Release Note
GCap Version 2.5.3.105

Note version : V2

Translated from original manual version 2

Creation Date : September, 2022

Last update : September, 2022

Contents

Contents 1

1 Presentation of GCap version 2.5.3.105 3

2 New features 4
2.1 High availability 4
2.2 SSH key authentication 4
2.3 Statistics and health information 5
2.3.1 Displaying statistics and health information 5
2.3.2 New statistics and health information via Netdata 5
2.4 Improvements to the Sigflow detection engine 5
2.4.1 New version of the engine 5
2.4.2 New protocols supporting the analysis 5
2.4.3 New protocols supported for rebuilding files 6
2.4.4 Adding MAC addresses from the network 6
2.4.5 Optimisation of TLS encrypted flow analysis 7
2.4.6 Dynamic change of CPU assignments 7
2.4.7 MTU configuration for interfaces *monvirt*, *gcp0* and *gcp1* 7
2.4.8 Enabling TLS connection fingerprinting 7
2.4.9 Adding the community-id for the hash of flows 7
2.4.10 Adding the « activehunt » classetype 7
2.4.11 Grace period granted to the capture interface start-up 8
2.4.12 Manual assignment of all GCap interfaces 8
2.4.13 Detection engine grace period option 8
2.4.14 Sanity-checks option for the detection engine 8
2.5 vpn-link speed option for the VPN tunnel 9
2.6 Addition of an automatic restart mechanism for crashed services 9
2.7 Addition of the possibility of placing a command from the CLI with the SSH connection 9

3 Other features and improvements 10
3.1 Change of operating system 10
3.2 Change of the programming language 10
3.3 Update of the kernel 10
3.4 Performance improvement 10
3.4.1 Codebreaker performance improvements 10
3.4.2 Optimising the network communication between the GCap and the GCenter 10
3.4.3 Improved load management of *monx* capture interfaces 11
3.5 Global security improvements 11
3.5.1 Network security 11
3.5.2 Security system 11
3.6 Changes to the CLI 13
3.6.1 Changing the scope of interface-related commands 13
3.6.2 Selecting the protocols to be analysed by the detection engine 13

3.6.3 The configuration GUI is marked obsolete . . . 14
3.7 Features available for extracting diagnostic data to Gatewatcher technical support . . . 14
3.8 Changing the driver reload strategy . . . 14
3.9 Modification of the crisis management strategy (emergency mode) . . . 14

4 Patches **15**
4.1 Eve-logs are automatically truncated if size > 65536 bytes . . . 15
4.2 TCP transactions and extracted files (« unknown ») . . . 15
4.3 Using RELP protocol and adding a queue between GCap and GCenter . . . 15
4.4 Protection of the authentication mechanism (anti-bruteforce) . . . 16
4.5 HTTP parsing problem . . . 16
4.6 Problem when replaying some pcap files . . . 16
4.7 Problem replaying pcap files with multi-tenancy enabled . . . 16
4.8 Display of the GCap status as « undetermined » in the GCenter management interface . . . 16
4.9 Erroneous status display of the monitoring interfaces . . . 17

5 Known problems and limitations **18**
5.1 Netdata: displaying information in the GCenter v101 WebUI . . . 18
5.2 Changing the MTU of a VPN interface and tunnel . . . 18
5.3 Restoring the backup on the GCenter. . . . 18

6 Software compatibility **19**
6.1 Compatibility with another GCap . . . 19
6.2 Compatibility with GCenter . . . 19

7 Hardware compatibility **20**

8 Updating procedure **21**
8.1 Prerequisites . . . 21
8.2 Retained data . . . 21
8.3 Installation procedure via the GCenter . . . 21
8.4 Installation procedure directly from the GCap . . . 22

Chapter 1

Presentation of GCap version 2.5.3.105

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 High availability

In order to increase the operational readiness of the application, Gatewatcher implemented a high availability mechanism.

It enables maintaining the captured flows. For example, in the event of a GCap failure or shutdown, this is achieved by setting up two redundant GCaps.

These two GCaps capture the same flow while communicating with a single GCenter.

In the event of any problems with the « leader » GCap, the « follower » GCap takes over thus ensuring continuity of service during the maintenance operation.

The following commands were added:

- `` `show advanced-configuration high-availability` `` to view the status of redundancy (HA),
- `` `set advanced-configuration high-availability` `` to configure the redundancy (HA).

For further information on how this mechanism works, please refer to the documentation.

2.2 SSH key authentication

In order to increase the access security to the GCap, SSH key authentication was implemented.

