Release note
GCenter Version 2.5.3.102

Note version: V3

Translated from original manual version 3

Creation date: January, 2023

Last update: May, 2023

Table of contents

Chapter 1

Presentation of GCenter version 2.5.3.102

This release note provides a description of:

- New features and improvements
- Patches
- Known issues
- Software compatibility
- Hardware compatibility
- Hotfixes
- Upgrade procedure

Chapter 2

New features and improvements

2.1 WebUI - New NDR interfaces and options

2.1.1 Home page and global overview table

The new homepage and the new global overview table provide a summary of the strategic risks according to the input chain and the MITRE framework.

2.1.2 Alert dashboard

A new dashboard is available providing a summary of alerts listed by risk level and aggregated by signature.

2.1.3 User dashboard

A new dashboard is available displaying the list of users classified by risk level.

2.1.4 Host Dashboard

A new dashboard is available showing the list of hosts classified by risk level.

2.1.5 Relationship Mapping

On the basis of the various alert feeds, the solution is able to dynamically generate a map of the monitored environment by displaying users, hosts, associated risks, and their relationships.
This new display enables identifying the main threats more quickly.

2.1.6 Investigation dashboards

Browsing the investigation dashboards was revised, creating dynamic filters from other dashboards to make it easier to find items.

2.1.7 Creating Tags

Tags can be created and associated with users, hosts, and alerts.

2.1.8 Creating Notes

Notes can be created and associated with users, hosts, and alerts.

2.1.9 Managing association rules

A new menu is available enabling the customisation of association rules when detecting users and hosts.
It is possible, among other things, to define the IP address subnets concerned, to make static declarations, and to make exclusions.

2.1.10 Limiting metadata

A new menu is available enabling the limitation of the metadata volume indexed by the GCenter for the following protocols: DNS, HTTPS, HTTP, SMB.

2.1.11 Dark Mode

The new graphical interface features the “dark mode” option.

2.2 WebUI – Administration

2.2.1 Configuring GCap probes

The GCap configuration has been simplified for defining network variables, file rules, and activating the various protocols that will be analysed.

2.2.2 Diagnostic menu

Generating tech support is now possible via the GCenter WebUI (Diagnostics menu).

2.2.3 Update menu

In the “GUM” section, the “Hotfix” and “Upgrade” menus have been merged into “Software update”.

2.3 Analysis / CTI features

2.3.1 Host Detection

A new mechanism is now in place to create and maintain a list of all hosts on the monitored network.
This passive detection is carried out thanks to the information from the different protocols analysed by the GCap.

2.3.2 User detection

A new mechanism is now in place to create and maintain a list of all users on the monitored network.
This passive detection is based on information from the Kerberos protocol.

2.3.3 Aggregate risk calculation per host

For each host, a risk assessment is performed based on the individual risks (alerts) and the number of related individual threats.

2.3.4 Unified risk calculation

A new module calculates the risk of each alert triggered by the various analysis and detection engines.

2.3.5 Identifying the type of host

A new mechanism has been introduced to identify the type of host in the monitored network - computer, server, virtual machine, mobile, firewall, and others.
This identification process is primarily based on analysing user-agents and MAC addresses.

2.3.6 Host Identity persistence and enrichment

Host identification data is stored and populated over time to create a summary for each host.
The main information available consists of:

- Host name
- Related IP address
- Assigned MAC address
- Operating system
- Protocols in use and their proportion
- Details of detected threats
- Associated MITRE tactics
- Aggregated risk score
- Risk score timeline
- Top 10 URLs visited
- Top 10 IP addresses contacted
- Tags
- Notes

2.3.7 User identity persistence and enrichment

User identification data is stored and populated over time to create a summary for each host.
The main information available consists of:

- Host name
- Assigned IP address
- Last seen

- Protocols in use and their proportion
- Details of detected threats
- Associated MITRE tactics
- Aggregated risk score
- Risk score timeline
- Top 10 URLs visited
- Top 10 IP addresses contacted
- Tags
- Notes

2.3.8 Connectivity with the CTI

The GCenter is now able to receive feeds directly from Gatewatcher's Cyber Threat Intelligence (named LastInfoSec/LIS) to automatically generate new detection rules.

2.3.9 Retro-Hunting and CTI

A new retro-hunting engine reanalyses past metadata and communications using new IOCs from Gatewatcher CTI (LIS) streams.

2.3.10 Re-directing to the CTI platform

By clicking on an alert it is possible to be redirected to the Gatewatcher CTI platform (LIS) web portal and perform an automatic search in an attempt to obtain additional information about the initial alert. Please note that a specific LIS licence is required to activate this feature.

