RACOM
RADIO DATA NETWORKS

Application notes

Link to ISP

No IDU unit needed !

Gb Eth + PoE

Switch / Router

Network management via HTTP(s) or SSH

WiFi hotspot

PC/SERVER

more LAN devices

Surveillance IP camera

RAy2 – Microwave link

version 1.5
7/15/2016
fw 1.1.x.x

Table of Contents

List of Figures

1. Simple Network Management Protocol in RAy2 Units

RAy2 utilises SNMP versions **SNMPv1** and **SNMPv2c** – using a **community string** for authentication, which is by default "**snmp-racom**", but can be changed. SNMP uses UDP protocol for communication; delivery checks are implemented from version 2 onwards.

> **Note**
>
> The RAy2 MIB module complies with Severity level 3 validation.

By default RAy2 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. RAy2 replies from port 161 to the port dynamically selected by the manager.

RAy2 launches the SNMP agent automatically on start-up if enabled. RAy2 also sends alarm states (traps) to the manager via the port 162 (SNMPTRAP).

> **Note**
>
> To see the RAy2 MIB table, download it from the RAy2 web interface (**Maintenance → Backup → SNMP MIB → Download**) and use any document reader you prefer.

1.1. RAy2 SNMP Settings

The SNMP agent is switched off by default. You can enable or disable it in the **Link Settings → Service access → Services** menu.
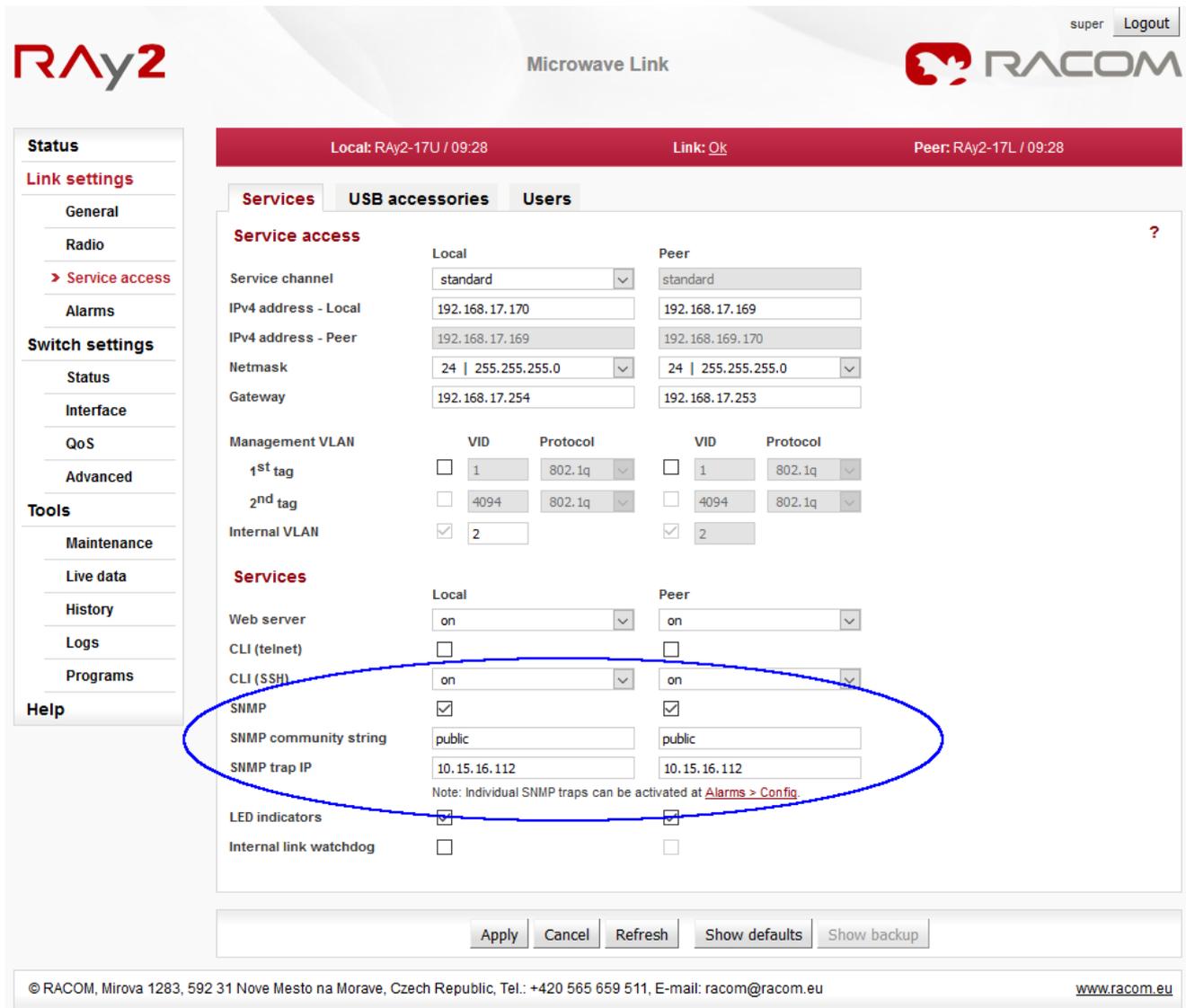
Fig. 1.1: RAy2 SNMP settings

