Release Note
GCap Version 2.5.4

version: V1

Translated from original manual version 1

Creation date: December, 2024

Contents

Chapter 1

Presentation of GCap version 2.5.4

This release note provides a description of:

- new features
- improvements and other characteristics
- patches
- known issues
- software compatibility
- hardware compatibility
- upgrade procedure

Chapter 2

New features

2.1 Sigflow detection engine

2.1.1 Update of detection engine

The detection engine Sigflow was updated.
This update includes security fixes for critical vulnerabilities published recently.

2.1.2 Adding new event type « flow »

The generation of « flow » event is now available for Sigflow detection engine.

2.1.3 Multitenant configuration

The multitenant configuration was improved to offer the possibility to configure specific network variables (network port and IP addresses) for each tenant.

2.1.4 Adding of network fingerprint HASSH

A new field « hassh » is available for SSH events, in order to record client and server SSH fingerprints, when a transaction using this protocol is analyzed by Sigflow engine.

2.1.5 Recording of certificat fields

It's now possible to select the certificat fields that we want to record when a TLS transaction is analyzed (handshake).

2.1.6 Adding new keyword for detection rules

`dns.query.name` keyword was added to Sigflow detection engine and it can be used in detection rules related to DNS protocol.
It's a sticky buffer that is used to look at the name field and supports both DNS requests and responses.

2.1.7 Pcap files for test

Two new pcap files were added for testing ransomware-detect and beacon-detect engines (GCenter v2.3.5.103).

2.2 Virtualization of the sensor

2.2.1 VMware support

GCap is officially supported on ESXi hypervisor from VMware.

2.2.2 AWS support

GCap is officially supported on AWS Cloud infrastructure.

2.3 Network configuration of the sensor

2.3.1 Presentation

- Network interfaces are now identified by their system name as in the example above with the commande `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

- Network interfaces gcpX were removed.

- **Concept of role and label** is introduced in this release.
  - Following is the list of roles:
    - **capture** to define an interface for capturing the flow
    - **tunnel** to define an interface used to IPsec communication between GCap and GCenter
    - **management** to define an interface used to manage GCap (via SSH)
    - **management-tunnel** to define an interface which carry the two previous roles (management and tunnel)
    - **capture-cluster** to define an interface for capturing the flow in cluster mode
    - **inactive** to disable an interface
  - Following is the list of labels:
    - **Management***
    - **Tunnel**
    - **MonX**

2.3.2 Associated command

To assign a specific role to an interface, the following command must be used:

```
`set interfaces assign-role {management|tunnel|management-tunnel|capture|capture-cluster|inactive}`
```

2.4 Update process

A rollback functionality was implemented in case of issue during the system update process.
It will be possible to revert to the previous version when the GCap start menu is displayed.

2.5 Hardware support

2.5.1 Support of DELL servers

This release is compatible with DELL servers gen 16 th.

2.5.2 UEFI support

This release introduced the support of UEFI.

Chapter 3

Other features and improvements

3.1 Performance

Sensor performance was improved with a dynamic resource allocation at the first boot and a better flow distribution during the capture.

3.2 Pairing process of the sensor

The command `unpair` is now available to remove all pairing configuration from the sensor.

3.3 Business data deletion

The command `system delete-data` is now available to remove all business data from the sensor.

3.4 `show status` command

Additional information is available with the command `system delete-data` :

```
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
```

(suite sur la page suivante)

(suite de la page précédente)

```
 Paired on Gcenter     : Yes
 Monitoring interfaces : mon0,mon2,mon4,monvirt

   © Copyright GATEWATCHER ...
```

3.5 System update

The GCap probe operating system and the kernel have been updated.

3.6 Compatibility mode

A new compatibility mode is available for supporting GCenter v2.5.3.103.

3.7 IPSec connection

The configuration of IPsec service was optimized to improve the connection reliability between GCap and GCenter.

3.8 Visualization of the configuraiton in the CLI

All « show » commands are available when the detection engine is up.

3.9 Deprecated commands and features

3.9.1 High-availability

High-availability feature was removed from this release.
To implement a redundant architecture, contact Gatewatcher Technical Support.

3.9.2 Sigflow: local rules

Local rules are no longer supported.

3.9.3 Creation of techsupport file

The creation of techsupport file must be exclusively performed with an non-interactive SSH session:

- From a Linux workstation:

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

- From a Windows workstation:

  `ssh -t setup@GCapX "show tech-support large" > C:\Temp\tech-supp-GCap`

3.9.4 Removed commands

The following orders have been removed:

- The command `set advanced-configuration packet-filter` to configure local XDP filters
  The configuration of XDP filters must be exclusively performed on GCenter
- The command `show advanced-configuration cpu-config` to display CPU configuration
- The command `show/set advanced-configuration interfaces-names` to display or configure the interface name
- The command `show/set advanced-configuration load-balancing` to display or configure the loadbalancing for capture interface
- The command `show/set advanced-configuration local-rules` to display or configure the local rules
- The command `show advanced-configuration memory-settings` to display the memory configuration of detection engine
- The command `system reload-drivers` to reload the drivers of network cards
- The command `show/set clusters` to display or configure the cluster interfaces
  The configuration of cluster interfaces must be performed with the command `set interfaces [interface-name] assign-role capture-cluster`.
- The command `gui` to enter in the graphical configuration menu
- The command `show/set setup-mode` to display or configurer de default mode for the configuration interface
- The command `show configuration` to display Sigflow configuration
- The command `show logs` to display log files