2.3.11 Alerts: help with investigating and responding

When clicking on an alert, several actions are suggested:

- Redirecting to different dashboards for investigation
- Downloading files (samples)
- Displaying details of the threat
- Sending the sample to a sandbox
- Downloading the report generated by the sandbox

Actions are contextually linked depending on the content of the alert.

In the case of redirecting to a dashboard for investigation, a filter is automatically created with the alert elements in order to improve the user experience and the analysis time.

2.3.12 Associating with the MITRE ATTACK repository

Each alert is automatically associated with the tactics and techniques of the MITRE repository.

2.4 Detection

2.4.1 DGA detection engine

A new version of our Domain Generated Algorithm (DGA) detection engine is available featuring:

- An optimised algorithm to reduce false positives
- Dedicated DGA events with the same alerts as the command and control "C&C" type
- The ability to add domains from a generated alert to a white list or black list

2.4.2 Shellcode detection engine

The Shellcode detection engine (Goasm) has been improved:

- Quota and automatic cleaning added to avoid saturation
- Code is optimised to increase stability and performance
- New Windows features and patches implemented
- The hash (SHA256, md5) in the alerts no longer corresponds to the content of the ".data", but to the analysis results enabling to recognize identical shellcodes in different network frames
- Shellcode alerts include a "Display Data" action to show the hexdump of the ".data"

2.4.3 Powershell detection engine

The Powershell detection engine (Gps) has been improved:

- Quota and automatic cleaning added to avoid saturation
- Code is optimised to increase stability and performance
- Improved extraction, analysis, and scoring to reduce false positives
- The hash (SHA256, md5) in the alerts no longer corresponds to the content of the ".data", but to the analysis results enabling to recognize identical powershell commands in different network frames
- Powershell alerts include a "Display Data" action to show the hexdump of the ".data"

2.4.4 Malcore detection engine

The Malcore detection engine has been improved:

- An orchestrator has been added to detect failures and perform automatic actions to correct them
- 16 detection engines are now activated if the licence so enables
- Improvement of the alert and metadata content that are now extracted from the fileinfo

2.4.5 Yara Rules

Yara rules can be added to the Malcore engine to improve detection capability.

2.4.6 Improved processing of suspicious files

A new option is now provided in the analysis chain to mark suspicious files for automatic reanalysis upon the next engine update, until these files are no longer detected as suspicious.

2.5 API

2.5.1 API and Swagger

The vast majority of possible interactions with the solution can be achieved through the API.

More than 200 API points are available. They are described using Swagger and can be tested through the GCenter WebUI (URL: https://FQDN//docs/swagger/).

2.6 System

2.6.1 Change of operating system

A complete overhaul of the GCenter operating system has taken place at V2.5.3.102.

2.6.2 Update of the kernel

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

2.6.3 Optimising the communication between the GCap and the GCenter

A new component controls the communication between the probe and the manager.
The file transmission mechanism has been optimised with a new communication protocol, database for received files, and more.

2.6.4 File processing mechanism redesign

A complete overhaul of the file processing mechanism has been implemented to:

- improve the reliability of enrichment
- obtain all the information related to a reconstructed file
- be able to systematically find a file from a flow-id

2.6.5 Database for the NDR

A new database has been created to store NDR related data including users, hosts, alerts, risks, and more.

2.6.6 Improved updates

Improvements were made to the solution's update mechanism.

2.6.7 Performance optimisation for access to event related data

A complete overhaul of the architecture used to process and store event data was carried out.
This enables optimising response times and limiting the problems linked to an excessive amount of stored data.

2.6.8 Netdata: increased retention time

The retention time for metrics reported via Netdata has been increased.

2.6.9 Licences

A new, more detailed licensing system is available.

Chapter 3

Patches

3.1 Status of the latest updates

When restoring a GCenter, information related to the signature update status on GCaps is not restored.
The status will update when the GCap retrieves a new rule file.

This problem is fixed in V2.5.3.102.

3.2 Pairing to a GCAP is not possible if there is no gateway set for the VPN interface

Pairing between the GCenter and the GCap will fail if there is no default gateway set when configuring the network interface *mgmt0* of the GCenter.
The error message sent back by the GCap when pairing is `Can't connect to \<Gcenter IP\>`.
This happens even though the GCap and GCenter are in the same subnet and a default gateway should not be required.

This problem is fixed in V2.5.3.102.

3.3 Pairing to a GCAP is not possible after the GCenter network configuration has been changed

After reconfiguring the network settings of the GCenter's VPN interface (e.g. IP, subnet, FQDN), it is possible that re-pairing with a previously paired GCap will no longer work.
Upon pairing, the GCap will display the following error message: `pairing not established`.