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

Up to three SNMP trap IP addresses can be defined. The IP addresses must be delimited with a comma, e.g."192.168.1.1, 192.168.20.8". All traps are then sent to all defined IP addresses.

1.1.1. 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. 1.2: Alarms – Status screen

Alarm severity scale:

- critical

- major

- minor

- 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.

1.1.2. 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.
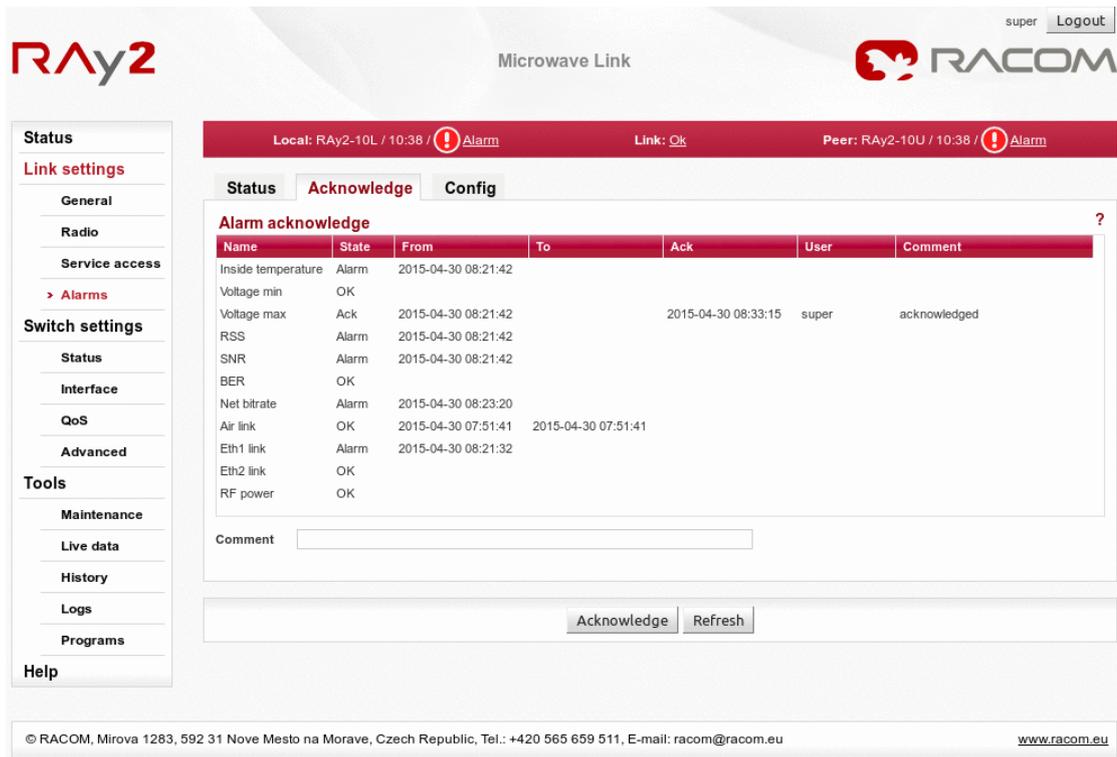
Fig. 1.3: Alarm Acknowledge screen

1.1.3. 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. 1.4: Alarm Config screen

Configurable traps:

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
SNR [dB]	- Signal to Noise Ratio
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
RF Power fail	- Loss of transmit power (not applicable for RAy2-17 and RAy2-24)

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 RAy2 template.

