RADIO DATA NETWORKS

Application notes

RAy3
SNMP

version 1.3
2023-01-11

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

Table of Contents

1. Introduction - Simple Network Management Protocol

SNMP is a simple, widely used and useful standardised protocol typically used by Network Management Software (NMS) to read values from devices. Values can be obtained at regular intervals or on requests, saved to a database and then displayed as graphs or tables.

SNMP also enables devices to generate (trigger) the alarms by themselves and notify the NMS explicitly (SNMP traps).

1.1. How does SNMP work?

SNMP requires two parties for communication:

1. *SNMP "manager"* (software installed at your computer)
   - You can use commercial software or free software such as Zabbix, Zenoss, Nagios, Cacti, etc. If you want to read values manually, you can use tools such as snmpwalk, snmpget or Mibbrowser software.
2. *SNMP "agent"* (a part of firmware in remote devices such as RAy3)
   - The agent receives SNMP requests to query information and responds to the manager. Several managers may read values at once and they can send their requests at any time. Alternatively, the agent sends SNMP traps whenever the monitored values are outside the threshold range (RAy3 alarm management). RAy3 is capable of sending SNMP traps to one SNMP manager.

1.2. SNMP communication

In SNMP, each value is uniquely identified using Object Identifier (OID).

The standard SNMPv1/v2c communication starts by sending a request and then the response is returned. Alternatively, an agent can send an SNMP trap.

A **request** is sent	the manager sets message-type to GET, includes OID for the required value and sets this value to NULL.
A **response** is returned	the agent sets message-type to RESPONSE and sends the requested value along with its OID back to the manager.
A **trap** is sent	to the manager without its request.

1.2.1. Basic Message Types

GetRequest	returns a single value.
GetNextRequest	returns the next value (using the next OID).
GetBulkRequest	returns several values in a single packet (useful for data bandwidth optimization)
Trap	sent from the agent to the manager whenever any monitored value is beyond its thresholds.
SetRequest	used to set various parameters (unsupported by RAy3).

1.3. MIB database – Management Information Base

The MIB is a virtual database used for managing the entities in a communications network. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. “Higher-level” MIB OIDs belong to different standards organizations, while “lower-level” OIDs are allocated by associated organizations (e.g. RACOM).

OID example:

Name	productName
OID	.1.3.6.1.4.1.33555.4.1.1.1
MIB	RacomRay3
Syntax	DisplayStringRaw (OCTET STRING) (SIZE(0..16)). Hi..
Access	read-only
Status	current
DefVal	
Indexes	
Descr	Product name.

As you can see, numbers 1.3.6.1.4.1.33555 are the “higher-level” OIDs. The “lower-level” OIDs are .4.1.1.1 which are allocated by RACOM.

2. Simple Network Management Protocol in RAy3 Units

RAy3 utilises SNMP versions **SNMPv1** and **SNMPv2c** – using a **community string** for authentication, which is by default “**mwl-snmp**“, but can be changed. SNMP uses UDP protocol for communication; delivery checks are implemented from version 2 onwards.

Note

The RAy3 MIB module complies with Severity level 3 validation.

By default RAy3 uses UDP port 161 (SNMP) for queries. The manager, which sends the query, dynamically chooses the source port. The use of destination port 161 is fixed. RAy3 replies from port 161 to the port dynamically selected by the manager.

RAy3 launches the SNMP agent automatically on start-up if enabled. RAy3 also sends alarm states (traps) to the manager via the port 162 (SNMPTRAP).

Note

To see the RAy3 MIB table, download it from the RAy3 web interface (**Maintenance** → **Backup** → **SNMP MIB** → **Download**) and use any document reader you prefer.

Note

Since RAy3 FW 1.0.14.0, the SNMP non-table items OIDs are defined in accordance with the RFC (ending '.0') - to improve SolarWinds compatibility. Keep this in mind when upgrading RAy3 firmware. Firmwares < 1.0.14.0. are able to reply to SNMP queries with OIDs ending with .0, but the reply does not contain .0 in its OID. This works fine (for example) with Zabbix NMS, but (for example) SolarWinds does not accept such replies.

Important

Since RAy3 FW 1.0.16.0, the SNMP product OID of RAy3 changed from '1' to '4'. Keep this in mind and replace the older RAy3 NMS configuration. Find more details in *Section 3.1.1.3, “RAy3 Firmware and Template Compatibility”*.

2.1. RAy3 proprietary MIB

MIB can be read via any text editor, but it might be better to browse it (see the trap's variable bindings, OID's unit, descriptions, OID tree, getting values from RAy3 units, receiving and testing traps, etc.) in some special SNMP browser such as MIBBrowser from iReasoning. The following section explains some details about RAy3 MIB for firmware version 2.0.3.0. MIB consists of "revision history" information so you can quickly find out what has been changed.

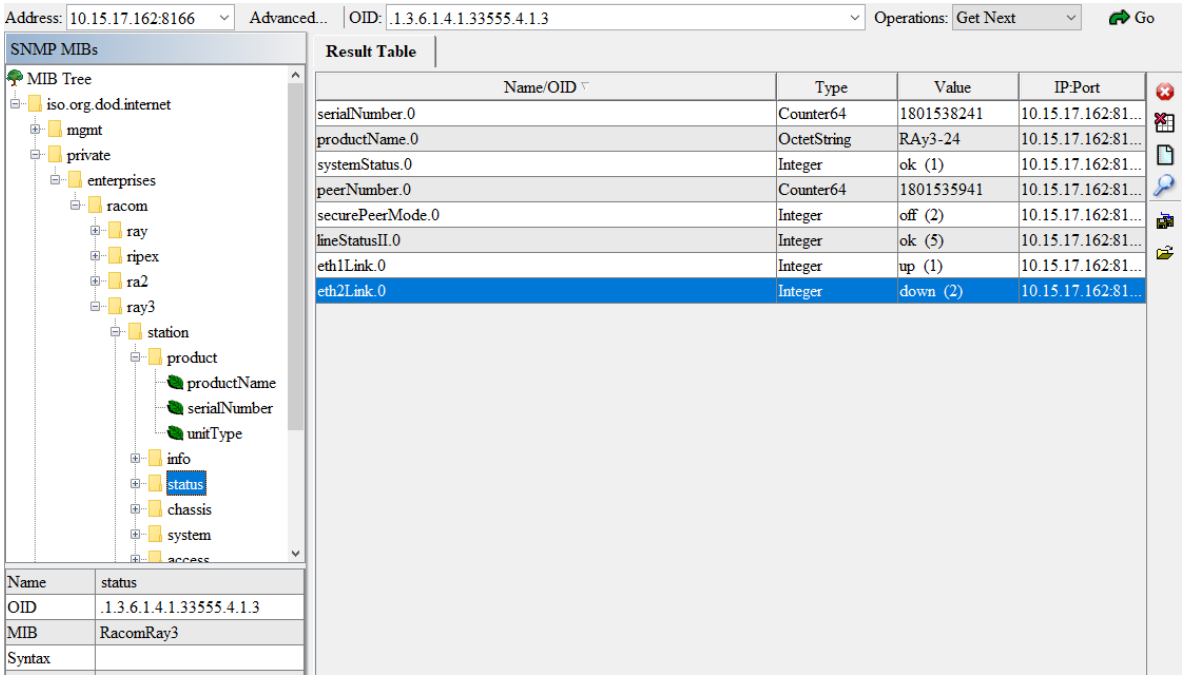

Fig. 2.1: MIB Browser example

Note

CSV file containing all proprietary RAy3 OIDs can be sent upon request, or exported from MIBBrowser software.

The RAy3 MIB module complies with the Severity level 3 validation.

Supported MIBs and its OIDs:

- Values from general MIBs such as SNMPv2-MIB, IF-MIB, RMON, ...
- Proprietary MIB – RacomRay3
  - Alarm states, services states
  - Product information
  - Environmental information (e.g., temperature, voltage, …)
  - Reading configuration parameters
  - Reading operation statistics (reliability, BER, ETH throughput, RSS, …)
  - Sending traps (thresholds are configurable)

RAy3 MIB utilizes custom types declaration so that SNMP reply is numeric, but each number corresponds to a particular meaning. E.g., Alarm states:

- 0 - na
- 1 - up

- 2 - down
- 3 - ack

Make sure your NMS is configured to translate numeric values to their meaning correctly (Value mapping in Zabbix).

Some of the returned values are in decimal notations. E.g., temperature returned as 4800 means 48. If a particular value requires it, it also has a predefined unit such as degrees of Celsius, Volts, decibels, percent, … Again, make sure you utilize your NMS with correct unit.

Current MIB can always be downloaded from *RACOM website*[1] together with Zabbix templates.

2.2. RAy3 SNMP Settings

Basic SNMP parameters are described in RAy3 user manual sections *Service access*[2] and *Alarms*[3]. The following section highlights some important parameters or explains something in more details.

The SNMP agent is switched off by default. You can enable or disable it in the **Link Settings** → **Service access** → **Services** menu.

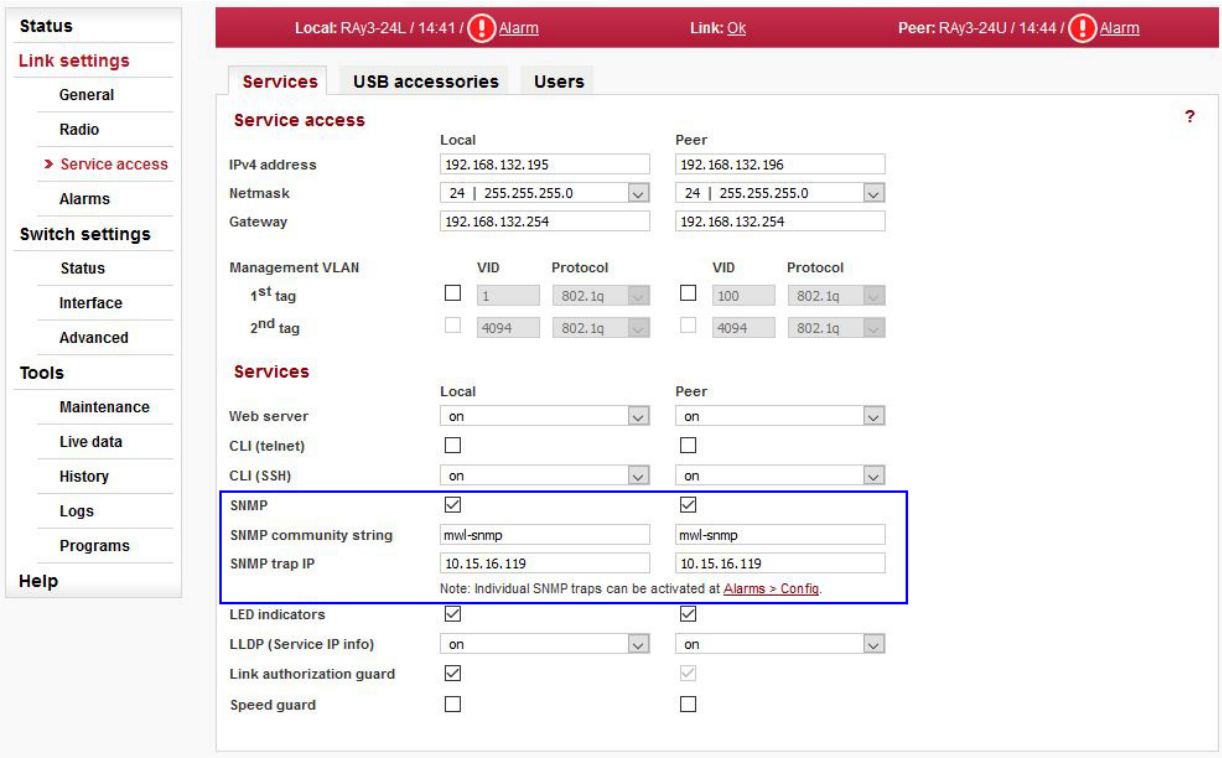

Fig. 2.2: RAy3 SNMP settings

The SNMP community string is "mwl-snmp" by default, but can be changed to another string.

[1] https://www.racom.eu/eng/products/microwave-link.html#dnl_fw3
[2] https://www.racom.eu/eng/products/m/ray3/conf.html#conf-link-serv
[3] https://www.racom.eu/eng/products/m/ray3/conf.html#conf-link-alarm

2.2.1. Alarm Status

All system alarms are listed on this screen. Inactive alarms are colored white with an "OK" text label. Active alarms are colored according to the severity of the alarm with a text message describing the measured value status.