This feature enables defining a key for a given user, guaranteeing traceability of connections and accountability of actions.

GCap supports RSA, ECDSA, and ED25519 keys.

This mode is to be preferred to the user name/password pair.

Adding an SSH key for an account is set via the `` `set ssh-keys` `` command.

Note:

```
The password management policy is not used in connection with SSH keys.
```

2.3 Statistics and health information

2.3.1 Displaying statistics and health information

In order to improve GCap monitoring, new counters on statistics and health information were introduced, covering the following categories:

- counters and statistics related to mass storage material, processors, RAM, and exchange space,
- counters related to emergency mode, pairing of GCenter, high availability (HA), availability, and system initialisation features,
- counters of the Sigflow detection engine and its load such as engine information, network interfaces, received packets by processor core, NUMA node, and average GCap load.

These counters and statistics can be viewed via the ``show health`` command.

2.3.2 New statistics and health information via Netdata

New statistics and health information are available via Netdata.

2.4 Improvements to the Sigflow detection engine

2.4.1 New version of the engine

The Sigflow engine was updated to take into account new features, new protocols, and so forth.

2.4.2 New protocols supporting the analysis

The table below displays the **new** protocols that are supported.

The protocol detection is divided in 2 parts:

- **parsing**:

- this 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**:

- this enables generating metadata for a given protocol to the GCenter.
- if logging is enabled for a protocol then the observed flow generates metadata.
- if logging is disabled for a protocol then no metadata is generated.

Protocol	Type	GCAP Versions	
		V2.5.3.104	V2.5.3.105
DCERPC	parsing	supported	supported
	logging	not supported	supported
ENIP	parsing	not supported	supported detection only
	logging	not supported	supported
FTP	parsing	supported	supported
	logging	not supported	supported
HTTP2	parsing	not supported	supported
	logging	not supported	supported
IMAP	parsing	not supported	supported detection only
	logging	not supported	supported
MQTT	parsing	not supported	supported
	logging	not supported	supported
RDP	parsing	not supported	supported
	logging	not supported	supported
RFB	parsing	not supported	supported
	logging	not supported	supported
SIP	parsing	not supported	supported
	logging	not supported	supported
SNMP	parsing	not supported	supported
	logging	not supported	supported

2.4.3 New protocols supported for rebuilding files

The table below displays the **new** protocols that are supported.

	GCAP Versions	
Protocol	V2.5.3.104	V2.5.3.105
FTP	supported via defined rules on GCAP only	supported
HTTP2	not supported	supported
NFS	not supported	supported
SMB	supported via defined rules on GCAP only	supported

2.4.4 Adding MAC addresses from the network

As of V2.5.3.105, MAC addresses observed on the network are recorded for the proper functioning of Network Detection & Response (NDR).

2.4.5 Optimisation of TLS encrypted flow analysis

Up until V2.5.3.104, the entire TLS flow is analysed by the detection engine (both the plaintext and encrypted parts).

From V2.5.3.105 onwards:

- the plaintext part of TLS flows is analysed,
- the encrypted part of TLS flows is no longer analysed thanks to the addition of a dynamic bypass rule (XDP filter).

2.4.6 Dynamic change of CPU assignments

Up until V2.5.3.104, assigning CPUs to the detection engine could cause instabilities, requiring a restart of the GCap after modification.

As of V2.5.3.105, it is no longer necessary to restart the GCap after a new assignment.

2.4.7 MTU configuration for interfaces *monvirt*, *gcp0* and *gcp1*

As of V2.5.3.105, it is possible to configure the MTU of the *monvirt* virtual interface and the *gcp0* and *gcp1* physical interfaces via the ``set advanced-configuration mtu`` command.

2.4.8 Enabling TLS connection fingerprinting

As of V2.5.3.105, a new option enabling JA3 is available.

JA3 will enable retrieving information exchanged during TLS negotiation to detect malicious connections.

This option is only available in v102 compatibility mode.

2.4.9 Adding the community-id for the hash of flows

The addition of the community-id, a hash based on a 7-tuple algorithm, will simplify the analysis of a flow between several detection engines.

2.4.10 Adding the « activehunt » classetype

Adding the classetype « activehunt » to the classification file of the detection engine was made in order to take into account the category related to the rules generated from the CTI LIS.

2.4.11 Grace period granted to the capture interface start-up

As of V2.5.3.105, the grace period for starting up the capture interfaces is configurable.

The following commands were added:

- `` `show interfaces delay` `` to view the current value,
- `` `set interfaces delay` `` to set this value.