1.2. 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.

The Zabbix website provides the following short description:
Zabbix is the ultimate enterprise-level software designed for monitoring availability and performance of IT infrastructure components. Zabbix is open source and comes at no cost.

If you have chosen the Zabbix software, please read the following pages where we offer a basic Starting Guide to RAy2 and Zabbix co-working.

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

Note

The following guide was tested with Zabbix release 3.0.1. If you use any older release, refer to the previous version of this Application note (in the Archive section).

Take the opportunity to remotely access and test a live Zabbix demo[1]. Contact us for access[2] details.

1.2.1. Installation and Documentation

Due to security requirements and the mission-critical nature of the monitoring server, we believe UNIX is the only operating system that can consistently deliver the necessary performance, fault tolerance and resilience.

Zabbix has been tested on the following platforms:

- AIX
- FreeBSD
- HP-UX
- Linux
- Mac OS X
- Open BSD
- SCO Open Server
- Solaris
- Tru64/OSF
- Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, Windows 8 (Zabbix Agent only)

For further details, visit Zabbix Documentation at http://www.zabbix.com/documentation.php. It contains a large body of information about installation steps, configuration, performance etc. If you are unsure how to proceed with any task, refer to the Zabbix documentation first. You can find an installation guide there, too.

This Guide does not present all Zabbix settings, but should help you incorporate the RAy2 SNMP functionality into the Zabbix software.

---

[1] http://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
[2] http://www.racom.eu/eng/products/remote-access.html#load(product=zabbix)

Note

The following guide requires the use of MySQL database in Zabbix. If you choose other software, you will need to alter at least the trap handling bash script provided. This guide was tested in the CentOS 7 Operating System; some tasks may require a different approach in other systems.

Windows Installation

If you choose to use the Windows platform as the host operating system for Zabbix, VMware/VirtualBox software and then the Zabbix Appliance. The Zabbix Appliance can be downloaded from http://www.zabbix.com/download.php. Please remember that Zabbix Appliance is not intended for serious production use at this time.

VMware download: https://www.vmware.com/support/
VirtualBox download: https://www.virtualbox.org/wiki/Downloads
See the respective documentation to install and use virtualisation software.

1.2.2. Templates

After successful installation, you can import any of the predefined templates. Each template is the collection of Zabbix Items corresponding to a set of OIDs, triggers, graphs and applications. The template can be easily linked to any monitored host (RAy2) allowing quick access to the required values.

What Templates do we Provide?

The Templates list:

- Name: RAy2 Template
  - Consists of all specific OIDs provided by RACOM for RAy2 units RAy2-11, RAy2-17, ... and OIDs for the Ethernet statistics
- Name: PING Template
  - Pings a defined host and triggers whenever the host is unreachable

All templates can be downloaded from the RAy2 download site at http://www.racom.eu/download/hw/ray/potencial/eng/02_fw/RAy2_Zabbix_templ.zip

Note

For RAy1 templates, see the Archive section on our WEB page at http://www.racom.eu/download/hw/ray/free/eng/08_ray1/RAy-AppNote-en.pdf

How do I Import the RAy2 Templates?

In order to import the template, click on the **Configuration → Templates** button at the top of the Zabbix web page. Select the Import Template button at the top right corner.

Fig. 1.5: Importing Template button

Note

With Zabbix 3, Value mappings can be imported together with the template.

Import file	Procházet...	zbx_export_ray2.xml		

Rules	UPDATE EXISTING	CREATE NEW	DELETE MISSING
Groups		☑	
Hosts	☐	☐	
Templates	☑	☑	
Template screens	☑	☑	☐
Template linkage		☑	
Applications		☑	☐
Items	☑	☑	☐
Discovery rules	☑	☑	☐
Triggers	☑	☑	☐
Graphs	☑	☑	☐
Screens	☐	☐	
Maps	☐	☐	
Images	☐	☐	
Value mappings	☐	☑	

Import   Cancel

Fig. 1.6: Importing Template options

Now you can see the RAy2 template in the Template list window along with the other default templates.