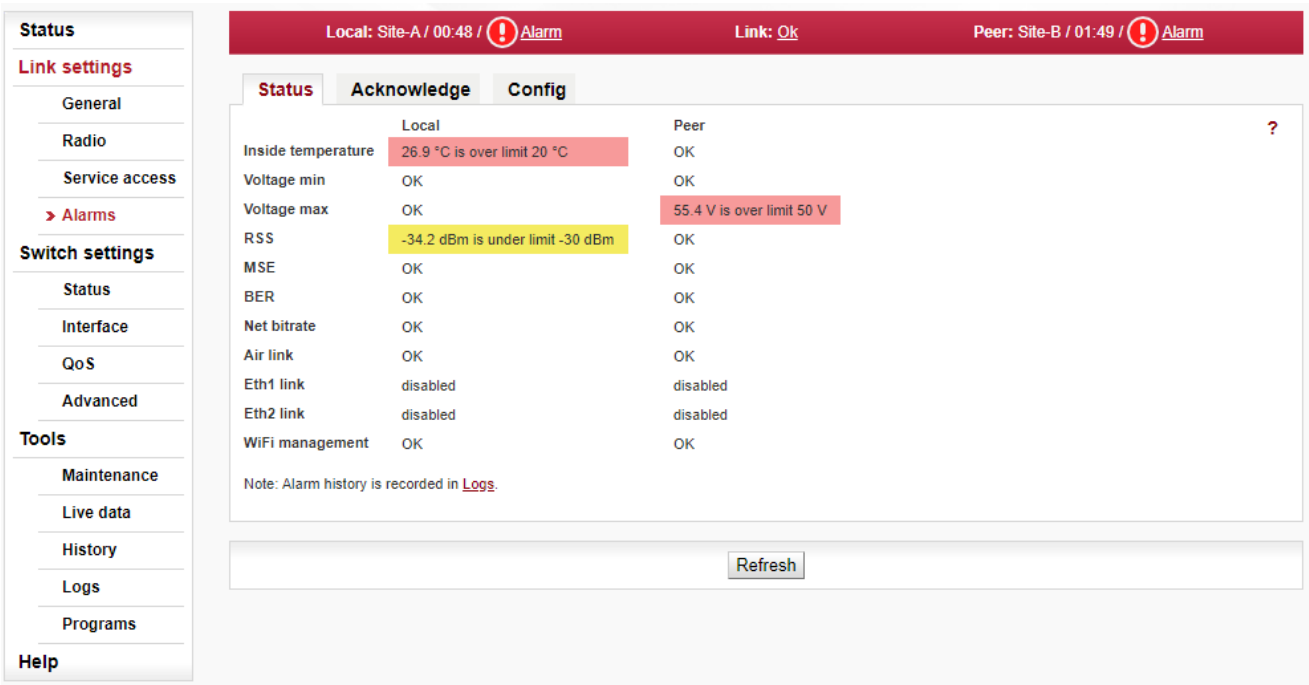

Fig. 2.3: Alarms – Status screen

Alarm severity scale:

- alarm
- warning
- OK (cleared)
- acknowledged (confirmed)

Note

If you click on the "Alarm" text (if any Alarm is UP) on the top of the screen (next to the exclamation mark), you will be redirected to this Alarms – Status screen.

2.2.2. Alarm Acknowledge

Alarm acknowledgement is a way to let the operator confirm the system is in alarm state. Only an active alarm can be acknowledged.

Multiple selection of active alarms (to acknowledge groups of alarms) can be performed using Shift or Ctrl keys.

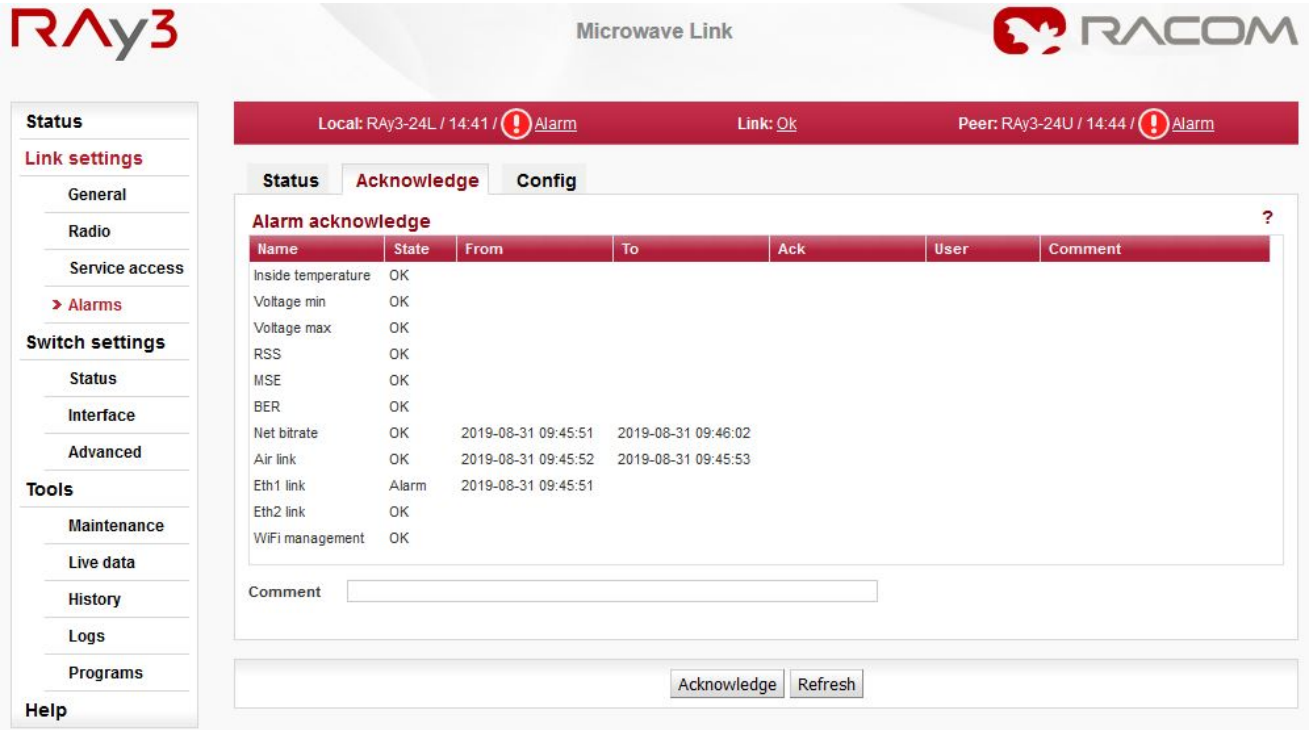

Fig. 2.4: Alarm Acknowledge screen

2.2.3. Alarm Config

The link diagnostic system monitors the operation of the unit. It generates various output of events - system warnings and alarms. The event is always written to the system log and indicated in the status bar and Alarm – Status screen. Some events have adjustable thresholds. Events with no adjustable thresholds may either be Enabled or Disabled. If they are Disabled, the system event is not activated even if the system status is changed. For each event you can choose whether the SNMP trap should be sent if the event occurs.

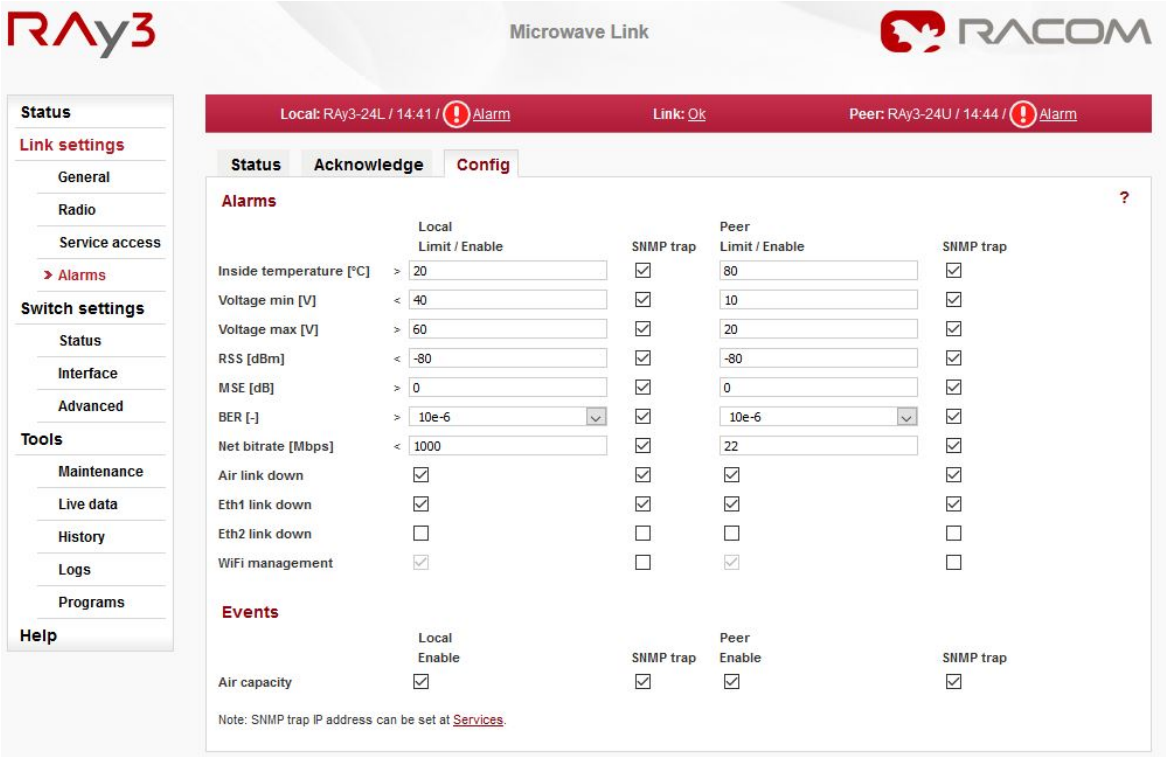

Fig. 2.5: Alarm Config screen

Configurable Alarms / Events:

Inside temperature [°C]	Temperature inside the unit (on the modem board)
Voltage min [V]	Supply voltage Lower threshold
Voltage max [V]	Supply voltage Upper threshold
RSS [dBm]	Received Signal Strength
MSE [dB]	Mean square error
BER [-]	Bit Error Rate is registered at the receiving end; instantaneous value
Net bitrate [Mbps]	The system warning is generated when the radio channel current transfer capacity drops below the set threshold
Air link down	Radio link interruption
Eth1/Eth2 link down	Corresponding user Eth link (Eth1/Eth2) on station interrupted

WiFi management	Warning is generated when WiFi passphrase is not set or WiFi adapter is permanently enabled
Air capacity	Event is generated when Net bitrate of the air channel changes (e.g. because of ACM operation)

Note

For all these traps, there are also special OIDs for the alarm states. The states can be one of "n/a", "up", "down", "ack". See the Application "Alarms" within the RAy3 template.

3. Network Management System – ZABBIX

To access our SNMP values, any Network Management System (NMS) can be used. However, we recommend using the ZABBIX open source monitoring system. It can be downloaded at *http://www.zabbix.com/download.php*[1].

Zabbix features are explained here - *https://www.zabbix.com/features*.

If you have chosen the Zabbix software, please read the following pages where we offer a basic Starting Guide to RAy3 and Zabbix co-working.

Whatever your choice of NMS, these sections may provide general hints and tips anyway.

Note

The following guide was tested with Zabbix LTS version 6.0. If you have older Zabbix releases, check the *RAy3 Archive download section*[2] for previous versions of this application note.

Take the opportunity to remotely access and test a live *Zabbix demo*[3]. See the credentials within the text on the given link.

3.1. Installation and Documentation

Follow the *Zabbix documentation*[4], download packages from *https://www.zabbix.com/download* and install Zabbix 6.0 LTS. We suggest using Debian11 (or newer) OS, MySQL database and Apache web server, because of our good experience and knowledge. If using different solution, our help can be limited.

Note

With previous Zabbix versions, we suggested using CentOS7 and CentOS8, but due to changes in distributing these operating systems, Debian OS seems to be much more appropriate.

Zabbix also offers paid support – see all the possible support tiers at *https://www.zabbix.com/support*.

Once Zabbix 6.0 LTS is installed, multiple additional installation steps are required so that you can monitor and maintain your RAY3 (and any other RACOM products) network(s). Required steps are explained later within this application note.

We also offer Zabbix 6.0 LTS as a virtual, ready-to-be-used, image. It is called “RACOM Zabbix Appliance” or in short “**RZA6**”. Within this .ova image, functionality for all RACOM products is already installed and ready to be used. Contact *RACOM support*[5] to obtain this virtual machine and stay in touch with us for more details.

You can run this RZA6 as a virtual machine, e.g., within your VMware or VirtualBox environment (or any similar one).

[1] http://www.zabbix.com/download
[2] https://www.racom.eu/eng/products/microwave-link.html#dnl_archive
[3] https://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
[4] https://www.zabbix.com/documentation/current/en/manual
[5] mailto:support@racom.eu

3.1.1. Zabbix Installation from packages

Once you finish basic Zabbix 6.0 LTS installation following the Zabbix documentation, you can and should check this part for more details about required steps for RACOM products Zabbix support. The order of explained steps is not so important usually.

Note

If there is any particular Linux command, it is based on Debian11 OS.

We suggest various applications for future usage:

- traceroute
- nmap
- zabbix-sender
- sshpass

All the commands can be installed from the command line with:

```
# apt-get install traceroute nmap zabbix-sender sshpass
```

If you need, you can implement sending **PDF reports** automatically. The installation and functionality can vary from version to version so we do not describe step-by-step procedure here. Use *Zabbix documentation*[6] for more details.

For RACOM products, multiple steps are required. Upload all the MIBs from respective devices (RAy3 in our case) to /usr/share/snmp/mibs/ directory. For a proper functionality, add them to SNMP configuration file /etc/snmp/snmp.conf. E.g.:

```
mibs +/usr/share/snmp/mibs/MG-MIB.txt
mibs +/usr/share/snmp/mibs/RacomRay3.mib
mibs +/usr/share/snmp/mibs/RacomRay2.mib
mibs +/usr/share/snmp/mibs/RACOM-RipEX-1.0.4.0.mib
mibs +/usr/share/snmp/mibs/SNMPv2-TC.txt
mibs +/usr/share/snmp/mibs/RACOM-RA2-MIB
```

3.1.1.1. Templates

Download RAy3 Zabbix 6.0 template from *RACOM website*[7]. Unzip the file and import zbx_export_ray3.yaml into your Zabbix instance in Configuration -> Templates menu via web interface.

Approximately 90 enabled items are included in RAy3 templates. Most items are implemented by RACOM, but there are also items from the well-known MIB files IF-MIB and RMON.

Note

Some items are disabled by default.

The provided templates have predefined update intervals and for how many days each item keeps its history and trend values. All of these parameters define the requirements for the Zabbix server performance and the database size.

