of files sent<br>• Number of files duplicated |
| suricata.received_packets | • ReceivedPackets.value<br>• DroppedPackets.value | • Number of packages captured<br>• Number of packets dropped |
| suricata.rules | • RulesLoaded.value<br>• RulesFailed.value | • Number of rules loaded and validated<br>• 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 by Sigflow |
| suricata.flows | • FlowTCP.value<br>• FlowUDP.value | • Number of TCP sessions observed<br>• Number of UDP sessions observed |

### 7.2.3 Details of GCap statistics counters and health information.

#### 7.2.3.1 Details of quota counters

| Name | Dimensions | Commens |
|---|---|---|
| quotas.uid.block | • block.used<br>• block.soft_limit<br>• block.hard_limit | • Number of blocks used<br>• Software limit<br>• Hardware limit |
| quotas.uid.file | • file.used<br>• file.soft_limit<br>• file.hard_limit | • Number of files used<br>• Software limit<br>• Hardware limit |
| quotas.uid.grace | • grace.block<br>• grace.file | • Grace time for the blocks<br>• Grace time for the files |

#### 7.2.3.2 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<br>• blocked | • processes | • Status of the processes |
| proc_stat.cpu.cpu[0-n] | • softirq<br>• irq<br>• user<br>• system<br>• nice<br>• iowait<br>• idle | • percentage | • Percentage of CPU usage |

#### 7.2.3.3 System information

| Name | Dimensions | Unit | Comments |
|---|---|---|---|
| sys_block.blocks.<disque> | read<br>written | bytes | I/O on the disk <**disk**> |
| proc_uptime.uptime | uptime.uptime | seconds | System uptime |
| disk_inodes.<partition> | avail<br>used<br>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 |

#### 7.2.3.4 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) |
| 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 |

#### 7.2.3.5 Details of interface counters - Statistics on network interfaces

| Name | Dimensions | Unit | Comments |
|---|---|---|---|
| proc_net_dev.net.**<iface>** | • received<br>• sent | bytes | Traffic on the interface <**iface**> |
| proc_net_dev.net_drops.**<iface>** | • rx drops<br>• tx drops | pkts | Number of packets lost on the interface <**iface**> |
| proc_net_dev.net_errors.**<iface>** | • rx errors<br>• tx errors | pkts | Number of packets in error on the interface <**iface**> |
| proc_net_dev.net_pkts.**<iface>** | • received<br>• sent | pkts | Number of packets on the interface <**iface**> |

#### 7.2.3.6 Details of loadavg counters - Statistics on the GCap average load

| Name | Dimensions | Comments |
|---|---|---|
| proc_loadavg.Load_average | • load.load1<br>• load.load5<br>• load.load15 | • Average load over the last minute<br>• Average load over the last five minutes<br>• Average load over the last fifteen minutes |
| proc_loadavg.Active_processes | active_processes.active | Number of active processes |

#### 7.2.3.7 Details of meminfo counters - Statistics on RAM

| Name | Dimensions | Comments |
|---|---|---|
| suricata.memuse | • MemUseTCP.value<br>• MemUseTCPReassembly<br>• MemUseFlow.value<br>• MemUseHTTP.value<br>• MemUseFTP.value | • TCP memory<br>• TCP reassembly memory<br>• Flows memory<br>• HTTP memory<br>• FTP memory |
| suricata.memcap | • MemCapTCPSession.value<br>• MemCapTCPSegment.value<br>• MemCapFlow.value<br>• MemCapHTTP.value<br>• MemCapFTP.value | • TCP session allocation failures<br>• TCP segment allocation failures<br>• Flow allocation failures<br>• HTTP allocation failures<br>• FTP allocation failures |
| proc_meminfo.ram | • free<br>• used<br>• cached<br>• buffers | • Unused memory in kilobytes<br>• Memory used<br>• Memory used by the cache<br>• Memory used by operations |
| proc_meminfo.available | available | Total physical memory in kilobytes |
| proc_meminfo.swap | • swap_free<br>• swap_used<br>• swap_cached | • swap file available<br>• swap file used<br>• swap file used for caching |
| proc_meminfo.kernel | • kernel.slab<br>• kernel.kernel_stack<br>• kernel.page_tables<br>• kernel.v_malloc_used | • Memory used by kernel data structures<br>• Memory used by kernel stack allocations<br>• Memory used for page management<br>• Memory used by large memory areas allocated by the kernel |
| proc_meminfo.hugepages | • hugepages_free<br>• hugepages_used<br>• hugepages.surplus<br>• hugepages.reserved | • Number of huge transparent pages available<br>• Number of huge transparent pages used<br>• Number of extra huge transparent pages<br>• Number of huge transparent pages reserved |