This problem is fixed in V2.5.3.102.

3.4 LastInfoSec rules

Inconsistency between the LIS rules and the generated file, as the rules with the hashes are missing.

This problem is fixed in V2.5.3.102.

3.5 Machine Learning engine and CIE editing

The GATEWATCHER tables of the Machine Learning engine do not take into account the license restriction if the GCenter is a CIE edition.

This problem is fixed in V2.5.3.102.

3.6 Netdata Export - Netdata versions higher than 1.19 are not compatible

Exporting GCAP/GCENTER monitoring statistics to an external Netdata is only compatible with a Netdata server whose version is equal or lower than 1.19.
In higher versions, the data is exported and can be queried within the external Netdata. However, an error in the graphic interface occurs and it is impossible to view the data.
This does not affect GCenter, only the external Netdata server.

This problem is fixed in V2.5.3.102.

3.7 GScan - Edition *Critical Infrastructure Edition* (CIE)

The GScan functionality does not take into account the license restriction if the GCenter is a CIE edition.

This problem is fixed in V2.5.3.102.

3.8 DGA - Field not present

The absence of the `dga_probability` field in the events will be done if the following conditions are met:

- The activation of logging on DNS event types
- Activation of the DGA Detection Machine Learning module
- A heavy DNS network load

This problem is no longer apparent because in V2.5.3.102 dedicated events exist for the DGA.

3.9 Third Party - Intelligence

Interconnection configuration with intelligence raises a 500 error if the token is incorrect.

This problem is fixed in V2.5.3.102.

3.10 Kibana - Inaccessible tables

KIBANA tables may not be displayed after a restart on GCenter and/or the WEB interface.
The error message displayed is `Elastic did not load properly. Check the server output for more information`

This problem is fixed in V2.5.3.102.

3.11 Kibana - “Not ready yet”

In a few special cases, a failure of the log rotation system can lead to the /var/log/ partition being saturated. This results in a `not ready yet` error message in Kibana.

This problem is fixed in V2.5.3.102.

3.12 Malcore Management - GScan Profile

The `Number of files` option in Malcore Management's GScan profile enables an alert to be issued based on the number of files in the archive.
This feature is not operational.

This problem is fixed in V2.5.3.102.

3.13 Malcore - Incorrect healthcheck status in *Critical Infrastructure Edition* (CIE) license

The health status of the Malcore engine may be incorrectly displayed on the home page in global **status/healthcheck**.
This can happen when the GCenter is running with the **CIE** license: the healtcheck may display *Malware Analysis engine has one or more issues*, even if the engine is running.

This problem is fixed in V2.5.3.102.

3.14 Malcore - No flow_id

In rare cases, the `flow_id` field of a Malcore alert may not appear.
Correlation with the metadata for this Malcore event can be made using the SHA256 and timestamp_detected of the Malcore alert.
From version 2.5.3.101-HF2 onwards, if the `flow_id` is missing, it is set to 0, enabling the export of alerts.

This problem is fixed in V2.5.3.102.

3.15 Malcore - Duplicate Analysis

Malcore analysis duplicates can occur during elasticsearch database shrinking operations.
These operations take place every day at 02:00 UTC. They aim at optimising the memory consumption of elasticsearch by reducing the number of shards per index.

his problem is fixed in V2.5.3.102.

3.16 Malcore - Engine crash due to an overload

The Malcore engine can become unstable if it is under extreme load and hundreds of thousands of files are waiting to be processed.
This results in a total blockage of the engine (no more analysis) or a very significant reduction in the number of analyses being performed.

This problem is fixed in V2.5.3.102.

3.17 Malcore - analysis engine saturation

If the speed of rebuilding files on the GCap is faster than the speed of Malcore analysis, a queue is formed at the GCenter. This causes engine saturation and loss of real time in Malcore alerts.

This problem is fixed in V2.5.3.102.

3.18 Malcore - Service discontinued due to saturation

In exceptional cases, if the Malcore analysis queue holds several thousand large files, a slowdown or stoppage of the service may result.

This problem is fixed in V2.5.3.102.

3.19 Malcore - Disabling an antivirus engine

The Malcore solution is made up of 16 detection engines.
One of the engines is causing malfunctions. It was disabled in version 2.5.3.101-HF2.
This can be seen in the `total_found` field of the Malcore logs which is XX/15.

This engine was re-enabled in V2.5.3.102 and this can be seen in the ``total_found`` field of the Malcore logs which is XX/16.