[6] https://www.zabbix.com/documentation/current/en/manual/appendix/install/web_service
[7] https://www.racom.eu/eng/products/microwave-link.html#dnl_fw3

Update interval [seconds]	Refresh the item every N seconds.
Keep history [days]	Number of days to keep detailed history in the database. Older data will be removed by the Housekeeper.
Keep trends [days]	Keep aggregated (hourly min, max, avg, count) detailed history for N days in the database. Older data will be removed by the Housekeeper. Note that trends are only stored for numerical items.

Based on these parameters, items are divided into four groups:

1. *Update interval = 1 day (86400 seconds), History = 30 days, Trends = 400 days*
2. *Update interval = 1 hour (3600 seconds), History = 30 days, Trends = 200 days*
3. *Update interval = 5 minutes (300 seconds), History = 60 days, Trends = 400 days*
4. *Update interval = 1 minute (60 seconds), History = 400 days, Trends = 400 days*

Group 4 consists of the most useful values to watch:

- *Input "Ethernet1" data port throughput in bps*
- *Output "Ethernet1" data port throughput in bps*
- *Current net bitrate in bps*
- *Current RF Power in dBm*
- *Receive RSS indicator in dBm*
- *Receive MSE indicator in dB*

From our experience, all these values are important to watch and to have them updated each 60 seconds. It is also useful to be able to display these values in detail even if they are one-year-old.

If you need to have even more accurate values, you can decrease the update interval. The smallest useful value for the throughput items is 10 seconds. Reading RSS or SNR can be done every second, because its value is always the current one.

Important

We calculated that with the predefined RAy3 template (enabled values only), you approximately need about 0.75 GB of data for one RAy3 link (two units). Have this in mind when considering the database size. It can be increased a lot in case of many traps being sent from the RAy3 units

3.1.1.2. Hints & Tips

The link reliability, link uptime, downtime or BER can be read because of our own OIDs. These values are updated every 5 minutes by default.

Watching the number of CRC errors can detect faulty cables and the number of dropped packets can warn you about high Ethernet traffic (bursts) so RAy3 drops some of them.

By default, the templates automatically populate the Inventory of individual hosts (serial number, unit type, MAC address, ...). If you enable Inventory of your RAy3 hosts (in the host configuration menu), you'll be able to see those values within the unit's Inventory without any additional steps or without configuring them manually.

Note

You can define the default Inventory mode in the Administration - Others menu.

It is also recommended to utilize SNMP BULK requests which significantly reduce amount of data being exchanged between RAy3 and NMS, because it is possible to query multiple OIDs within a single packet, as well as reply to such multiple requests within just one SNMP reply packet.

Note

There are many Network Management Systems available on the market. Whichever you choose, keep in mind the described limitations. E.g., never use NMS, which can download only the entire remote device MIB and not single OIDs

SNMP Traps

Other important steps are for SNMP traps. Once the trap is received, it is handled by our script and for its proper functionality, the OID cannot be translated to text. Edit the snmptrapd:

```
# systemctl edit snmptrapd.service --force -full
```

Change the ExecStart variable:

```
ExecStart=/usr/sbin/snmptrapd -Lsd -f -p /run/snmptrapd.pid -On
```

The whole file should be:

```
# cat /etc/systemd/system/snmptrapd.service
[Unit]
Description=Simple Network Management Protocol (SNMP) Trap Daemon.
After=network.target
ConditionPathExists=/etc/snmp/snmptrapd.conf
[Service]
Type=simple
ExecStart=/usr/sbin/snmptrapd -Lsd -f -p /run/snmptrapd.pid -On
ExecReload=/bin/kill -HUP $MAINPID
[Install]
```

For a proper functionality of RAy3 SNMPv2c traps, multiple additional steps are required. Also keep in mind that you could configure RAy3 traps different way (e.g., via SNMPTT) – here is just one approach described.

If not yet installed, install ‘snmptrapd’ daemon and enable it to be run automatically.

Within the downloaded .zip templates from *RACOM website*[8], snmptrap.sh script is included. Copy the script into /usr/lib/zabbix/externalscripts/ directory and change the file privileges and make it executable.

```
# chown zabbix:zabbix /usr/lib/zabbix/externalscripts/snmptrap.sh
# chmod +x /usr/lib/zabbix/externalscripts/snmptrap.sh
```

Note

Your ‘zabbix’ user should be enabled. It should have a HOME directory set to /var/lib/zabbix/ and this user should be able to run the shell. E.g., this command can be helpful:

```
# usermod --shell /bin/bash zabbix
```

[8] https://www.racom.eu/eng/products/microwave-link.html#dnl_fw3

Check your ‘zabbix_sender’ path and if required, change it within the provided snmptrap.sh script accordingly.

```
# which zabbix_sender
/usr/bin/zabbix_sender
```

So, the script has this line inside:

```
ZABBIX_SENDER="/usr/bin/zabbix_sender";
```

The script parses the output of each received SNMP trap, selects the appropriate host and declares an associative array containing trap descriptions. Eventually, it sends the whole message to your Zabbix server.

The default path to a LOG file from snmptrap.sh script is /var/log/snmptrap/snmptrap.log. Create the directory and a file manually, if not yet created.

Another required step from the command line is to edit /etc/zabbix/zabbix_server.conf file. Find the appropriate lines and edit them to:

```
SNMPTrapperFile=/var/log/snmptrap/snmptrap.log
StartSNMPTrapper=1
```

Zabbix, and especially your snmptrapd must know how to authenticate against the received traps/informs. If it is SNMPv2, it is quite easy – you just need to allow particular community strings and also explicitly say that our snmptrap.sh must be executed upon a received trap/inform. Do this via /etc/snmp/snmptrapd.conf file. Example of such file:

```
authCommunity log,execute public
authCommunity log,execute mwl-snmp
authCommunity log,execute racom-snmp
traphandle default /bin/bash /usr/lib/zabbix/externalscripts/snmptrap.sh
```

Note

There is third trap state on the RAy3 WEB interface - "acknowledged". This is not recognized automatically within the Zabbix frontend, but you can acknowledge the trap in Zabbix separately from the Dashboard menu.

3.1.1.3. RAy3 Firmware and Template Compatibility

Since RAy3 FW 1.0.14.0, the SNMP non-table items OIDs are defined in accordance with the RFC (ending '.0') - to improve SolarWinds compatibility. Keep this in mind when upgrading RAy3 firmware. Firmwares < 1.0.14.0. are able to reply to SNMP queries with OIDs ending with .0, but the reply does not contain .0 in its OID. This works fine (for example) with Zabbix NMS, but (for example) SolarWinds does not accept such replies.

Since RAy3 FW 1.0.16.0, the SNMP product OID of RAy3 changed from '1' to '4'. The old template will NOT work with new RAy3 firmware. See the procedure below.

Suggested way of updating the RAy3 template is very straight-forward. Download the latest template from our *RAy3 Firmware download site*[9]. The name of the template is "RAy3 Template". There are two possible procedures and situations.

[9] https://www.racom.eu/eng/products/microwave-link-detail#dnl_fw3

1. All RAy3 units in your NMS already have firmware >= 1.0.16.0. Rename your current RAy3 template to "RAy3 Template" and Import the new one with the same name. This will replace the older template.

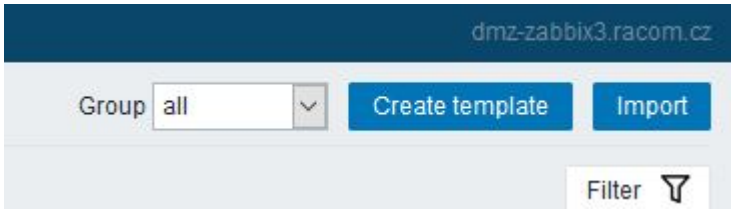

Fig. 3.1: Importing RAy3 template

2. You operate both RAy3 links with newer and older firmware. In such a case, you need two different templates. Make sure that your current template in Zabbix has a different name than "RAy3 Template", e.g. "RAy3 old firmware Template". Then, import the new template.

   Mark hosts with new firmware (>= 1.0.16.0) and use "Mass update" button.

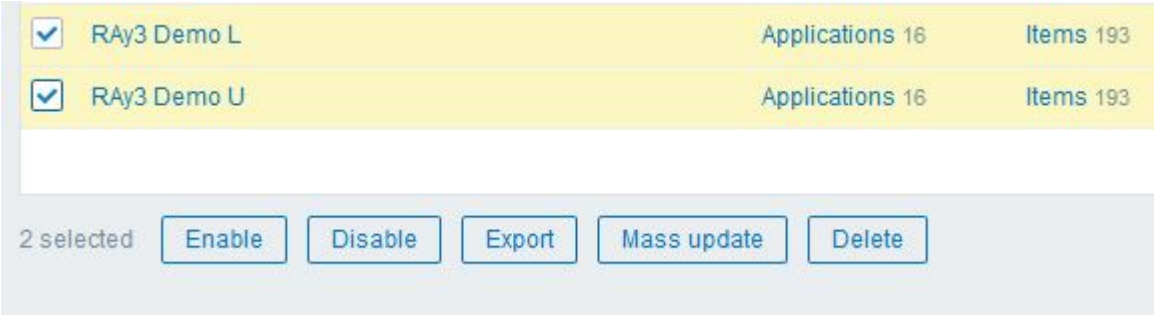

Fig. 3.2: Mass update of RAy3 units

Select the "Templates" submenu and select a new template. Check the "replace" box and apply the changes.

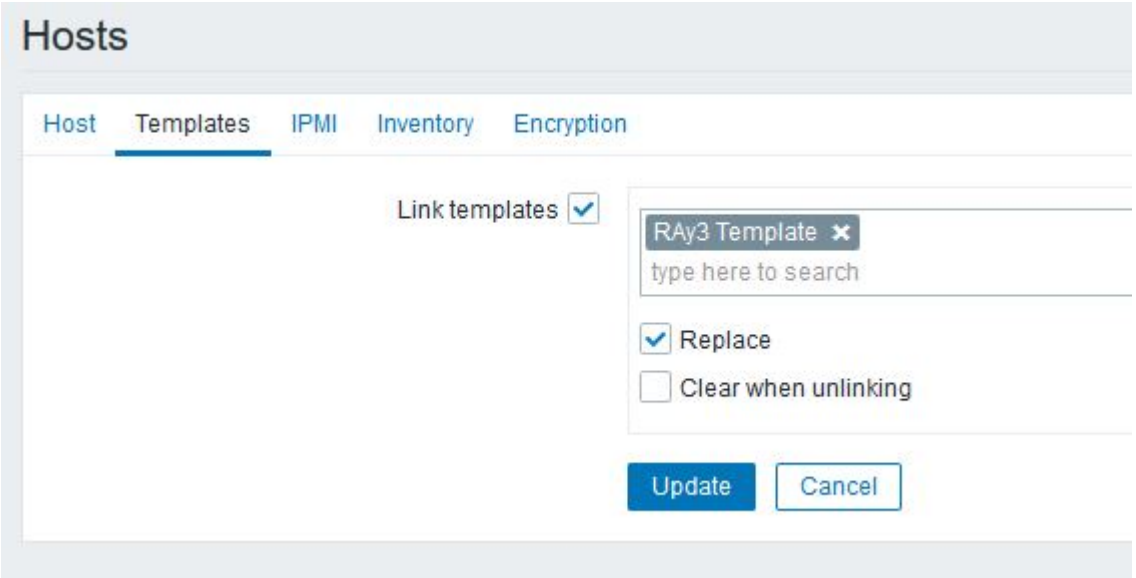

Fig. 3.3: Replacing RAy3 template for selected units

In both situations, the history values should still be available and new values will be queried successfully.

If you have any issues updating RAy3 firmware and/or Zabbix templates, contact RACOM technical support group via *support@racom.eu*[10].

Note

If you use template utilizing Item's KEYs of non-table items with '.0' at the end, you need to check the "Clear when unlinking" box once replacing hosts' template, because you would double the Items of each host. Unfortunately, you lose your historical data. You could manually edit all Item keys with trailing .0 manually in Zabbix GUI.

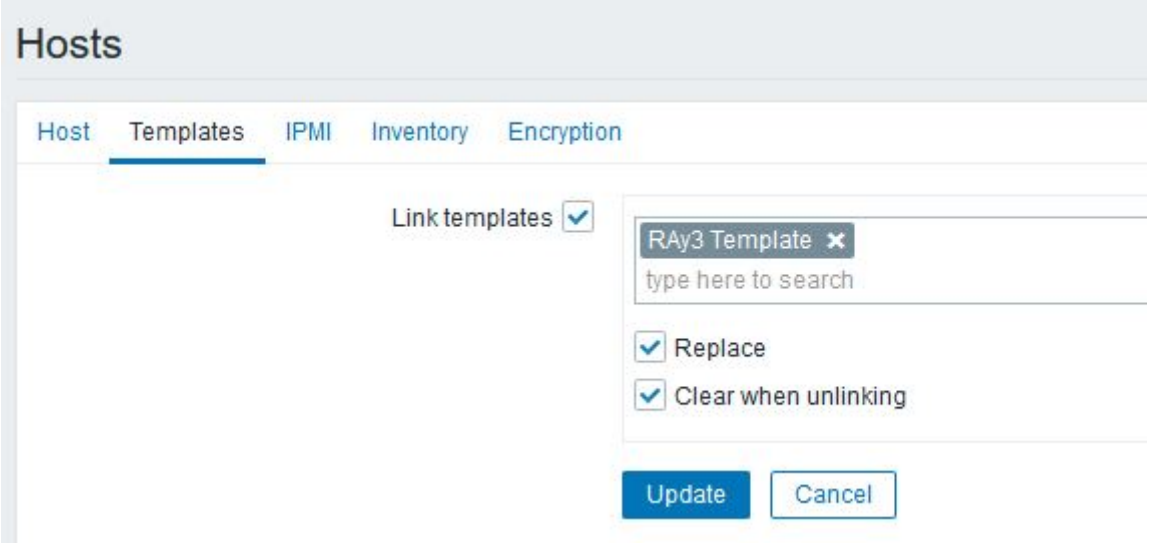

Fig. 3.4: Replacing RAy3 template for selected units with Clearing the hosts' items

[10] mailto:support@racom.eu

3.1.1.4. RAy3 images

Hosts can be displayed in graphs. For such a purpose, we created multiple RAy3 images of different size and with different borders (e.g., red border in case the unit is in a problem state). These images are included in the mentioned .zip file with RAy3 template. Import them one by one in Administration – General – Images menu, or via directly via MySQL.