2.4.12 Manual assignment of all GCap interfaces

Up until V2.5.3.104, it is possible to:

- view the interfaces using the `` `show monitoring-interfaces` `` command,
- automatically detect interfaces using the `` `set advanced-configuration rescan-interfaces` `` command.

As of V2.5.3.105, the following command is completed for detecting and assigning interfaces: `` `set advanced-configuration interface-names` ``.

It enables the following actions:

- **assigning the physical interfaces of the GCap:**
  - the management interfaces (*gcp0* et *gcp1*)
  - the *mon0* to *monx* or virtual *monvirt* capture and detection interfaces.
- resetting the current assignment and returning to an automatic assignment. This assignment is done with the `` `set advanced-configuration interface-names reset` `` command.

2.4.13 Detection engine grace period option

Up until V2.5.3.104, the grace period for starting the detection engine is only configurable with root rights.

It is related to the loading times of the rules by the detection engine.

From V2.5.3.105 onwards, this grace period can be modified.

The following commands were added:

- `` `show monitoring-engine start-timeout` `` to display the current value,
- `` `set monitoring-engine start-timeout` `` to configure this value.

2.4.14 Sanity-checks option for the detection engine

As of V2.5.3.105, the check for prerequisites to start the detection engine can be enabled or disabled.

This check consists of verifying whether the *monx* capture interfaces that are enabled are properly connected in order to allow the engine to start.

The following commands were added:

- `` `show monitoring-engine start-checks` `` to display the current value,
- `` `set monitoring-engine {disable-sanity-checks|enable-sanity-checks}` `` to activate or deactivate the check.

2.5 vpn-link speed option for the VPN tunnel

From V2.5.3.105 onwards, it will be possible to specify the link quality between the GCap and the GCenter in order to adapt to low speed links.

The following commands were added:

- `show network-config vpn-link speed` to view the current status,
- `set network-config vpn-link speed {fast|slow}` to enable or disable the check.

2.6 Addition of an automatic restart mechanism for crashed services

Up until V2.5.3.104, some services were not restarted when they were inoperative.

As of V2.5.3.105, a mechanism was added to automatically restart crashed services.

2.7 Addition of the possibility of placing a command from the CLI with the SSH connection

From V2.5.3.105 onwards, in order to simplify the automation of interactions with the GCap, it is now possible to issue a single command:

- to connect remotely via SSH,
- to execute a command,
- to display the result of the command,
- to close the remote connection.

Chapter 3

Other features and improvements

3.1 Change of operating system

A complete overhaul of the GCap operating system has taken place at V2.5.3.105.

3.2 Change of the programming language

The main programming language changed to V2.5.3.105.

3.3 Update of the kernel

The operating system kernel was updated to the latest Long-Term Support (LTS) version.

3.4 Performance improvement

3.4.1 Codebreaker performance improvements

From V2.5.3.105 onwards, in order to improve Codebreaker's performance, a new programming language was used and the code was optimised.

3.4.2 Optimising the network communication between the GCap and the GCenter

Up until V2.5.3.104, there was a systematic exchange of files between the GCap and the GCenter.

From V2.5.3.105 onwards:

- only the updated files are compressed and downloaded in several parallel sessions and no longer file by file,

- to manage the sending of eve-logs between GCap and GCenter, a new exchange mechanism was implemented,
- to download configurations and files between the GCenter and the GCap:
  - for the GCenter in V2.5.3.104, rsync was used,
  - for GCenter in V2.5.3.105, there was a new exchange mechanism only compatible with GCenter version 102. For GCenters in version 101, rsync will remain the method used.

3.4.3 Improved load management of *monx* capture interfaces

Up until V2.5.3.104, load balancing from the *monx* capture interfaces to the GCap CPUs was implemented on an experimental basis.

As of V2.5.3.105, this feature has matured although the functionality is only compatible with certain GCap models.

For more information on this enhancement, please contact the Gatewatcher technical support.

3.5 Global security improvements

3.5.1 Network security

3.5.1.1 Stricter isolation of the SSH service using VRF

From V2.5.3.105 onwards, in order to further secure the SSH service, VRFs are used for better partitioning.

3.5.1.2 Redesign of internal firewall rules

As of V2.5.3.105, iptables were replaced by nftables for filtering internal GCap flows and dynamically managed rules were abandoned in favour of static rules predefined according to the GCap status.