3.20 Malcore - Export logs with flow_id=0

In rare cases, the `flow_id` field of Malcore logs is not set, preventing them from being exported.

This problem is fixed in V2.5.3.102.

3.21 Malcore - Inconsistent healthcheck webui and update status

On the GCenter administrator home page, there is a graphical inconsistency between the `Updates Status` panel and the `Malcore Update Status` panel.
These two panels alert the user if updates are older than 7 days:

- The first does so after a period of time strictly longer than 7 days
- While the second one does so for a duration greater than or equal to 7 days

This problem is corrected in V2.5.3.102 with the complete redesign of the healthcheck page.

3.22 Malcore enrichment error on the `app_proto` field

In the Malcore logs, the `app_proto` field specifies the protocol by which an analysed file was transported.
If the same file is transported by two different protocols, for example HTTP and then SMTP, for the duration of the file_resend_interval (configurable in `Operator > Gcap profiles > Base variables > File resend interval`):

- An initial log replica=false with app_proto=HTTP will be generated
- Then a second log with replica=true will be issued. The `app_proto` field will be set to HTTP, when it should have been set to SMTP

This problem is fixed in V2.5.3.102.

3.23 Inconsistency in the Malcore alerts on the `total_found` field

In Malcore alerts, in some instances, the `total_found` field and the `engine_id` number are not identical.

This problem is fixed in V2.5.3.102.

3.24 API - Authentication parameter

Requests to the GCenter API use the API-KEY keyword to provide the authentication token as a parameter. In swagger (https://HOSTNAME-GCENTER/docs/swagger/) the example of generated requests use the keyword *apikey*.

This problem is fixed in V2.5.3.102.

3.25 API - endpoint */api/alerts* not working

The */api/alerts* endpoint of the GCenter API is not working:

- When using descending date sorting, a 500 error is returned if the page parameter is not set or equals 1
- The page parameter determines the number of results returned instead of the specified
- The page_size parameter is not taken into account

This problem is fixed in V2.5.3.102.

3.26 Proxy - Error 500 if unable to resolve name

If the proxy specified in Configuration/Proxy Configuration cannot be resolved by the DNS server configured for the GCenter, then this produces two errors:

- A 500 error in the proxy configuration page (/configuration/proxy_settings/);
- An error in the GUM configuration menu (/gum/configuration

This problem is fixed in V2.5.3.102.

3.27 Gcenter-setup - error message

When running *gcenter-setup*, the following error message may appear:

```
`Could not connect to home directory /nonexistent: No such file or directory`.
```

This does not interfere with GCenter's operation in any way.

This problem is fixed in V2.5.3.102.

3.28 LDAP Configuration - TLS

User management can be achieved by connecting the GCenter to an Active Directory or other solution running LDAP via `Accounts/LDAP.configuration` menu.
If an LDAP server is used with TLS settings, the status visible in the `LDAP interconnection status` configuration panel may indicate an error even though the configuration is operational.
The error displayed is as follows:

```
`Cannot connect to LDAP with current settings: {'desc': "Can't contact LDAP server",
↪'errno': 115, 'info': '(unknown error code)'}`.
```

This problem is fixed in V2.5.3.102.

3.29 LDAP with SSL or STARTTLS

If LDAP is configured with SSL or STARTTLS and uses a certificate to validate the server, it may disappear when changing the configuration via the GCenter WebUI.
However, it is well preserved and used.

This problem is fixed in V2.5.3.102.

3.30 Syslog export: no Malcore analysis of “unknown” files

A bug affecting the suricata engine under very specific conditions can result in the appearance of so-called *unknown* files. This means that the metadata could not be recovered by suricata.
See detailed description of conditions here.
The Malcore analyses for these files are viewable in Kibana, but are not exported via syslog.

This problem is fixed in V2.5.3.102.

3.31 Syslog export: behaviour during saturations

If the throughput of the logs to be exported is such that it saturates the syslog export, gcenter will first process the metadata events in a *best-effort* manner (possible losses) in order to preserve the export of sigflow, Malcore, and codebreaker alerts.

This problem is fixed in V2.5.3.102.

3.32 Syslog export - Exceptions in log formats

Minor inconsistencies may exist in Malcore (malware index) logs when exported.
The following fields can be of integer type, without quotes around the field value, or of string type with quotes:

- *src_port*
- *dest_port*
- *detail_scan_time*

For example:

- “src_port”: “25”
- or “src_port”: “25”.

This problem is fixed in V2.5.3.102.

3.33 Syslog export - duplicate sigflow alerts

In the syslog export, logs of type “sigflow alert” (type=suricata AND event_type=alert) are sent twice.