Note

If you already imported the template and you need to update it, just import the newer version with the same name and the current template will be automatically overwriten.

Each **Item** has a Description, SNMP OID number, community string, UDP port (161), key, update interval and other parameters assignet to it. One of the key parameters is the update interval, because it defines how often Zabbix will request various replies from the RAy2 stations. These intervals are different for individual OIDs and are predefined based on our experience. You could consider changing these to suit your needs. For more details, read Section 1.2.3, "RAy2 Templates in Detail".

Individual items can be enabled or disabled.

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

The items are divided into usage groups, called **Applications** in Zabbix. These applications serve to provide better clarification of the defined items.

If you wish to be notified whenever any monitored value is out of its threshold range, you can define a **Trigger** for this purpose. These notifications are viewable on the Zabbix dashboard, item history or you can have e-mail / jabber / sms notifications enabled. Each notification can have one of six predefined severity levels (warning, critical, …).

> **Note**
>
> You can use a Clone option to create a copy of any template item or trigger for an individual host. In this case, you can edit its predefined values to meet your requirements for each host separately.

Graphs are automatically created for each monitored numeric value, but you can also create special graphs with several values on a single graph. We provide 4 predefined graphs containing for example RSS & SNR & RF Power within one graph.

For more information, see the Zabbix documentation. You can delete, add or edit any template component. The predefined state serves as a quick start, but you do not have to use these at all and you can create your own set of monitored values/items.

1.2.3. RAy2 Templates in Detail

Approximately 75 enabled items are included in RAy2 templates. Most items are implemented by RA-COM, 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.

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 devided 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 SNR 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 RAy2 template, you approximately need about 0.5 GB of data for one RAy2 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 RAy2 units – we keep one year traps history.

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 RAy2 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 RAy2 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.

1.2.4. How to Import Monitored RAy2 Stations?

Now you have a working template, you need to define hosts (RAy2 stations). Each RAy2 station has its own IP address. The following steps will guide you through the Host Configuration.

To create a host, go to **Configuration → Hosts** and click on the **Create Host** button. Define the Host name and its IP address.

Host name	192.168.120.248
Visible name	RAy2-24 L
Groups	In groups
	RAy2-24

Fig. 1.7: Defining the Host name and its IP address

Alternatively you can define a Group for the hosts. Creating a **Group** is straightforward. You can create a new one while creating a host or you can do so by going to the **Configuration** → **Groups** tab and clicking on the **Create Group** button.

Linking a template to the host(s) is achieved under the same tab or you can open Template settings and link any desired host to it.

You have to set the IP address and the port number (161) for the SNMP interface. Otherwise, you won't be able to use any SNMP item.

The option "Use bulk requests" can be enabled with RAy2 units. This feature enables sending multiple SNMP queries within one UDP datagram.

Fig. 1.8: Defining the SNMP interface

> **Note**
>
> In this Host configuration menu, configure the Host Inventory to be filled in automatically.

Fig. 1.9: Defining the Host Inventory

Where can I See the RAy2 Monitored Values?

To check monitored values, go to the **Monitoring** → **Latest data** tab and choose the desired host from the Menu.

	NAME ▲	LAST CHECK	LAST VAL
▶	**Interface - Ethernet** (12 Items)		
▼	**Interface - radio** (11 Items)		
☐	Channel arrangement	2016-03-18 10:00:31	accp (1)
☐	Channel matching	2016-03-18 10:00:32	on (1)
☐	Configured RF Power in dBm	2016-03-18 10:00:38	3 dBm
☐	Current net bitrate in bps	2016-03-18 10:51:16	170.69 Mb
☐	Current RF Power in dBm	2016-03-18 10:51:16	-3 dBm
☐	Maximum net bitrate in bps	2016-03-18 10:00:26	358 Mbps