Fig. 3.5: RAy3 images in Zabbix

3.1.2. RACOM Zabbix Appliance – RZA6

RZA6 is widely preconfigured.

You will still need to go through SNMP traps section above so that you can use your particular community strings. Otherwise, all should be prepared.

3.2. How to use RAy3 template

Now, Zabbix should be ready for monitoring RAy3 network. This chapter gives you a brief procedure to get started, but feel free to utilize different approach.

First, we suggest to create a Host – probably RAy3 unit directly accessible via Ethernet from Zabbix. Go to the Configuration – Hosts menu and click on the “Create host” button on top right corner.

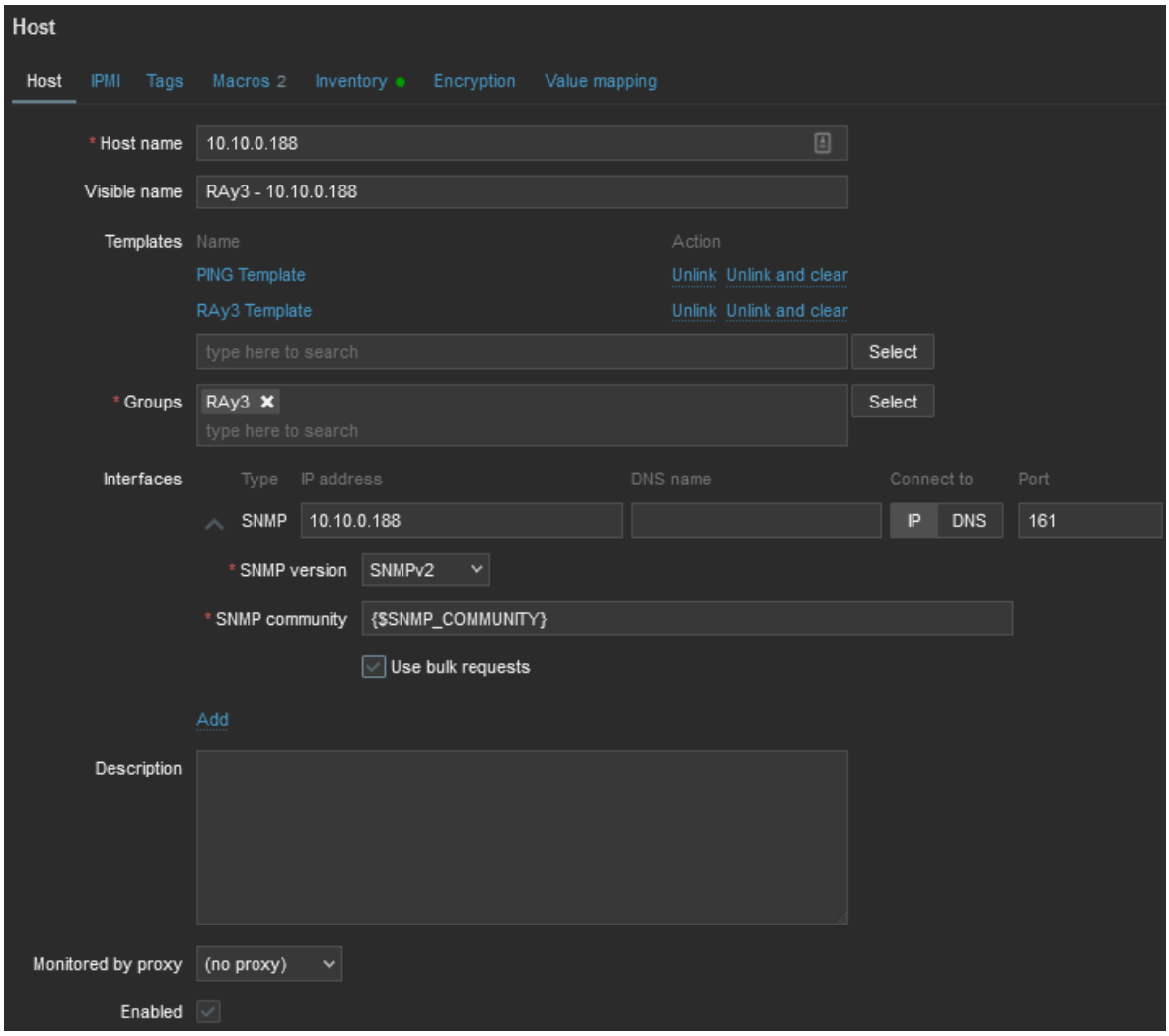

Fig. 3.6: New RAy3 host

Always put the IP address of the unit to the “Host name” field so the SNMP traps work (the script works with IP addresses). The “Visible name” can be set to any required value.

Select the “RAy3 Template” so that the unit is preconfigured with all RAy3 supported Items. Create a new, or add it to an existing one, RAy3 group. You can name it as required – e.g., based on RAy3 network location or particular customer company name. Set the SNMP Interface:

- IP address
- Port (usually UDP/161)
- SNMP version 2
  - Set the community string to MACRO {$SNMP_COMMUNITY}
  - Now, check and change MACROs in “Macros” tab

- HOST_SSHKEY and HOST_SSHPORT macros are used for RAy3 scripts

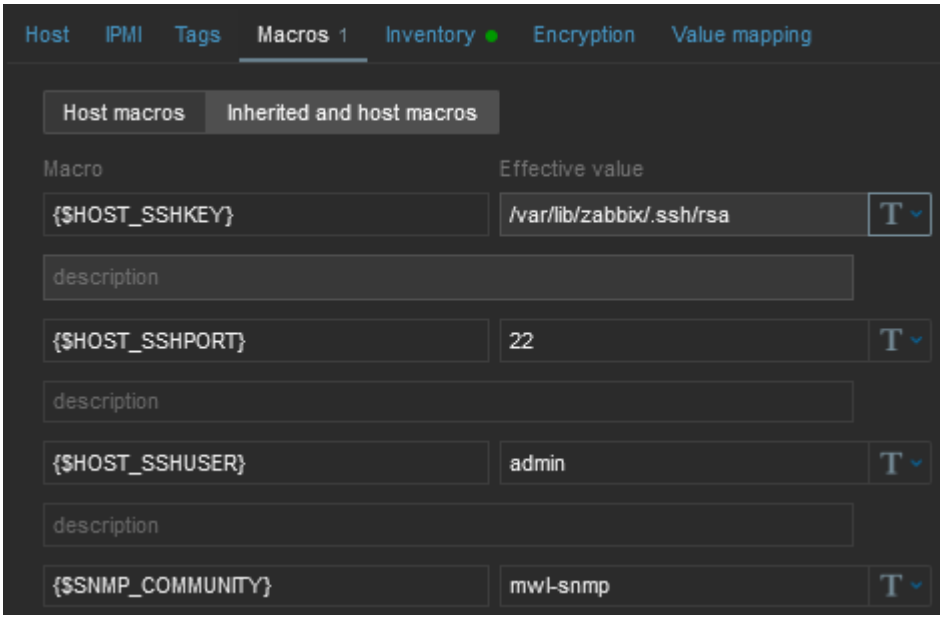

Fig. 3.7: RAy3 Host MACROs

You can either change the values in Template so it is the same in all your RAy3 units, or you can set it per Host.

- Check the “Use bulk requests” option because it optimizes data traffic being sent

Verify the Inventory tab – it should be set to “Automatic” so some of the values are automatically filled by SNMP queries. Click on the “Add” button – a new Host is created.

But the host is not monitored yet, because all the Items and Discoveries are disabled by default.

Only monitor the values which you really need and with reasonable update times.

Go to the Host’s Items and enable required Items, you can also edit the SNMP query intervals and other parameters.

If you want Traps to be working, you need to enable particular traps with App tag equal to TRAPS and enable Triggers accordingly (i.e., if you enable “TX Lost value out of range” Item, you also need to enable a Trigger for this Item).

You can check the data in the Monitoring – Latest data menu. Filter the values are required. All numeric values can be depicted in graphs. String values have their own history.

Other units can be easily added by a “Clone” button from this Host configuration. Just change appropriate IP addresses and ports. Divide them into groups (e.g., geographically). Choose wisely the monitored values and enabled discovery rules.

3.3. Zabbix Usage Hints and Tips

This application note cannot target all possible information about Zabbix and its usage. Check Zabbix documentation and Google forums for general help and guides. The following section provides several hints and tips for quicker and easier RAy3 network monitoring. Information provided might not be fully explained or might be different in any other Zabbix version other than 6.0 LTS.

3.3.1. Maps

Having a map is handy way for a network overview. On a single map, or multiple maps (even hierarchical) you may see all RAy3 units (and any other devices) and their status overview. There can be a plain/empty background, or e.g., some picture of a map (static).

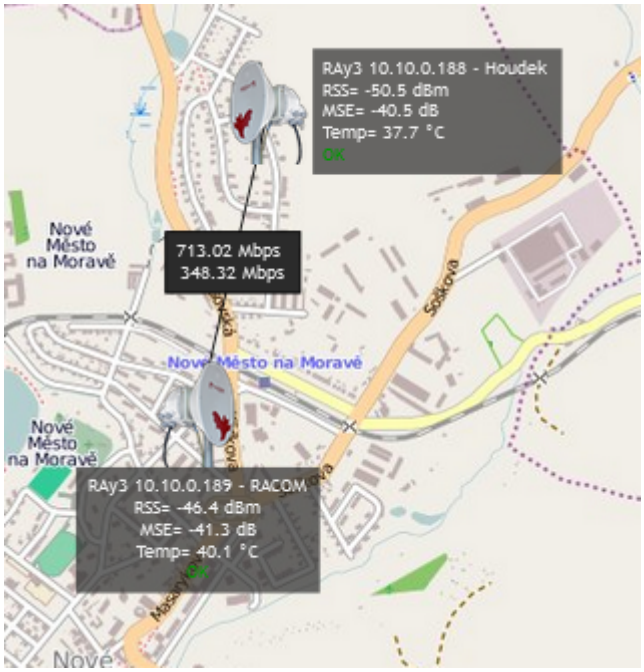

Fig. 3.8: Zabbix simple RAy3 map

On the map above, we can see two RAy3 units with a displayed name and current RSS, MSE and temperature. If the unit has no Problem, an “OK” message is displayed and the Host borders are in green color. We also depict a radio link between these units and its throughput values.

Host details:

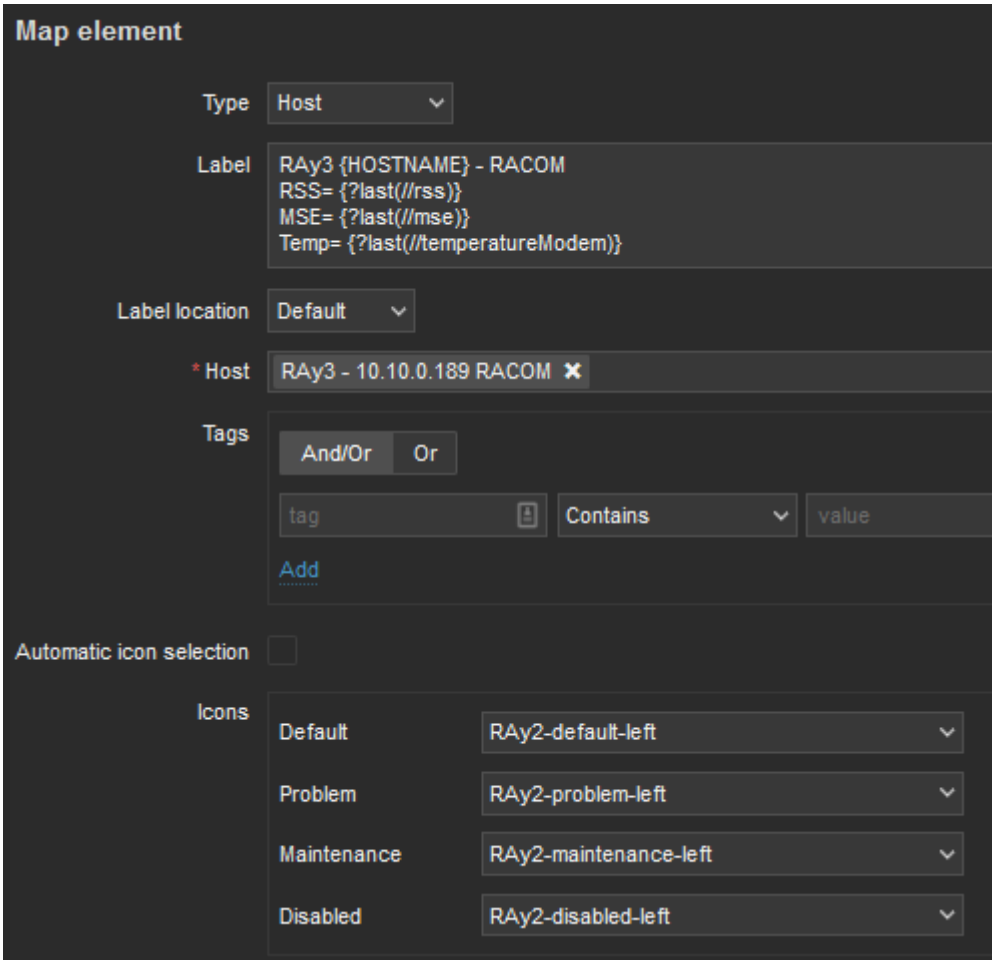

Fig. 3.9: Host details in maps

Label is set as follows:

```
RAy3 {HOSTNAME} - RACOM
RSS= {?last(//rss)}
MSE= {?last(//mse)}
Temp= {?last(//temperatureModem)}
```

Select a particular host and you can change icons for various situations.