This problem is fixed in V2.5.3.102.

3.34 Redirect Trackwatch Logs to the Syslog dashboard

If one clicks on `Administrator > Gcenter > Trackwatch logs`, the user is redirected to the `Tactical` dashboard instead of the `Syslog` dashboard.

This problem is fixed in V2.5.3.102.

3.35 Default accounts reactivated

When configuring a GCenter, the default accounts *administrator* and *operator* must be disabled or the password changed.
If an upgrade is performed, these accounts are reset to their default values and reactivated.

This problem is fixed in V2.5.3.102.

3.36 Default activation of the CIP/ENIP protocol

The CIP/ENIP protocol parsing is enabled by default. It cannot be disabled in the GCenter interface.

This problem is fixed in V2.5.3.102.

3.37 Display bug for adding IPs in the external_net section

In `Operator > Gcap profiles > Netvariables` , if one tries to add an EXTERNAL_NET of the list type with a mask other than /24, a display bug prevents the network from being added.

This problem is fixed in V2.5.3.102.

Chapter 4

Known problems and limitations

4.1 Netdata export - temporary lack of information

When repeatedly enabling/disabling the netdata export, the monitoring information related to the detection probes may become momentarily unavailable for a period of 5 to 20 minutes.

Workaround: No solution.

4.2 GCenter Backup/Restore - Error management

If an error is made by the user when following the restoration procedure, the menu progress bar remains blocked and no error message can be seen in the WebUI.

Workaround: No solution.

4.3 GCenter Backup/Restore - Pairing GCap

Following a GCenter backup, if the GCap pairing is deleted, then restoring the backup will not enable restoring the connection with the previously deleted GCap.

Workaround: Reapply the pairing.

4.4 Disable LDAP configuration with LDAP server off

Disabling an LDAP configuration generates an error if the LDAP server is inaccessible.

Workaround: Make a valid LDAP configuration with the accessible LDAP server in order to disable the desired configuration

---

4.5 Incorrect GCap status after updating the GCenter

The status of the GCap may be erroneous following the GCenter update (Last update = unknown / Status: Online but update outdated)

Workaround: Reapply the ruleset configuration at the GCap level.

4.6 Kibana - Maps GeoIP

Viewing GeoIP information within Kibana dashboards is impaired.

Workaround: No solution.

4.7 Sigflow Manager - Transform Category

Applying a Transform category raises a 500 error if no ruleset is available on GCenter.

Workaround: Create a ruleset.

4.8 Sigflow Manager - Error 500 when adding a rule to a custom source

Adding a rule raises a 500 error if the following conditions are present:

- The rule is added by editing a custom source;
- The rule already exists in another custom source (same SID)

Workaround: Change the rule's SID that is to be added in order to avoid the SID conflict.

4.9 Sigflow Manager - Inconsistency in the display of the number of categories and rules of a category

The `Sigflow > Sources` homepage shows the number of categories and rules contained in each source.
It is possible that the information displayed is inconsistent with the sources' actual content.
This situation may occur after editing a custom source or an update.

Workaround: No workaround.

4.10 LDAP configuration made in v2.5.3.100 and never modified since generates an error

The LDAP configuration made in v2.5.3.100 and never modified since causes a problem when migrating to v2.5.3.102.

Workaround : This problem is fixed in V2.5.3.102-HF1.
If in doubt, please contact Gatewatcher technical support.

4.11 Sigflow configuration - custom source name cannot contain space

In the Config - sigflow/sources screen of the legacy web UI, it is possible to define a custom source of signatures for the Sigflow detection engine.
During the addition procedure, the source name must be entered.
This name must not contain any space otherwise it will generate an error.

Workaround: Change name by removing spaces.

4.12 Not enought storage for ElasticSearch indices

In v2.5.3.102, ES indices have been migrated to a more performant storage but it reduces space available to keep the data.

Workaround: This problem is fixed in V2.5.3.102-HF1.
Please refer to the procedure in the Hotfix section of this release note.
If in doubt, please contact Gatewatcher technical support.

4.13 A component crashes when it receives an empty evelog

In v2.5.3.102, sending an empty evelog causes the crash of a Gcenter component.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.14 ActiveHunt - Problem with SID duplication

In v2.5.3.102, in somes cases ActiveHunt could generate Sigflow rules with a duplicate SID.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.15 LDAP - Problem to activate the module

In v2.5.3.102, in somes cases, activating LDAP module is impossible .