Fig. 1.10: RAy2 latest data

For each item, you can see a graph or a history table. If a trigger is configured for the item, the graph shows a line with a threshold value.
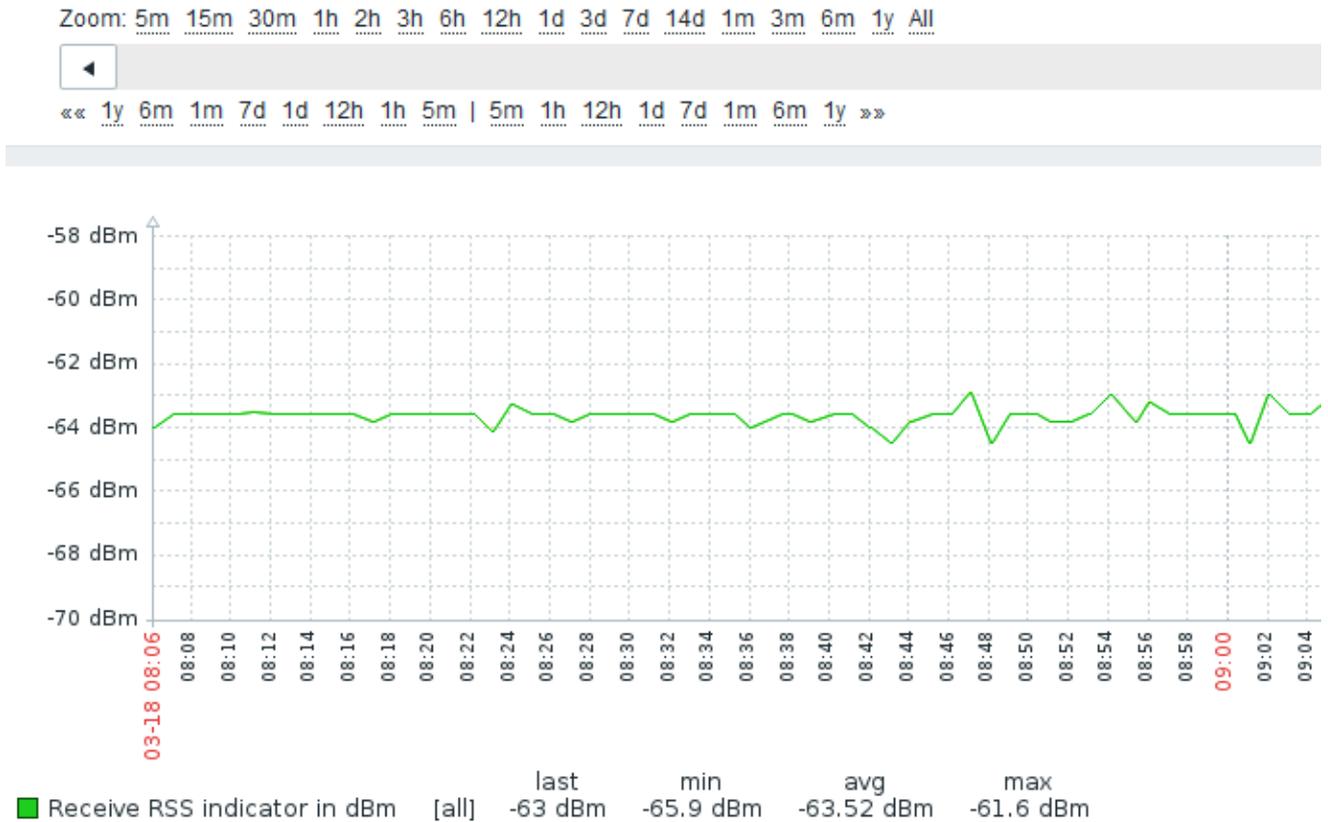
Fig. 1.11: RAy2 graph

1.2.5. Value Mappings

Responses from Several OID objects are unsigned integers, but these values do have a special meaning.

Example 1.1. Example RacomRay.systemStatus

- "0" stands for "na" (not available)
- "1" stands for "ok"
- "2" stands for "warning"
- "3" stands for "alarm"

Unfortunately, by default, you can see only the numeric values at the Zabbix front-end. The Value mappings are automatically imported with the RAy2 template or it can be imported separately in the Administration - General - Value Mappings menu.

Note

This syntax feature is used throughout all MIB tables, not only the RAy MIB table.

If you create any Value map manually, follow this procedure.

To add new value mappings, go to *Administration → General → Value Mapping*. Click on the "**Create value map**" button and insert the values, which are mentioned on the following lines. There is an Item list, which uses these value mappings (either link them manually or automatically by importing the template).