3.5.1.3 Redesign of the IPsec management between the GCap and the GCenter

From V2.5.3.105 onwards, in-depth changes to the IPSec service were made in order to improve the stability and security of exchanges between the GCap and the GCenter.

3.5.2 Security system

3.5.2.1 Improved quality of the cryptographic keys

As of V2.5.3.105, an entropy injection mechanism was introduced to improve the quality of the cryptographic keys generated, particularly during the first start-up.

3.5.2.2 Strengthening the SSH service configuration

In V2.5.3.105, the SSH service was tightened up to follow the ANSSI recommendations.

3.5.2.3 Improving process isolation

From V2.5.3.105 onwards, better process isolation is provided by Systemd with a limitation of the memory space allocated to processes, read-only access, and more.

3.5.2.4 PAM policy and account lock management

As of V2.5.3.105, a complete overhaul of the PAM policy and account lock management was carried out.

3.5.2.5 Protection of read-only disk partitions

Starting with V2.5.3.105, partitions containing GCap code are now set to read-only when the server is started and not when the detection engine is started.

3.5.2.6 Changing the root password policy

Starting with V2.5.3.105, the root password is randomly generated. It is no longer available to users of the system.

For more information on this subject, please contact the GATEWATCHER technical support.

3.5.2.7 Sanctioning of configuration management and related right

From V2.5.3.105 onwards, a central system for managing rights and access controls was implemented and requests for configuration changes are submitted to this system.

3.5.2.8 Risk reduction on SUID rights

As of V2.5.3.105, all programs having the SUID property, which are not used, are either removed or disabled.

3.5.2.9 Improved XDP filter support daemon

As of V2.5.3.105, the following improvements were applied to the XDP filter daemon:

- reduction of the attack surface with more dynamic code compilation, hardening of the daemon, and more.
- increased performance.

3.5.2.10 Improved Netdata security

As of V2.5.3.105, the native Netdata measurement modules are replaced by a secure daemon developed by Gatewatcher.

3.5.2.11 Creation of a specific initrd image

From V2.5.3.105 onwards, a secure initrd image, generated by Gatewatcher, is now being used.

3.5.2.12 Replacement of the start-up system

As of V2.5.3.105, the OpenRC initialisation system is replaced by systemd.

3.6 Changes to the CLI

3.6.1 Changing the scope of interface-related commands

Until V2.5.3.104, the commands enabling the interaction with the detection interfaces were:

- `` `show monitoring-interfaces` ``,
- `` `set monitoring interfaces` ``.

From V2.5.3.105 onwards, the management interfaces and the detection interfaces are managed by the same commands:

- `` `show interfaces` ``,
- `` `set interfaces` ``.

3.6.2 Selecting the protocols to be analysed by the detection engine

Until V2.5.3.104, the selection of protocols to be analysed by the detection engine was done via the GUI or the `` `Protocols-selector` `` command.

From V2.5.3.105 onwards, this function is handled via the detection engine rules, so it is managed by the GCenter.

The `` `Protocols-selector` `` command was therefore removed from the CLI.

3.6.3 The configuration GUI is marked obsolete

As of V2.5.3.105, the GUI is considered deprecated or obsolete.

The new features will therefore only be fully usable through the CLI.

3.7 Features available for extracting diagnostic data to Gatewatcher technical support

In order to easily collect the data necessary for diagnosis by Gatewatcher technical support, an automated extraction of the GCap operating data was developed.

This extraction is performed by using the `` `tech-support` `` command of the `` `show` `` subgroup.

3.8 Changing the driver reload strategy

Up to V2.5.3.104, a reboot was performed with a driver shutdown and then a service reboot + file load: `` `system restart-drivers` `` command.

From V2.5.3.105 onwards, a reload of the configuration files is performed: `` `system reload-drivers` `` command.

3.9 Modification of the crisis management strategy (emergency mode)

From V2.5.3.105 onwards, disk space management was added with the implementation of quotas to avoid the saturation of these spaces that would render the GCap inoperative.

If these quotas are exceeded, emergency mode is triggered, which dynamically changes the GCap's data retention time to 2 minutes.

Thus all files older than this retention time will be deleted, starting with the oldest until the emergency mode is exited.

For further information on this feature, please consult the documentation.

Chapter 4

Patches

4.1 Eve-logs are automatically truncated if size > 65536 bytes

Up until V2.5.3.104, the detection engine automatically truncates eve-logs that are larger than 65536 bytes and does so in an abrupt manner that corrupts the following eve-log.

From V2.5.3.105 onwards, this truncation is done correctly. As a result, the truncated eve-log is not processable yet it does not corrupt the following eve-log.