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.16 GCenter Backup/Restore - Problem with NDR dashobards

In v2.5.3.102, after restoring a backup NDR dashboards are no longer operational.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.17 GCenter Backup/Restore - network configuration

In v2.5.3.102, when a backup file is applied, network configuration of MGMT0 is restored which it can cause issues.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.18 GCenter Backup/Restore - error with FQDN

In v2.5.3.102, when restoring a backup, if the FQDN of the target GCenter is different then an error occurs.

Workaround: Need to change GCenter FQDN and restart.

4.19 GCenter Backup/Restore - build number

In v2.5.3.102, it's impossible to identify the build number of a backup file.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.20 NDR - data deletion

In v2.5.3.102, when an administrator triggers a manual data deletion (in `Data Management > Data Deletion`), some data of NDR dashboard are not correctly deleted.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.21 WebUI - Access problem when MTU is modified

In v2.5.3.102, in some cases, If the MTU of MGMT0 is decreased, the WebUI access is no longuer possible.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.22 Upgrade - problem with the counters of files waiting to be analyzed

After an upgrade to v2.5.3.102, in some cases, the counters of the pending files no longer change and display an incorrect value.

Workaround: This problem is fixed in V2.5.3.102-HF1.

4.23 Upgrade - problem when Codebreaker processes payloads

After an upgrade to v2.5.3.102, in some cases, Codebreaker is not able to process payloads.

Workaround: This problem is fixed in V2.5.3.102-HF1. A problem could persist with the counters of files waiting to be analyzed.
If in doubt please contact Gatewatcher technical support.

4.24 Upgrade - problem with Syslog export when TLS is enabled

After an upgrade to v2.5.3.102, Syslog export, with TLS enabled, is no longuer operational.

Workaround: This problem is fixed in V2.5.3.102-HF1

4.25 Upgrade - problem of communication between internal components

After an upgrade to v2.5.3.102, communication between some components is no longuer operational.

Workaround: This problem is fixed in V2.5.3.102-HF1

4.26 WebUI - problem when a search is performed with a specific date range

On WebUI, in the NDR dashboards, when a search is performed with a specific date range, the search over a period of time is done in UTC while the results are displayed in UTC+1.

Workaround: This problem is fixed in V2.5.3.102-HF1

4.27 WebUI - problem to update password and user profil

Users belonging to Administrator group are not able to update their password or edit their profil throught the WebUI.

Workaround: This problem is fixed in V2.5.3.102-HF1

4.28 WebUI - display problem when some specific protocols are enabled

When some specific protocols are enabled, this can cause errors in some NDR dashboards.

Workaround: This problem is fixed in V2.5.3.102-HF1

4.29 Error code 500 after the modification of the storage for ES data

Following the change of ES data storage media, a temporary 500 error may appear when accessing Kibana.

Workaround: Wait few minutes.

4.30 Kibana - problem with shortcuts generated through NDR interface

When using the `Go hunting` feature in the NDR alerts dashboard, there is a time issue in the Kibana redirect.

Workaround: This problem is fixed in V2.5.3.102-HF1

Chapter 5

Software compatibility

5.1 Compatibility with GCap

GCenter version	GCap version	Compatibility
2.5.3.102	2.5.3.104	Unsupported configuration: Gcap is to be migrated in advance of the GCenter update
2.5.3.102	2.5.3.105 (or +)	Configuration ok

Chapter 6

Hardware compatibility

Version 2.5.3.102 is compatible with all hardware versions of GCenter.

GCENTER Reference	Local storage	Other storage	Interface network	Power electrique
GCENT8100r2	2 x 960GB RAID1	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9100r2	4 x 480GB RAID5	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9900r2	10 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W
GCENT10500r2	12 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W

Chapter 7

Hotfix

7.1 Package 1

Package 1 - Hotfix (HF1 / SHA256)
Package 1 - Upgrade/Install (HF1 / SHA256)

Hotfix 1 applies to the following versions:

- version 2.5.3.101-HF4
- version 2.5.3.102

If you want to update a Gcenter v.2.5.3.102, apply the **Package 1 - Hotfix** via the `GUM > Software Update` menu.
If you want to upgrade a Gcenter v.2.5.3.101-HF4 , apply the **Package 1 - Upgrade/Install** via the `GUM > Upgrade` menu.