Example of the link Label:

```
{?last(/10.10.0.188/netBitrate)}
{?last(/10.10.0.189/netBitrate)}
```

Even the link color can change in time – for example lower throughput than 20 Mbps. You can create your own Trigger monitoring throughput values.

3.3.2. Geographical Maps

New feature from 6.0 LTS Zabbix version are Geographical maps. If you add GPS coordinates to your RAy3 hosts, you can display them on geographical maps.

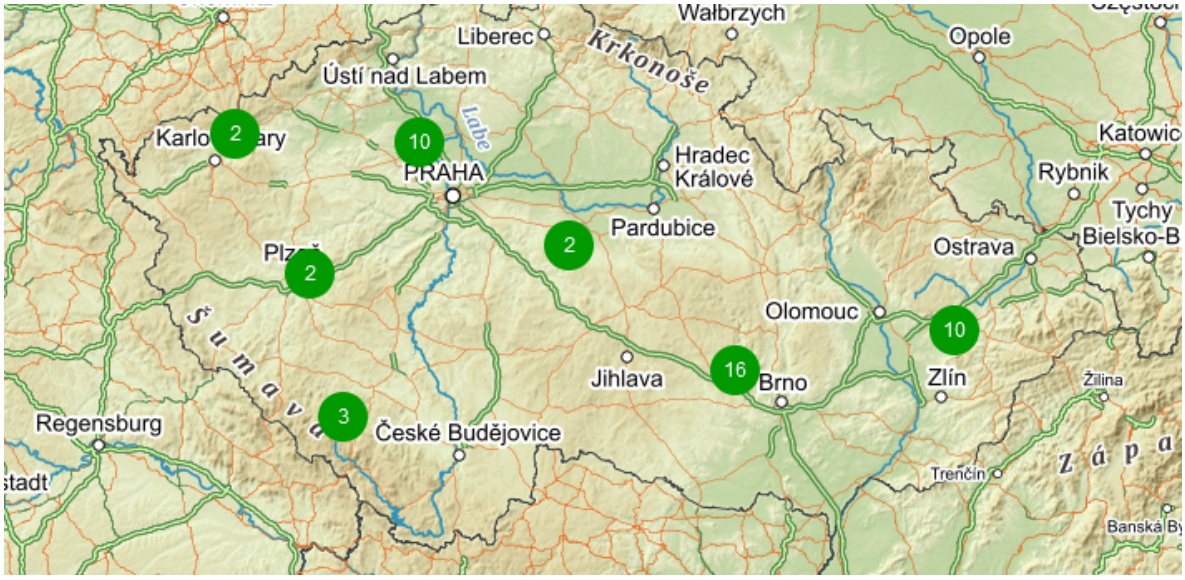

Fig. 3.10: Geographical map

First, you need to add GPS coordinates in the Host Inventory.

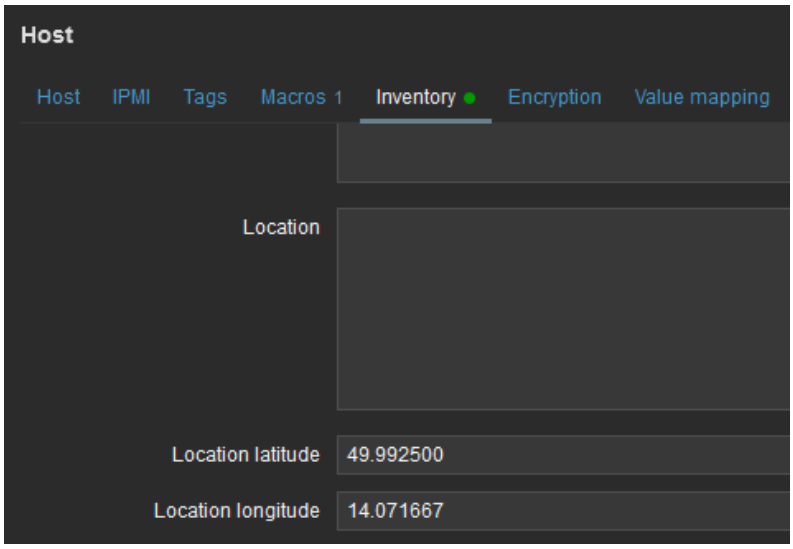

Fig. 3.11: Host GPS coordinates

Another step is to enable and configure Geographical graphs. Go to Administration – General – Geographical maps menu. Set the required map source/provider. There is a list of default supported map sources, but you can also add “other”. Here is the example for Czech mapy.cz map source.

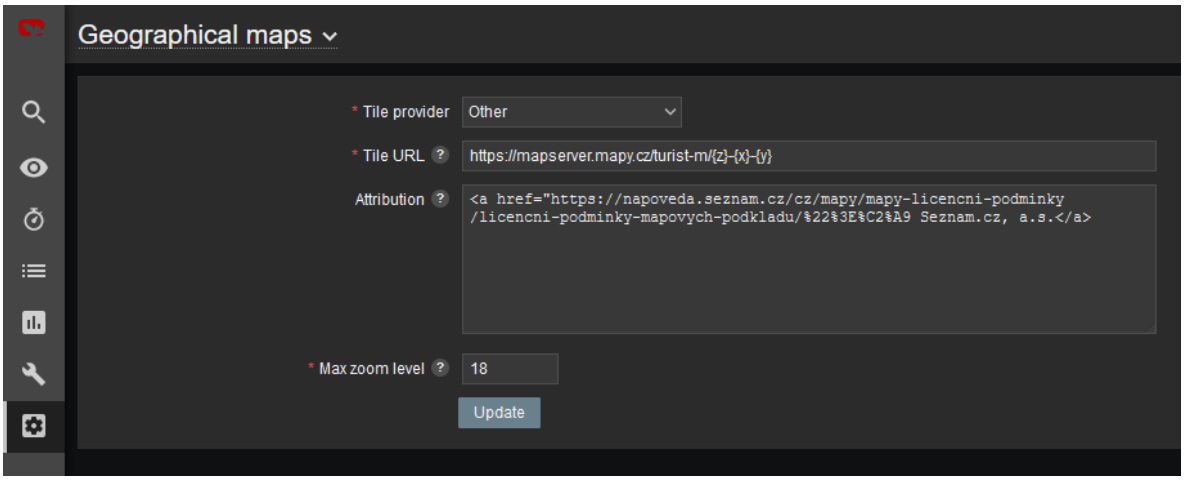

Fig. 3.12: Zabbix Geographical maps

Tile URL: *https://mapserver.mapy.cz/turist-m/{z}-{x}-{y}*

Attribution: <a href="https://napoveda.seznam.cz/cz/mapy/mapy-licencni-podminky/licencni-podminky-mapovych-podkladu/%22%3E%C2%A9 Seznam.cz, a.s.

Max zoom level: 18

The last step is to add Geographical map to your Dashboard. Edit the dashboard and add “Geomap” widget. Select its name, host group(s) and host(s). Save the changes.

Within the map, you can use a “zoom” feature. You can either see multiple hosts within one icon, or one icon is one host (it is zoomed enough). You can then be forwarded into particular menus etc. Color of the Icons can be changed upon Host status. Read more in Zabbix documentation.

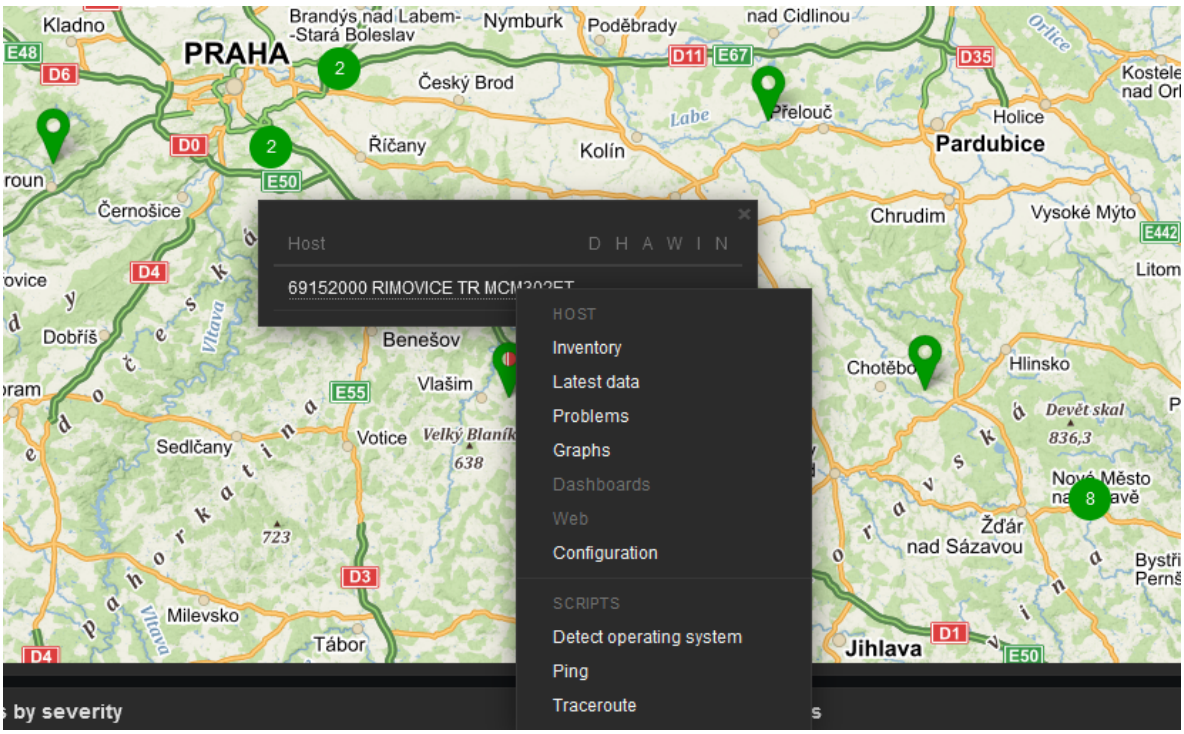

Fig. 3.13: Geographical map host details

3.3.3. Links from Zabbix to RAy3 GUI

Units' GUI can be accessed from Zabbix web interface from multiple menus.

A typical one is from simple maps. Configure the URL within the Host on the map and once you click on the Host in this map afterwards, you can be forwarded there. Keep in mind it is not possible from geographical maps.

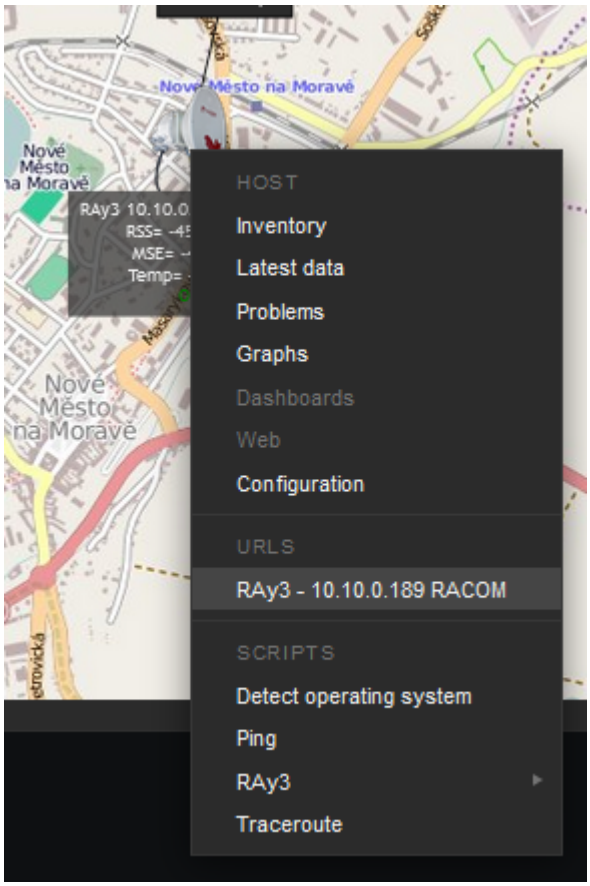

Fig. 3.14: URL link – maps

Another way is a link from Triggers so that if a Problem occurs, you can quickly go to the required web interface.

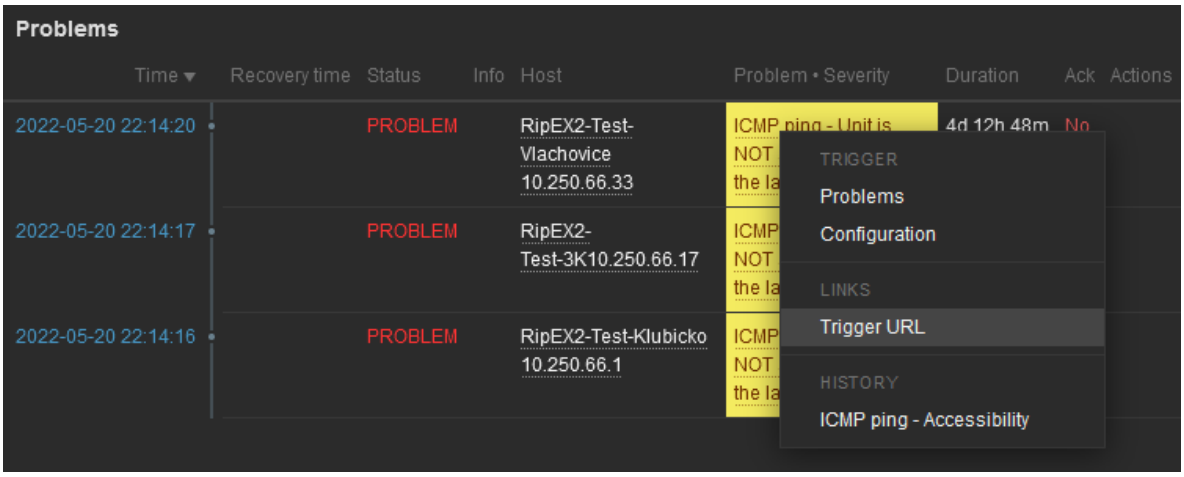

Fig. 3.15: URL link – triggers

The third option is to use Inventory for configuring URL. For every Host, you can enable the Inventory (serial number, OS, host type, ...). Within many Inventory options, the URL can be defined.