4.2 TCP transactions and extracted files (« unknown »)

TCP sessions operating in the following manner prevent the GCap from properly rebuilding a file at the GCenter:

- Initial 3-way handshake,
- Sending the entire file with the PUSH flag without intermediate ACK,
- ACK all segments and close the connection with RST.

This erroneous report disrupts the operation of the GCap and the file is not sent correctly to the GCenter.

A partial fix was present in versions greater than or equal to V2.5.3.104 (file « unknown »).

This problem is completely fixed in V2.5.3.105.

4.3 Using RELP protocol and adding a queue between GCap and GCenter

During a communication problem between GCap and GCenter, sending system logs could be disrupted (loss of information).

Using the RELP protocol and adding a queue for sending these logs enables this problem to be overcome in V2.5.3.105.

4.4 Protection of the authentication mechanism (anti-bruteforce)

The authentication attempt counter is incremented whenever a login attempt is made, even if no password is entered by the user.

This problem is completely fixed in V2.5.3.105.

4.5 HTTP parsing problem

Some HTTP requests analysed by the Sigflow engine are not correctly parsed. This causes a loss of information in the data sent back to the GCenter by the GCap.

The updated parser corrects this problem in V2.5.3.105.

4.6 Problem when replaying some pcap files

In some cases, replay of pcap files through the *monvirt* interface does not work properly due to an MTU problem.

The ability to configure the MTU of the *monvirt* interface in V2.5.3.105 fixes this problem.

4.7 Problem replaying pcap files with multi-tenancy enabled

The « replay pcap » function is not operational when multi-tenancy per interface is enabled.

This problem is fixed in V2.5.3.105.

4.8 Display of the GCap status as « undetermined » in the GCenter management interface

Incorrect display of the GCap status in the GCenter interface can be caused by various problems.

One of the causes is the crash of a service (gcap-heartbeat) that is not restarted.

The change in managing GCap services by implementing an automatic restart of services corrects this problem in V2.5.3.105.

4.9 Erroneous status display of the monitoring interfaces

In some cases, the monitoring interface status is not displayed correctly in the configuration utility. This problem is fixed in V2.5.3.105.

Chapter 5

Known problems and limitations

5.1 Netdata: displaying information in the GCenter v101 WebUI

Redesigning and adding new information at the Netdata level renders the graphs and statistics displayed in the GCenter 101 WebUI inoperative.

However, the data can still be viewed via the Netdata API.

5.2 Changing the MTU of a VPN interface and tunnel

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

This results in the loss of connectivity between the GCap and the GCenter (IPsec VPN) for approximately 4 minutes.

5.3 Restoring the backup on the GCenter.

When restoring the backup to the GCenter, the pairing with the GCaps must be made again.

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
2.5.3.105	2.5.3.100 HF7	Unsupported configuration: GCenter to upgrade to a newer version
2.5.3.105	2.5.3.101 HF2	Configuration ok (limitation during the installation process of the new GCap version)
2.5.3.105	2.5.3.101 HF3	Configuration ok
2.5.3.105	2.5.3.102	Configuration ok

Chapter 7

Hardware compatibility

Version 2.5.3.105 is compatible with all hardware versions of GCap.

STORAGE GCAP REFERENCE	EXTENSION LOCAL	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 V2.5.3.105 update from the GCenter GUI, the GCenter must be 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

1. Download the newly available version and the associated sha256 on the https://update.gatewatcher.com/upgrade/ platform (directory 2.5.3.105).
2. Check the image with the associated sha256.
3. Connect to the GCenter WebUI and go to the menu **Administrators** > **GUM** > **Upgrade**.
4. In the **Upload an upgrade** section, click on **choose a file** and then select the previously uploaded image to make it available on the GCenter. If you encounter a problem uploading the image, please try using a different browser.
5. Connect to the GCap with the SSH account **SETUP**.

6. Run the graphical configuration utility with the **gui** command.
7. Deactivate the monitoring engine and make sure that there are no more eve-logs and files to be transmitted to the GCenter.
8. Go to the **Upgrade** menu.
9. Confirm the upgrade by selecting **"Yes, upgrade this GCap"**. The GCap should restart automatically.
10. Log in to SSH with the **SETUP** account to verify that the update was successfully applied.
11. Re-enable the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

If you have any problems, 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 2.5.3.105).
2. Check the image with the associated sha256.
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. Re-enable the monitoring engine with the **monitoring-engine start** command (GCAP-CLI).

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

PDF Release Note