Hotfix 1 corrects the following problems:

- *Migration - LDAP configuration made in v.2.5.3.100 and never modified since*
- *Limiting the storage of indexed data in ElasticSearch*
- *Crash of a component when receiving an empty evelog*
- *ActiveHunt - SID duplication issue*
- *LDAP - LDAP activation issue*
- *GCenter Backup/Restore - NDR Dashboard Issues*
- *GCenter Backup/Restore - network configuration*
- *SaGCenter Backup/Restore - version number*
- *NDR - Data deletion*
- *WebUI - Access problem when changing the MTU*
- *Migration - Problem with pending file counters*
- *Migration - Problem in the analysis of Codebreakers payloads*
- *Migration - Problem with Syslog export to TLS*
- *Migration - Communication problem between some components*
- *WebUI - Problem when searching over a period of time*
- *WebUI - Password change and profile editing issue*
- *WebUI - Display problem when some protocols are enabled*
- *Kibana - Problem with shortcuts generated via NDR interface*

7.2 Storage Media Migration Procedure

Hotfix 1 added an additional command in the configuration menu: `` `Elasticsearch storage mode` ``.
This command moves the ES indexes:

- can be moved from HDD disks to SSD disks
- can be moved from SSD disks to HDD disks

As part of the installation of the HF1, the ES indexes have been migrated to the best-performing GCenter storage (SSDs) which limits the volume available for storing this data.
If the size reserved for ES indexes has become too low, it is possible to transfer ES indexes to HDD disks (disk space will be larger but the access time will be longer).

To perform this transfer from SSD disks to HDD disks, perform the following procedures:

7.2.1 Verification procedure

- Access the configuration menu in SSH with the setup account
- Use the `` `Elasticsearch storage mode` ``
  In the `` `Elastic storage mode` `` window, the `` `Current storage type` `` line indicates the current configuration :
  - if the parameter is `` `slow` ``, it means that the ES indexes are already located on the HDD drives
  - if the parameter is `` `fast` ``, it means that the ES indexes are located on the SSD: perform the following procedures
- In the `` `Elastic storage mode` `` window, the following information is displayed (the values given here are an example):

```
Current storage type: fast
Maximum size on fast storage for elasticsearch: 411G
Maximum size on slow storage for elasticsearch: 1.8T
Current space used by elasticsearch: 273G
```

- In this example:
  - ES indexes are located on SSD disks
  - current size is 273G
  - Maximum size is 411G on SSD disks
  - Maximum size will be 1.8T on HDD disks if ES indexes are transferred

7.2.2 Transfer procedure

- In the `Elastic storage mode` window, click the `Switch storage type` button.

  The following window gives information on:
  - Data preservation
  - The duration of the operation
  - Maximum size available on HDD disks
  - The chosen size of the space reserved for the ES indexes after the transfer: this value can be modified via the WEB UI
  - The current size of ES indexes
- Click on the `Switch storage type and launch data migration` button.

  The following window gives information on:
  - Configuration preparation: when the parameter is `Done` then the transfer begins
  - Transfer progress: transferred value / total value
  - Reconfiguration of storage mode
- Wait for the progress to display the same values and click on the `Refresh` button.

  The procedure is over.

  You go back to the initial window, but the line `Current storage type` is now `slow`.

Chapter 8

V101 to V102 upgrade procedure

8.1 Prerequisites

To install the **V2.5.3.102** update :

- The GCenter must be running **V2.5.3.101-HF3** or higher
- The GCap will need to be version **V2.5.3.105** or higher
- If an LDAP configuration exists in **v2.5.3.101**, redo this configuration in **v2.5.3.101** before migration to **V2.5.3.102**

  Important:

  For an upgrade to V2.5.3.102, you must use the following package to avoid some issues: https://update.gatewatcher.com/upgrade/2.5.3.102/gcenter/gcenter_2.5.3.102-8541~prod-hf1.gwp

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

  Important:

  It is highly recommended to have an iDRAC type connection in order to be able to connect post-upgrade if a problem occurs during the process.

  Important:

  Before proceeding with the update, it is strongly recommended to backup the GCenter configuration in the **Administrators** > **Backup** / **Restore** > **Operations** menu and save the file to an external server in a directory indicating the current GCenter version (example: 2.5.3.102-XXXX-HFX).

8.2 Retained data

The entire configuration of the GCenter is retained.
The data, both metadata and alerts, will have to be migrated beforehand with a specific hotfix. Please refer to the data retention installation procedure below.

Important:

Once migrated, the data will only be available through the Discover menu in the Kibana (Hunting) interface.