RacomRay.AlarmState	**Items:**
0 → na	Temperature alarm state
1 → up	Low voltage alarm state
2 → down	High voltage alarm state
3 → ack	RSS alarm state
	SNR alarm state
	Local Ethernet $1 Link Down alarm state
	RF Power Fail alarm state
	Net bitrate (air speed) below Limit alarm state
	BER alarm state
	Peer disconnect alarm state

RacomRay.channelArrangement	**Items:**
0 → na	Channel arrangement
1 → accp	
2 → acap	
3 → ccdp	

RacomRay.duplex	**Items:**
0 → na	Ethernet duplex - index $1
1 → full	

RacomRay.duplex	**Items:**
2 → half	

RacomRay.lineStatusII	**Items:**
0 → na	Radio link status
1 → setup	
2 → single	
3 → connecting	
4 → authorizing	
5 → ok	
6 → analyzer	

RacomRay.mdix	**Items:**
0 → na	Ethernet MDI-X / MDI - index $1
1 → mdi	
2 → mdi-x	

RacomRay.modulationIndex	**Items:**
0 → na	Tx modulation index
1 → qpsk	Rx modulation index
2 → qam16	
3 → qam32	
4 → qam64	
5 → qam128	
6 → qam256	

RacomRay.OptionSetting	**Items:**
0 → na	Management interface: Telnet
1 → on	Management interface: VLAN on/off
2 → off	Management interface: HTTP
	Secure peer mode
	Channel matching
	Ethernet pause - index $1
	Ethernet autonego - index $1
	Ethernet asymmetric pause - index $1

RacomRay.rfPowerStatus	**Items:**
0 → na	RF Power amplifier OK/Failure
1 → ok	
2 → fail	

RacomRay.ServiceState

0 → na

1 → up

2 → down

Items:

Peer station user Ethernet $1 link status

RacomRay.sshd

1 → na

2 → onlykey

3 → off

Items:

Management interface: SSH

RacomRay.systemStatus

0 → na

1 → ok

2 → warning

3 → alarm

Items:

Unit status

RacomRay.voltageSource

0 → na

1 → aux

2 → poe

Items:

Source of supply voltage

ICMP ping - Accessibility

0 → ICMP ping fails

1 → ICMP ping successful

Items:

ICMP ping - Accessibility

How can I Edit an Item to Link with a Value Map?

Go to **Configuration** → **Templates** and choose one of the imported template. Open the item configuration window and click on the chosen item to view and edit its settings.

Choose the appropriate value map in the Menu "Show value" and save the changes.

Example: RacomRay.sshd

Fig. 1.12: Linking a value map to an item

1.2.6. How do I Know that Something Has Happened to the RAy2 Station?

There are two ways to check the RAy2 stations. You can actively query the station in the defined time intervals or you can just wait for the trap to be received.

Active Querying

If you have a defined item which is updated e.g. every 10 seconds. Zabbix requests a reply to the SNMP GET message for the specific OID object and it stores this value in the database at 10 second intervals.

A trigger can also be configured for each item. For instance, temperature threshold alarm is set to 50°C. Whenever Zabbix receives an SNMP RESPONSE message from any monitored host with temperature higher than 50°C, an alarm is triggered. If the alarm is triggered, it is displayed at the Zabbix Dashboard. The Alarm will be visible in the "**Last 20 issues**" table and you will see which host is having an issue in the "**Host status**" table.

When the temperature falls back into the allowed range, the issue will be deleted from the Zabbix dashboard.

SNMP Traps

The key aspect of the SNMP are the TRAPS. These OID objects are not actively monitored by the Zabbix manager but by the RAy2 itself. For example an RSS value is too low: RAy2 sends a trap to the defined IP address of your NMS (Zabbix) which triggers an alarm.

How to Configure Traps in Zabbix?

This, unfortunately, is a somewhat complex procedure. There are several ways to configure traps – only one of them will be explained in this guide.

Note

Another approach could be using SNMPTT functionality.

You have to install an snmptrapd, a daemon which receives SNMP traps and passes them into the Zabbix front-end.

You can use the script (*snmptrap.sh*) which is included in the RAy2_Zabbix_templ.zip file downloadable from http://www.racom.eu/download/hw/ray/potencial/eng/02_fw/RAy2_Zabbix_templ.zip

website. Copy the script file 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
```

After that, you need to edit the file. By executing

```
$ which zabbix_sender
```

you will find the full path to this executable binary file. Change the path in the file, e.g.