#### 7.2.3.8 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<br>• 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 |

---

#### 7.2.3.9 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<br>• Dropped<br>• Flow limit count<br>• Process queue lengths | pkts | Packets processed on the relevant cpu |
| proc_net_softnet_stat.cpu[0-n].sched | • Received RPS (IPI schedules)<br>• Time squeeze | events | network stack events on the relevant cpu |
| proc_net_softnet_stat.summed.packets | • Processed<br>• Dropped<br>• Flow limit count<br>• Input/Process queue lengths | pkts | Packets processed by the network stack |

---

#### 7.2.3.10 Details of virtualmemory counters - Information on swap space

| Name | Dimensions | Unit | Comments |
|---|---|---|---|
| proc_vmstat.swapio | • in<br>• out | pkts | I/O swap |
| proc_vmstat.pagefaults | • minor<br>• major | faults/s | Memory Page Faults /s |

## 7.3 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 *Monitoring* 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 8

# Appendices

## 8.1 Event 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 |

### 8.1.1 Detection engine events: detection-engine-logs

This log contains the events of the detection 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
```

### 8.1.2 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
```

---

### 8.1.3 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.gatewat
cher.com]...2.3.4.5[CN=GCenter.domain.tld.com]
2022-02-03T13:38:13.085957+00:00 GCap.domain.tld charon: 16[IKE] IKE_SA deleted
2022-02-03T13:38:13.141553+00:00 GCap.domain.tld charon: 16[IKE] initiating IKE_SA GCenter[5]␣
↪to 2.3.4.5                                                    2022-02-03T13:38:13.
↪364748+00:00 GCap.domain.tld charon: 07[IKE] establishing CHILD_SA GCenter{18} reqid 2
2022-02-03T13:38:14.827308+00:00 GCap.domain.tld charon: 12[IKE] IKE_SA GCenter[5]␣
↪established between 10.2.19.152[C=FR, O=GATEWATCHER, CN=GCap.domain.tld]...2.3.4.
↪5[CN=GCenter.domain.tld.com]
```

---

### 8.1.4 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 synchronisation 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]␣
```

(suite sur la page suivante)

(suite de la page précédente)

```
↪Codebreaker file /data/containers/suricata/etc/suricata/rules/codebreaker_shellcode.rules␣
↪was identical
2022-02-03T16:25:35.975630+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO]␣
↪Successfully rsynced GCap.domain.tld-rules-static/v2.0/codebreaker_powershell.rules:
2022-02-03T16:25:35.975771+00:00 GCap.domain.tld GCenter_gateway.xfer [xfer] : [INFO]␣
↪Codebreaker file /data/containers/suricata/etc/suricata/rules/codebreaker_powershell.rules␣
↪was identical
```

### 8.1.5 User activity information: var-log-user

This log contains information about the activity of the GCap users.
Some examples of useful lines:

- Detection engine start-up

```
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
```

### 8.1.6 Debug events: var-log-debug

This log contains debug events.
This entry is mainly used by support during advanced troubleshooting.

### 8.1.7 Aggregation of different logs: var-log-messages

This log contains the aggregation of the different logs listed above.

---

### 8.1.8 Scheduled task start information: var-log-cron

This log contains the launch information of scheduled tasks.

---

# Chapter 9

# 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**
: GCenter is the component administering the GCap and performing the analysis of the 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.

# Index


C

CLI, 154

F

FQDN, 154

G

GCap, 154
GCenter, 154
gview, 154
gviewadm, 154

M

MTU, 154

O

OTP, 154

R

RAID1, 154
RAID5, 154

S

setup, 154
SIGFLOW, 154

T

TAP, 154