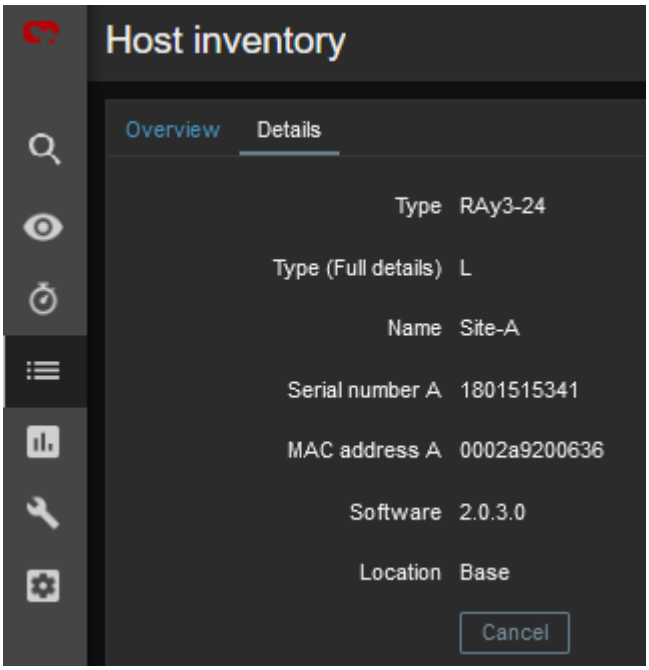

Fig. 3.16: URL link – Inventory

3.3.4. Scheduled Reports

Another useful feature is generating scheduled reports. You need to configure Scheduled reports in general. Once you have it, go to the Report – Scheduled reports menu and create a new one. Basically, Zabbix can send multiple users in regular intervals its Dashboard(s) as PDF.

More information e.g., see *Zabbix website*[11].

[11] https://www.zabbix.com/documentation/current/en/manual/config/reports#configuration

3.3.5. Actions, Email notifications

In case of any issue within your network, e.g., drop in the signal quality, or the unit being unreachable, Zabbix can automatically send an e-mail to predefined e-mail addresses. See the following example for your reference, but customize it to suit your needs.

The e-mail can be set in the Administration – Media Types menu. Edit the E-mail type corresponding to your server settings. In our example, we use our own SMTP server reachable from Zabbix server. No special security or password is required. You should be able to use any SMTP server.

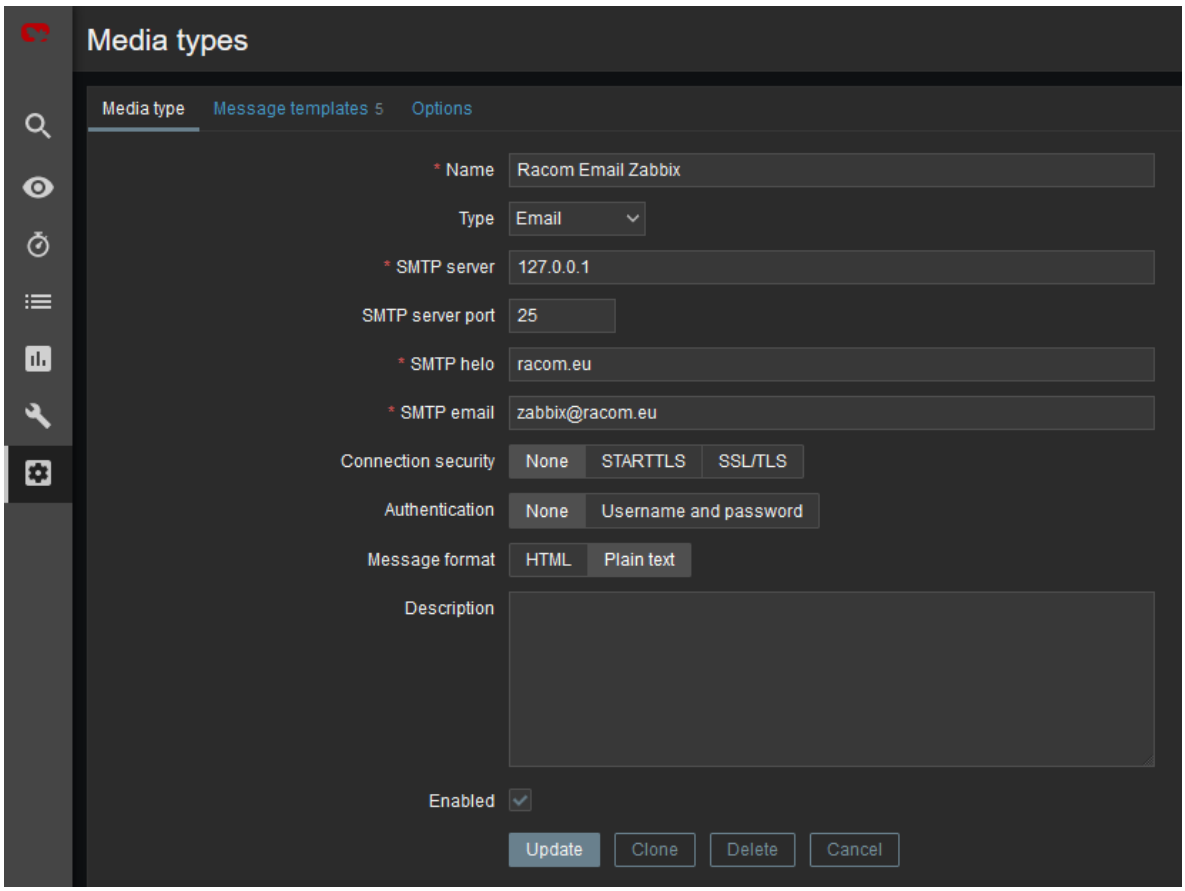

Fig. 3.17: Zabbix Media type – Email

The e-mails are sent to the users' e-mail addresses. Go to the Administration – Users menu and configure the required e-mail addresses within the user's details (Media).

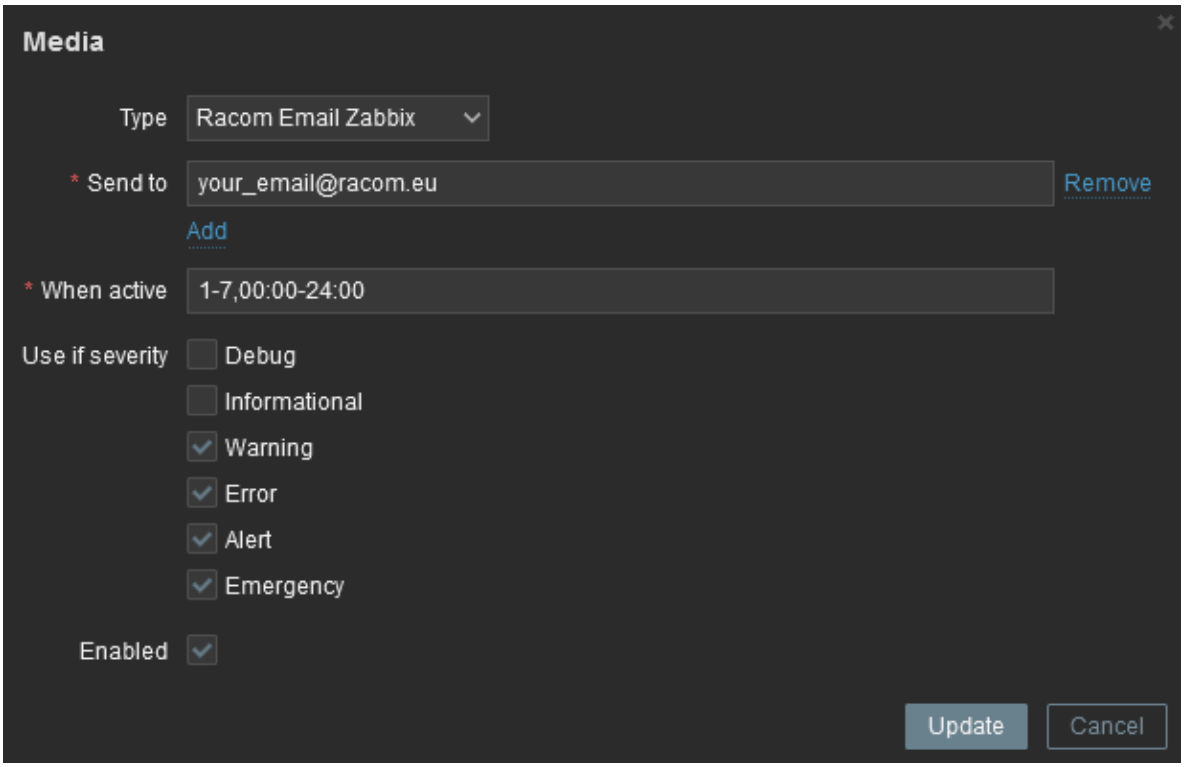

Fig. 3.18: User's e-mail

You define the time when the e-mail will be sent (e.g., do not send it over the night) and the severity of the issue (e.g., send me the e-mail just in case of a critical issue).

The last step is to configure the action – configure which issue causes the e-mail to be sent. Go to the Configuration – Actions – Trigger actions menu and create a new Action. Set a Name of the Action and its Conditions – trigger severities and host group are used within the screenshot below.

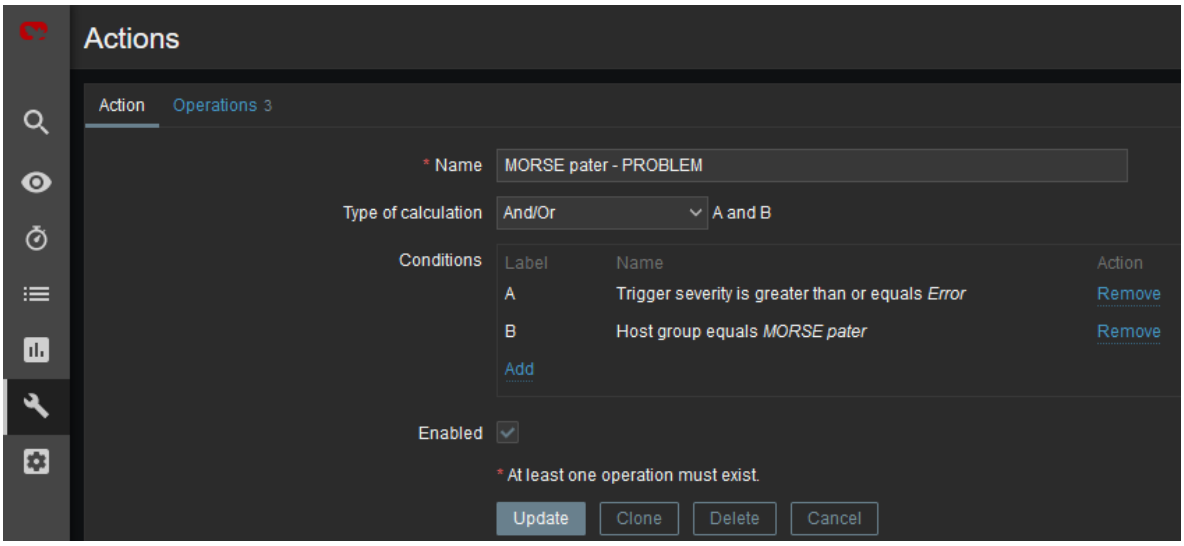

Fig. 3.19: Action and its conditions

Within the Operations tab, define one or multiple operations. In the example, once the Problem occurs, Zabbix sends an email. It sends such email every other day until the problem is fixed.

We also send a Recovery email to all involved recipients.

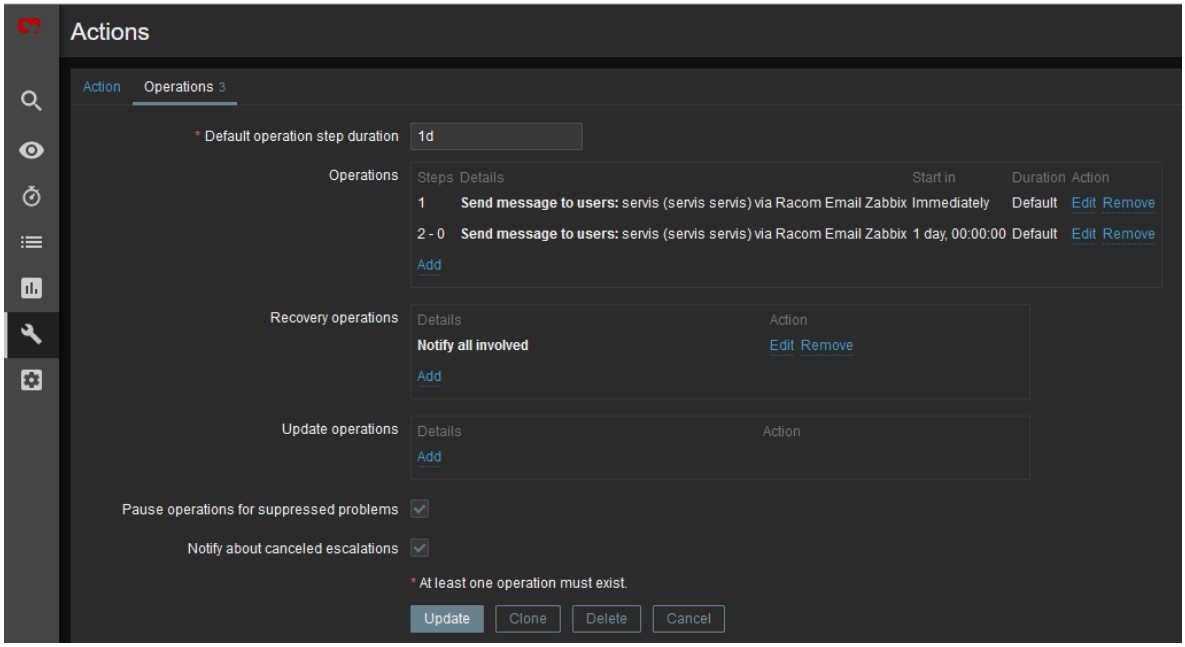

Fig. 3.20: Action Operations

Usually, you will use the MACROs for the e-mail body/subject. In this example, the Subject of the email will consist of the host's Name, Trigger status (Problem or OK) and Event Name. Within the body of the message, there can be additional information such as the Trigger Severity, URL and the Issue details.