The commands related to service management:

- `services start/stop/show {eve-generation|eve-upload|file-extraction|file-upload|filter-fileinf

---

Chapter 4

Patches

4.1 IPSec : the command `pairing reload-tunnel` doesn't fully restart the service

In some case, the command `pairing reload-tunnel` doesn't solve issue the IPSec tunnel between GCap and GCenter.
This issue is fixes in v2.5.4.0.

4.2 Netdata: Approximation with Sigflow metrics

Some Sigflow metrics are approximate.
This issue is fixes in v2.5.4.0.

4.3 Sigflow: Some network packets are counted twice.

In some cases, some network packets are counted twice in the statistics of the network cards sent by Sigflow engine.
This issue is fixes in v2.5.4.0.

Chapter 5

Known problems and limitations

There is no known bug.

Chapter 6

Software compatibility

6.1 Compatibility with GCenter

GCap version	GCenter version	Compatibility
2.5.4.0	2.5.3.101 HF4	Unsupported configuration: GCenter to upgrade to a newer version
2.5.4.0	2.5.3.102 HF3	Configuration OK

Chapter 7

Hardware compatibility

Version 2.5.4.0 is compatible with all hardware versions of GCap.

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

Chapter 8

Updating procedure

8.1 Prerequisites

To deploy the GCap V2.5.4.0 update from the GCenter GUI, the GCenter must be in the installed **V2.5.3.102-HF3** version.
If the GCenter is in a previous version, it will need to be updated (for versions below **V2.5.3.102-HF3**).
If you have any questions about these items, please contact Gatewatcher Technical Support.

Important:

It is mandatory to have an iDRAC connection so that you can connect post-upgrade if a problem occurs during the process.
Otherwise, physical access to the equipment (screen, keyboard) will be required.

8.2 Retained data

The following data is retained:

- the GCenter pairing
- the network configuration
- the SSH key of the root account
- the password of the root account
- the log files
- the pcap files in the /data/pcaps/ directory

8.3 Data deleted

Important:

The following data will be deleted:

- Local rules for Sigflow (local-rules)
- Local XDP filters

  please postpone the configuration of these filters at GCenter level using the **GCap Profiles** > **Packet filters**) menu

8.4 Installation procedure via the GCenter

On GCenter:

1. From the platform https://update.gatewatcher.com/upgrade/ (directory 2.5.4.0/gcap/), download:
   - the gwp file of the new version available
   - the associated sha256 gwp.sha256 file
2. Check the image (sha256sum command) and check the value obtained with the contents of the gwp.sha256 file
3. Log on to the GCenter WebUI via a web browser and go to the **Admin** > **Gum** > **Software Update** menu.
4. In the **Upload a software update** section, click on **Browse** and select the . gwp (previously uploaded image) to make it available on GCenter.
5. Validate by clicking on the **Choose** button.
6. Validate the upload by clicking on the **Submit** button.
   - A progress bar is displayed
   - If you encounter a problem when making the image available, try another browser.

On GCap:

1. Open a terminal and log into SSH on GCap with the **setup** account.
2. If needed, stop the monitoring-engine with the command **monitoring-engine stop** (GCAP-CLI).
3. Use the command **system upgrade list** to get the package list from the GCenter (GCAP-CLI).
4. Use the command **system upgrade apply [image_name] confirm** (GCAP-CLI).
   - GCap must restart automatically.
   - SSH session is down
5. Once the GCap has restarted, log into SSH with the **setup** account to see if the update has been correctly applied.
6. Check the current version with the **show status** command (GCAP-CLI).
7. Start the monitoring-engine with the command **monitoring-engine start** (GCAP-CLI).

In case of problem, please contact Gatewatcher Technical Support.

8.5 Installation procedure directly from the GCap

1. Download the newly available version and the associated sha256 on the https://update.gatewatcher.com/upgrade/ platform (directory 2.5.4.0/gcap/).
2. Check the image (sha256sum command) and check the value obtained with the contents of the gwp.sha256 file.
3. Copy the image (.gwp) to the /tmp/ directory of the GCap using a privileged account.
4. Open a terminal and log in via SSH on the GCap with the **setup** account.
5. If needed, stop the monitoring engine with the **monitoring-engine stop** command (GCAP-CLI).
6. Open a terminal and log in via SSH on the GCap with a privileged account.
7. Start the upgrade with the command **gcap-upgrade /tmp/file_name** (SHELL).
8. Restart the GCap with the **system restart** command (GCAP-CLI)
   SSH session is down
9. Log in to SSH with the **setup** account to verify that the update was successfully applied.
10. Check the current version with the **show status** command (GCAP-CLI).
11. Start the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

If you have any problems, please contact Gatewatcher Technical Support.

`PDF Release Note`