Release Note
GCap Version 2.5.3.107

version: V1

Translated from original manual version 1

Creation date: October, 2023

Contents

Chapter 1

Presentation of GCap version 2.5.3.107

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

No new features in this release.

Chapter 3

Other features and improvements

3.1 `pairing reload-tunnel` command

The command `pairing reload-tunnel` is now available when the monitoring engine is started.

Chapter 4

Patches

4.1 Sigflow: Issue with some statistics

Some statistics generated by Sigflow are not correct.

This issue is fixed in V2.5.3.107.

4.2 Autosetup: Issue when a wrong configuration is applied.

If a wrong configuration is applies via the autosetup feature, GCap will try to reload it at each boot.

This issue is fixed in V2.5.3.107.

4.3 Sending of eve-logs: A service could be unavailable in compatibility mode 2.5.3.101.

In some cases, one of service which it sends eve-logs to GCenter could be not operational in compatibility mode 2.5.3.101.

This issue is fixed in V2.5.3.107.

4.4 Codebreaker: Issue with source and destination IP adresses in an alert

There is an inversion with the source and destination IP adresses in a Codebreaker alert.

This issue is fixed in V2.5.3.107.

4.5 Sigflow: File reconstruction issue with SMTP protocol.

Randomly, file reconstruction is performed partially by Sigflow detection engine.

This issue is fixed in V2.5.3.107.

4.6 Configuration: Issue when GCap retrieves its configuration

In some cases, a timeout occurs when GCap tries to download its configuration

This issue is fixed in V2.5.3.107.

4.7 Sending of eve-logs: Issue with a unreliable network connexion

When a network connexion between GCap and GCenter is unreliable, the transfert of eve-logs fails.

This issue is fixed in V2.5.3.107.

Chapter 5

Known problems and limitations

5.1 Netdata: displaying information in the GCenter V2.5.3.101 WebUI

Revamping and adding new information at the Netdata level renders the graphics and statistics displayed on the GCenter V2.5.3.101 WebUI inoperative.

The data can still be accessed via the Netdata API.

5.2 Modification of the MTU of a VPN interface and tunnel

Changing the MTU of a GCap interface results in the network configuration of all interfaces being re-applied.

This has the effect of losing connectivity between GCap and GCenter (IPsec VPN) for about 4 minutes.

5.3 Restore the backup on GCenter.

When restoring the backup on the GCenter, pairing with the GCaps must be performed again.

5.4 Error during first network configuration

During initial network configuration, an error appears.

There are 4 steps to fully validate the network configuration:

- configure the hostname
- configure the domain name
- configure the ip address
- Selection of management/VPN interfaces;

As long as the 4 parameters are not filled in, an error appears when validating the first 3 parameters.

5.5 Error and logout when entering an incorrect value for the date

When configuring the date and time of a GCap, if an incorrect value is entered then an error is displayed and the SSH connection is closed.

Chapter 6

Software compatibility

6.1 Compatibility with another GCap

When used with high availability (HA), both GCaps must be of the same version.

6.2 Compatibility with GCenter

GCap version	GCenter version	Compatibility
2.5.3.107	2.5.3.100 HF7	Unsupported configuration: GCenter to upgrade to a newer version
2.5.3.107	2.5.3.101 HF2	Configuration ok (limitation during the installation process of the new GCap version)
2.5.3.107	2.5.3.101 HF3	Configuration ok
2.5.3.107	2.5.3.102	Configuration ok

Chapter 7

Hardware compatibility

Version 2.5.3.107 is compatible with all hardware versions of GCap.

REFERENCE GCAP	LOCAL STORAGE	PORTS CAPTURE	PORTS CAPTURE EXTENSION	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 V2.5.3.107 update from the GCenter GUI, the GCenter must be at least in the installed **V2.5.3.101-HF3** version.

If the GCenter is in a previous version, it will need to be updated (for versions below **V2.5.3.101**) or it will need to have the necessary administrator privileges at the GCap level to be able to deploy the image directly from the command line (for version **V2.5.3.101-HF2**).

If you have any questions about these items, please contact Gatewatcher Technical Support.

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 Installation procedure via the GCenter

On GCenter:

1. Download from the platform https://update.gatewatcher.com/upgrade/ (directory 2.5.3.107/gcap/):
   - 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 **Browse** and select the . gwp (previously uploaded image) to make it available on GCenter.
5. Validate by clicking the **Choose** button.
6. Validate the upload by clicking 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. Launch the graphical configuration utility with the **gui** command.
3. Stop the monitoring-engine with the command **monitoring-engine stop** (GCAP-CLI) and check that there are no more eve-logs and files to transmit to the GCenter.
4. Go to the **system/upgrade** menu.
5. Validate the update by selecting **'Yes, upgrade this GCap'**.
   - GCap must restart automatically.
6. Once the GCap has restarted, log into SSH with the **setup** account to see if the update has been correctly applied.
7. Restart the monitoring-engine with the command **monitoring-engine start** (GCAP-CLI).

In case of problem, please contact Gatewatcher Technical Support.

8.4 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 2.5.3.107/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. Stop the monitoring engine with the **monitoring-engine stop** command (GCAP-CLI).
5. Start the upgrade with the command **gcap-upgrade /tmp/file_name** (SHELL).
6. Restart the GCap with the **system restart** command (GCAP-CLI): be careful, the SSH connection will be interrupted.
7. Log in to SSH with the **setup** account to verify that the update was successfully applied.
8. Restart the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

If you have any problems, please contact Gatewatcher technical support.

`PDF Release Note`