```
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 script logs trap information into the /tmp/trap_messages.log file.

You should also check the LOG destination, which should be: /var/log/snmptrap/snmptrap.log. Create the directory if not already created and edit this in the snmptrap.sh script file.

```
LOGFILE=/var/log/snmptrap/snmptrap.log
```

Note

The log file could also be located in /var/log/zabbix/snmptrap.log if required.

Now we have our script prepared, let's configure the Zabbix front-end:

If you have not yet done so, import the RAy2 template. One application is called TRAPS and it consists of all traps. Link the template to desired hosts.

Note

If Zabbix receives a trap for an unknown host it will not be displayed.

The host MUST be configured using the IP address as the Host name, e.g.:

Host name: 192.168.10.1

Visible name: RAy2-17-L-1

SNMP interface: 192.168.10.1, port 161, IP

Along with this template, 11 new items and triggers appear at each used host. That is exactly the number of SNMP traps defined at the RAy2. Each trap should be recognized and the Zabbix should display the correct information message at the dashboard.

The template Application consists of 11 traps which corresponds with number of traps implemented in RAy2.

	WIZARD	NAME	TRIGGERS	KEY	INTERVAL ▲	HISTORY	TRENDS	TYPE	APPLICATIONS	STATUS
☐	•••	RF Power amplifier failure	Triggers 1	tr2RfPowerFail		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Supply voltage below minimal threshold	Triggers 1	tr2VoltageLowAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Local station Ethernet 1 link Up/Down	Triggers 1	tr2Eth1LinkDown		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	RSS exceeded the threshold	Triggers 1	tr2RssAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	BER exceeded the threshold	Triggers 1	tr2BerAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Supply voltage above maximal threshold	Triggers 1	tr2VoltageHighAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	SNR exceeded the threshold	Triggers 1	tr2SnrAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Temperature exceeded the threshold	Triggers 1	tr2TemperatureAlarm		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Air line disconnected	Triggers 1	tr2AirDisconnect		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Netbitrate (air speed) below threshold	Triggers 1	tr2NetBitrate		400d		Zabbix trapper	TRAPS	Enabled
☐	•••	Local station Ethernet 2 link Up/Down	Triggers 1	tr2Eth2LinkDown		400d		Zabbix trapper	TRAPS	Enabled

Fig. 1.13: RAy2 traps definition

RAy2 sends a trap whenever the watched value is out of range (or other configured condition is met) and whenever the value falls back within the corresponding range.

Every trap has two states in Zabbix. Each trap can either be in the alarm state (colors correspond to colors in the WEB interface) or in the OK state.

Note

There is third trap state on the RAy2 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.

You can also define Zabbix to send you an e-mail whenever any trap is triggered. See the Zabbix Documentation or Section 1.3, "Zabbix Alerting via e-mail" of this Application not for the e-mail configuration.

Please, find the file snmptrapd.conf usually it's in the /etc/snmp/ directory. Edit or create the file as root with the following lines:

```
authCommunity execute public
authCommunity execute PUBLIC
traphandle default /usr/lib/zabbix/externalscripts/snmptrap.sh
```

The first two lines will allow all received traps with community public or PUBLIC to be parsed and the third line will force the snmptrapd to use our script.

If you do not know what community names you will receive, add the following line to accept all community names.

```
disableAuthorization yes
```

Note

The default RAy2 community name is "racom-snmp", configure snmptrapd.conf accordingly.

Do not forget to restart snmptrapd. You should have similar snmptrapd parameters in the /etc/sysconfig/snmptrapd file:

```
OPTIONS="-Lsd -p /var/run/snmptrapd.pid -On"
```

This ensures that snmptrapd daemon will not translate the numerical OID numbers which is important for our script to run properly.

Important

If you install Zabbix on the CentOS distribution, do not forget to enable snmptrapd within SELinux security rules.

SELinux is an important security part of CentOS. Running all the functionality of Zabbix will require configuring these rules. If you do not understand it, consult the required changes with our technical support.