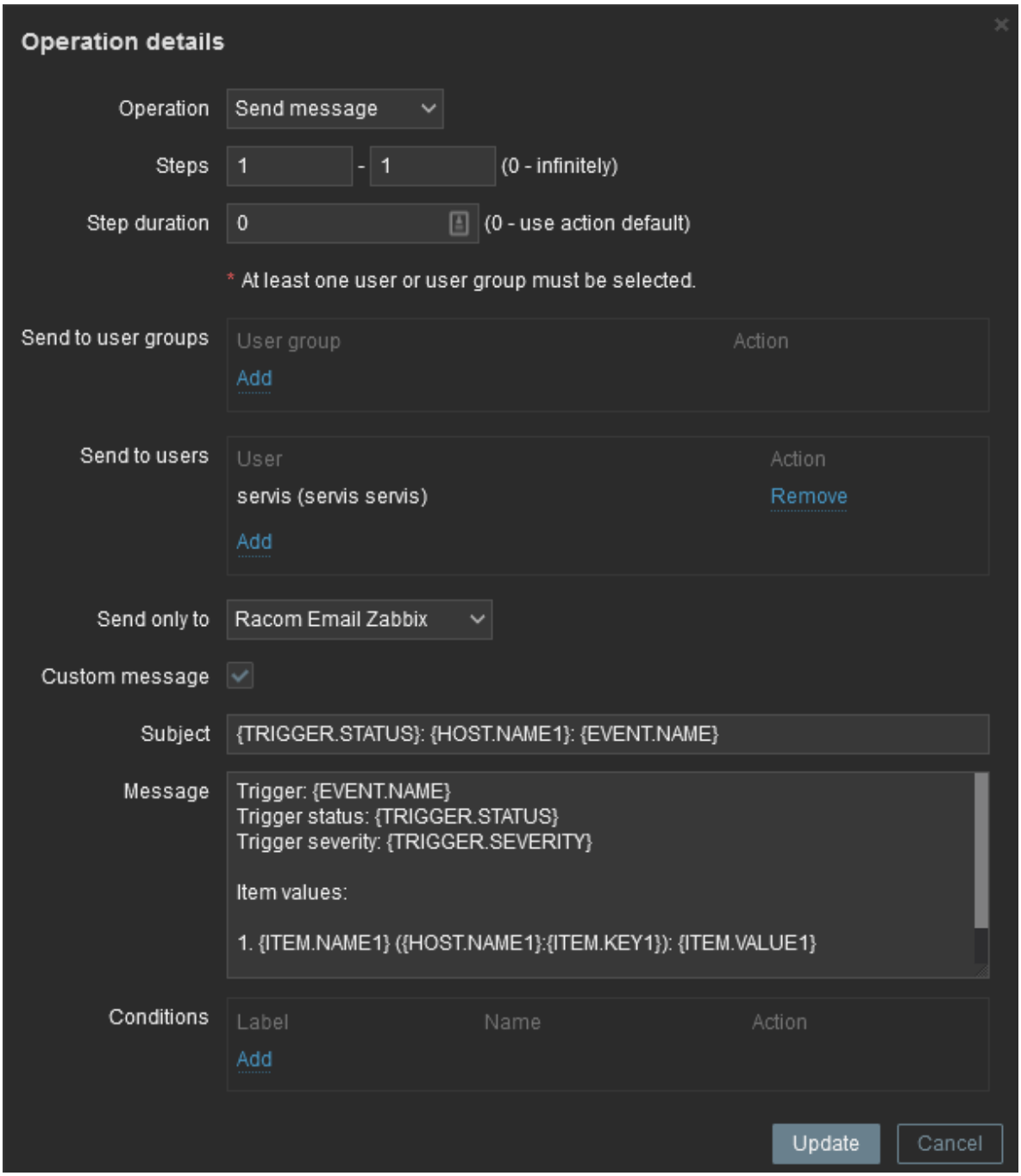

Fig. 3.21: Action Operations details

3.3.6. RAy3 Scripts in Zabbix

By default, there are no ready-to-be-used actions in Zabbix such as configuration backup or firmware upgrade. The Zabbix NMS is a general system which requires special features to be implemented by RACOM or by the user himself.

We provide the user with a guide how to use and define these special features and within the RAy3 template, we already prepared several examples:

- Configuration backup
- Displaying the current Firmware version
- Firmware upgrade

Note

If you have troubles running those scripts or making your own, contact RACOM technical support on *support@racom.eu*[12].

The whole implementation can be quite time consuming, but once you successfully run the first script, the others are very similar and its implementation is straightforward.

Within the Template, there are three scripts. As you realize, having the configuration backup files can be crucial if replacing the unit. There is nothing easier than just uploading the configuration file into a brand new RAy3 unit.

Before creating and running the first scripts, you need to prepare the Zabbix server (and the Linux operating system). In this example, we configure the Debian11 OS with Zabbix 6.0 LTS installed via packaging system.

The following steps can be done in different order, but following this order is absolutely fine.

By default, the zabbix_server configuration file is located in the /etc/zabbix/zabbix_server.conf file. Find the line with "SSHKeyLocation” parameter and define it with this value:

```
SSHKeyLocation=/var/lib/zabbix/.ssh
```

This is the location of the private SSH key which will be used to access the RAy3 units. Restart the Zabbix server afterwards.

```
systemctl restart zabbix-server
```

The scripts must be uploaded manually to a correct directory. The default directory is /usr/lib/zabbix/externalscripts/. Copy the script files from the ZIP Template file to this directory. The target state should look similar to this output:

```
ls -l /usr/lib/zabbix/externalscripts/
-rwxr-xr-x 1 zabbix zabbix 649 Mar 9 16:58 ray_cli_cnf_backup_get.sh
-rwxr-xr-x 1 zabbix zabbix 137 Mar 9 13:59 ray_cli_fw_show.sh
-rwxr-xr-x 1 zabbix zabbix 3202 Mar 15 08:40 ray_cli_fw_upgrade.sh
-rw-r--r-- 1 zabbix zabbix   9612 May 25 09:31 script-log.txt
-rwxr-xr-x 1 zabbix zabbix  39262 May 26 08:44 snmptrap.sh
```

[12] mailto:support@racom.eu

There are three executable scripts via the Zabbix web interface (starting with “ray_”). The LOG output of those scripts is in script-log.txt file. There is also the snmptrap.sh file which you should have there for the SNMP TRAP functionality.

Make sure that the files have the zabbix user/group and are executable.

```
# chown zabbix:zabbix /usr/lib/zabbix/externalscripts/*
# chmod +x /usr/lib/zabbix/externalscripts/*.sh
```

The Zabbix user cannot login to the bash by default. We need to enable it as follows (if not already done in RZA6).

```
usermod --shell /bin/bash zabbix
```

If not already created, create the HOME directory for the Zabbix user.

```
usermod -m -d /var/lib/zabbix zabbix
chown zabbix:zabbix /var/lib/zabbix
chmod 755 /var/lib/zabbix
```

Create the directories for the saved configuration and firmware files and change the access rights.

```
mkdir /var/lib/zabbix/configuration-backup
mkdir /var/lib/zabbix/configuration-backup/ray
mkdir /var/lib/zabbix/firmware
mkdir /var/lib/zabbix/firmware/ray3
chown -R zabbix:zabbix /var/lib/zabbix/
```

The directory for the SSH key should now be located in /var/lib/zabbix/.ssh directory. Change the current directory to this one and login as zabbix.

```
su zabbix
```

A new prompt appears. We need to upload the SSH keys into every unit we want to control. You can either have you own RSA/DSA key or you can create a new one following this example. Run

```
ssh-keygen -t rsa
```

Follow the guide of the ssh-keygen application and leave the passphrase empty. To copy our RSA key into RAy3 units, copy the public part of the key and run the following command:

```
ssh admin@192.168.132.200
```

Just replace 192.168.132.200 with the correct RAy3 IP address. The prompt will ask for the admin password, fill it in and click Enter. Now, you should be logged in RAy3 CLI. Run the following command:

```
vi .ssh/authorized_keys
```

Note

Browse the Internet for how to use ‘vi’ text editor if you are in trouble.

Insert (paste) your public part of the key to a new line. Save the changes and close the file. Logout and check, if you can access the unit without a password.

```
ssh -i rsa admin@192.168.132.200
```

We completed all Linux tasks, but we still need to edit Zabbix web interface.

Scripts must be manually created in the Zabbix Administration - Scripts menu. See the example below and create Zabbix scripts for RAy3 units.

Name	Scope	Used in actions	Type	Execute on	Commands	User group	Host group	Host access
RAy3 Configuration backup	Manual host action		Script	Server	/usr/lib/zabbix/externalscripts /ray_cli_cnf_backup_get.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr/lib/zabbix/externalscripts /script-log.txt	All	RAy3	Read
RAy3 Display the firmware version	Manual host action		Script	Server	/usr/lib/zabbix/externalscripts/ray_cli_fw_show.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr /lib/zabbix/externalscripts/script-log.txt	All	RAy3	Read
RAy3 Upgrade the firmware to 2.0.3.0 (both units)	Manual host action		Script	Server	/usr/lib/zabbix/externalscripts/ray_cli_fw_upgrade.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} "/var/lib /zabbix/firmware/ray3/ray3-fw-2.0.3.0.cpio" "2.0.3.0" 2>>/usr/lib/zabbix/externalscripts/script-log.txt	All	RAy3	Read

Fig. 3.22: RAy3 scripts in Zabbix

If you open one of them, you can modify them as required. If you do not have any, you need to create them from scratch.

Configuration backup – the script creates a configuration backup file in /var/lib/zabbix/configuration-backup/ray/ directory. The name is taken from RAy3 S/N and Ethernet IP.

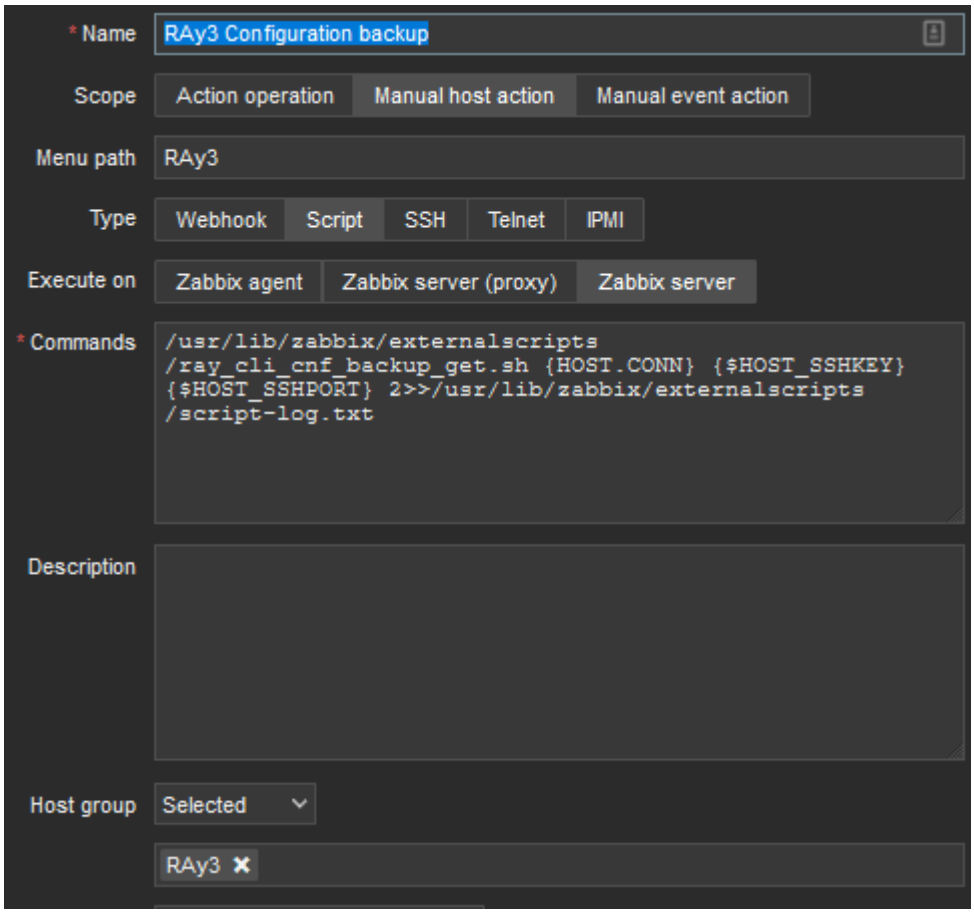

Fig. 3.23: RSS sample script details

- Name: RAy3 Configuration backup
- Scope: Manual host action
- Menu path: RAy3

- Type: Script
- Execute on: Zabbix server
- Commands:

  /usr/lib/zabbix/externalscripts/ray_cli_cnf_backup_get.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr/lib/zabbix/externalscripts/script-log.txt

Set other parameters to suit your needs.