8.3 Installation procedure with data retention

1. Make sure the GCap probes are in version **V2.5.3.105** or higher, otherwise refer to the following update procedure: https://releases.gatewatcher.com/fr/gcap/2.5.3/105/8_upgrade_procedure.html
2. Download the newly available version of GCenter and the associated sha256 on the https://update.gatewatcher.com/upgrade/ platform (directory 2.5.3.102).
3. Check the image with the associated SHA256.
4. Download the hotfix enabling the preparation of data before migration: https://update.gatewatcher.com/hotfix/2.5.3.101/gcenter/gcenter_2.5.3.101_hf_data-preparation-for-2.5.3.102.gwp and the related sha256.
5. Check the image with the associated SHA256.
6. Connect to the GCenter WebUI and go to the menu `Administrators > GUM > Hotfix`.
7. In the `Uploading a new hotfix package` section, click on the `Choose a file` button, select the previously uploaded hotfix then click on `Send hotfix`.
8. Again in the GCenter WebUI, go to the `Administrators > GUM > Upgrade` menu.
9. In the `Upload an upgrade` section, click on the `Choose a file` button, select the new GCenter version previously uploaded and click `Submit`.
10. Connect to the GCap with the SSH account **setup**.
11. Shut down the monitoring engine with the following command: `monitoring-engine stop`.
12. Change the compatibility mode using the following command: `set compatibility-mode 2.5.3.102+`.
13. Start the monitoring engine with the following command: `monitoring-engine start`.
14. Return to the GCenter WebUI, in the menu `Administrators > GUM > Hotfix`.
15. In the `Saved package list` section, at the location of the previously sent hotfix click on the `Apply` button.
16. Once activated, connect to the GCenter via SSH with the **setup** account.
17. Go to the new menu available `data persistence`.
18. In the `Warning data preparation` menu carefully read the warning and then click on `Continue (reversible)` to continue.

    The next menu provides the option of deleting the oldest data (indexes) to speed up the migration process so that the migrated data can be stored in the new architecture.

Important:

There may be some data present that is older than the configured retention time.
This data will be automatically deleted once the V2.5.3.102 upgrade is completed.
Therefore, it is important to manually delete this data at this stage.
To check the configured retention time, log into the GCenter WebUI then go to the `Administrators > GCenter > Configuration > Global settings menu`.
The configuration is located in the entry “Data retention (in days):”

Important:

The architectural changes in V2.5.3.102 imply a limitation in the amount of data retained extending to 95% of the partition.
The backup partition is no longer used for storing data related to Elastic Search.
This behavior can be changed in the next hotfix.

19. To delete indexes, select those that should not be retained and click on `Delete selected indices(irreversible)`.
20. Once this is done, click on `Continue (reversible)`.
21. The following menu displays the various phases of the migration and their status, click on `Continue (reversible)`.
22. The last window enables launching the migration that will then be irreversible, click on `Launch data preparation (irreversible)`.

Important:

The migration time will depend on the material and the volume of data to be migrated.
On average, it will take 1 hour for 100GB.

23. The following menu displays the various phases of the migration and their status, click on `Refresh` to see the progress of the operation.

    When the operation is complete, if all the steps are green **true**, it means the migration was successful, if not, please contact Gatewatcher technical support.
24. Exit the **setup** menu, connect to the GCenter WebUI, then go to the `Administrators > GUM > Upgrade` menu.
25. In the `Saved package list` section, under the previously sent update, click on the `Apply` button.
26. Once the operation is complete, restart the GCenter by connecting via SSH with the **setup** account and then going to the `Restart` menu.
27. Once the GCenter is restarted, connect to the WebUI and check whether new events appear in the `Hunting` section (Kibana interface).

8.4 Installation procedure without data retention

1. Make sure the GCap probes are in version **V2.5.3.105** or higher, otherwise refer to the following update procedure: https://releases.gatewatcher.com/fr/gcap/2.5.3/105/8_upgrade_procedure.html
2. Download the newly available version of GCenter and the associated sha256 on the https://update.gatewatcher.com/upgrade/ platform (directory 2.5.3.102).
3. Check the image with the associated sha256.
4. Connect to the GCap with the SSH account **setup**.
5. Shut down the monitoring engine with the following command: `monitoring-engine stop`.
6. Change the compatibility mode using the following command: `set compatibility-mode 2.5.3.102+`.
7. Start the monitoring engine with the following command: `monitoring-engine start`.
8. Connect to the GCenter WebUI and go to the menu `Administrators > GUM > Upgrade`.
9. In the `Upload an upgrade` section, click on the `choose a file` button, select the new GCenter version previously uploaded and click on the `Submit` button.
10. In the `Saved package list` section, under the previously sent update, click on `Apply`.
11. Once the operation is complete, restart the GCenter by connecting via SSH with the **setup** account and then going to the `Restart` menu.
12. Once the GCenter is restarted, connect to the WebUI and check whether new events appear in the `Hunting` section (Kibana interface).