Displaying firmware version – the script reads a current FW version installed in RAy3 unit.

All is the same, except the “Commands” parameter:

/usr/lib/zabbix/externalscripts/ray_cli_fw_show.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr/lib/zabbix/externalscripts/script-log.txt

Upgrading firmware version – the script uploads a firmware file and a special CLI script into local RAy3 unit which is then executed and FW of both units within the link are upgraded. The script command is:

/usr/lib/zabbix/externalscripts/ray_cli_fw_upgrade.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} "/var/lib/zabbix/firmware/ray3/ray3-fw-2.0.3.0.cpio" "2.0.3.0" 2>>/usr/lib/zabbix/externalscripts/script-log.txt

The parameters are MACROs which should be enabled by default due to our Template. Each RAy3 unit uses the SSH port 22 and the SSH key saved in /var/lib/zabbix/.ssh/rsa file by default. If you need to modify any of these parameters, go to the Configuration – Hosts menu and edit the particular Host’s MACROs.

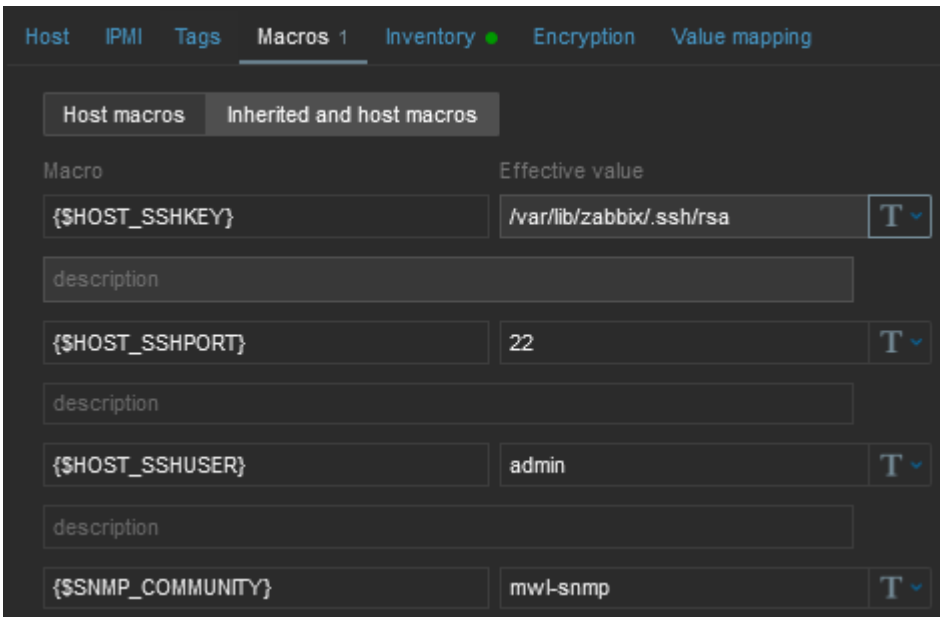

Fig. 3.24: Host MACROs

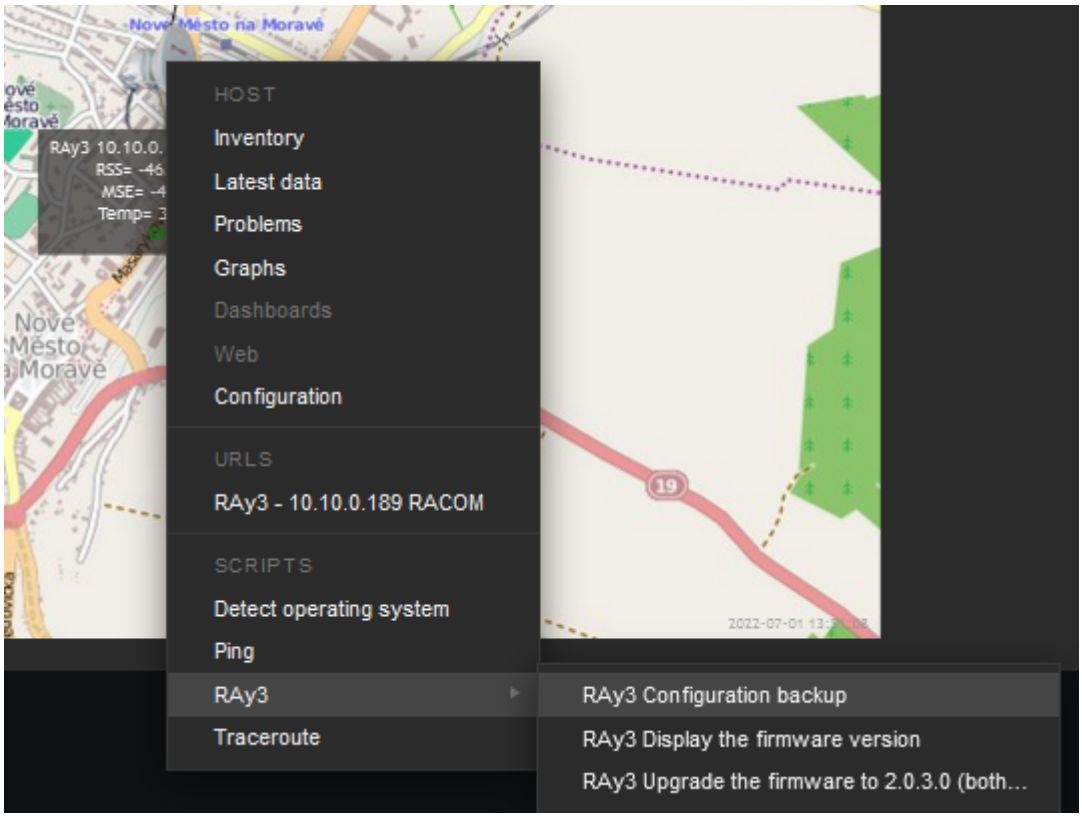

Fig. 3.25: RAy3 scripts – map

The easiest script displays the FW version.

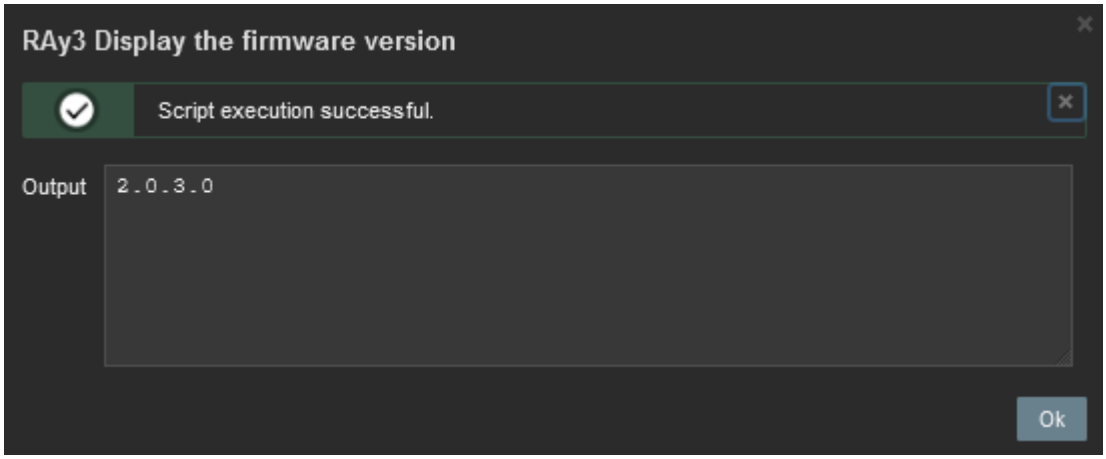

Fig. 3.26: Displaying FW version script output

Another script is the Configuration backup. The expected output should display a full path to the stored file.

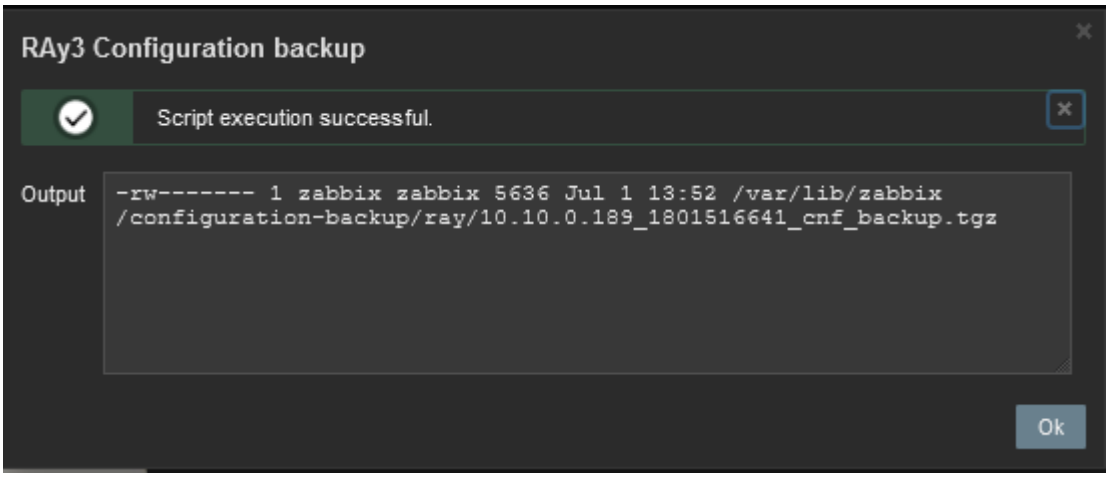

Fig. 3.27: RAy3 Configuration backup script output

The last script should be first tested and verified in RAy3 units/links which are e.g., on your desk so that you double-check a correct behaviour.

3.3.7. Branding

Zabbix 6.0 LTS offers you to use your own company's branding instead of Zabbix ones, or RACOM logos in case of using RZA6.

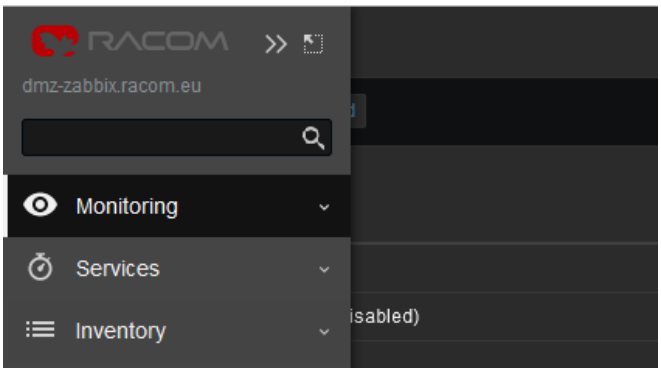

Fig. 3.28: RACOM Branding

General and brief procedure is described here:
https://www.zabbix.com/documentation/current/en/manual/web_interface/rebranding

For the RZA6, we created a file /usr/share/zabbix/local/conf/brand.conf.php with this content:

```
<?php
return [
'BRAND_LOGO' => 'racom/racom_logo.png',
'BRAND_LOGO_SIDEBAR' => 'racom/racom_logo.png',
'BRAND_LOGO_SIDEBAR_COMPACT' => 'racom/racom_logo_compact.png',
#'BRAND_HELP_URL' => 'https://www.racom.eu/ APP NOTE LINK '
];
```

Logos were scaled to 140x20 and 20x13 (compact one). The logos are placed in /usr/share/zabbix/racom/ directory. After these changes, the Login screen can look like:

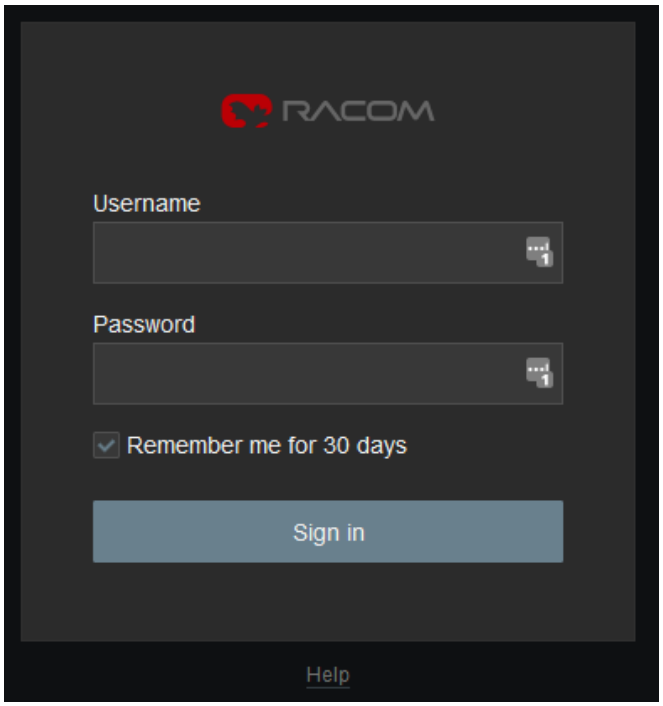

Fig. 3.29: RACOM Branding login page

If you need any additional help or information, do not hesitate to contact *support@racom.eu*[13]. We are ready and happy to help you.

We do recommend using our RZA6 solution. If not in your real network, then as a start for getting familiar with RAy3 SNMP and Zabbix NMS, because RZA6 has many configuration steps pre-configured and done.

[13] mailto:support@racom.eu

Revision History

Revision 1.0 2019-09-11
First issue - FW 1.0.14.0

Revision 1.1 2019-11-29
The SNMP product OID of RAy3 changed from '1' to '4'. FW 1.0.16.0.

Revision 1.2 2021-01-19
Small changes regarding CentOS8 and Zabbix5.

Revision 1.3 2022-07-28
Zabbix 6.0 LTS, Debian11 update.