Basic Trap Functionality Tests

Now Zabbix is ready to receive SNMP traps from all RAy2 stations and enter them into the database properly. In order to test it, force the trap to be sent from any RAy2 and see whether it appears in the Zabbix front-end. If not, check that the respective UDP port (162) is enabled at your firewall and check the settings again. You can also execute Tcpdump or Wireshark at the selected interface of your Zabbix server or somewhere along the intended packet path.

Another basic test can be run using the following command:

```
zabbix_sender -z localhost -p 10051 -s "192.168.10.1" -k tr2RssAlarm -o "tr2RssAlarm, ▶
ALARM: UP"
```

The IP address of your RAy2 station is 192.168.10.1, key is "tr2RssAlarm" and the message for the Zabbix server is "tr2RssAlarm, ALARM: UP". The command should trigger the host's "RSS exceeded the threshold" alarm. Note that you need to have a host configured with this IP address, otherwise the trap will not be shown.

It is important to set the KEY value correctly, otherwise the trap would not match the trigger. See more KEY values with their description below:

- *tr2TemperatureAlarm* - Temperature exceeded the threshold
- *tr2VoltageLowAlarm* - Supply voltage below minimal threshold
- *tr2VoltageHighAlarm* - Supply voltage above maximal threshold
- *tr2RssAlarm* - RSS exceeded the threshold
- *tr2SnrAlarm* - SNR exceeded the threshold
- *tr2BerAlarm* - BER exceeded the threshold
- *tr2AirConnectDisconnect* - Air line disconnected
- *tr2Eth1LinkDown* - Peer station Ethernet 1 link Up/Down
- *tr2Eth2LinkDown* - Peer station Ethernet 2 link Up/Down
- *tr2RfPowerFail* - RF Power amplifier failure
- *tr2NetBitrate* - Air speed below threshold

If you want to clear the trap alarm, just repeat the same zabbix_sender command, but change the message to contain the word "DOWN", E.g. "ALARM DOWN".

Fig. 1.14: RAy2 temperature trap triggered

You can also see Trap's output in **Monitoring → Latest Data → TRAPS of your RAy2 station → History**. The displayed information differs based on the trap received. See the detailed description in the respective Zabbix item.

1.2.7. How to Access RAy2 GUI from Zabbix

Zabbix can offer various ways of accessing the RAy2 web interface by clicking on the link within the Zabbix front-end.

Map URL

For every Host depicted in Maps, you can define its URL.

Fig. 1.15: Map URL definition

After clicking on the Host, a new Item appears (URL), defined with the Name and the actual link. And when you click on this URL, the RAy2 web interface appears.
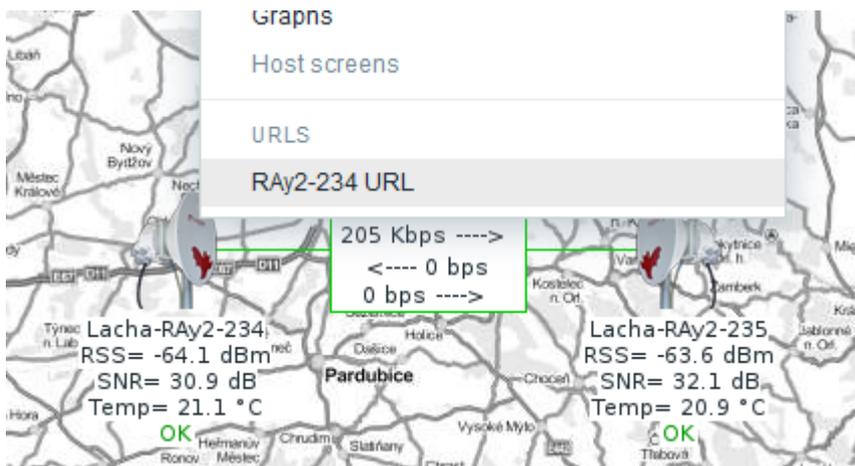
Fig. 1.16: RAy2 URL Link in maps

Trigger URL

Every host can have as many Triggers as required. And for every Trigger, the respective URL can be defined. Just add the URL in the Trigger configuration page.

Fig. 1.17: Trigger URL definition

After you do so, every time the trigger is activated, you can click on the Issue description within Dashboard's "Last 20 Issues" window and then on the URL link.

Fig. 1.18: Issue description used as a link

A simple click can forward you to the RAy2 web interface.

Inventory URL

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.
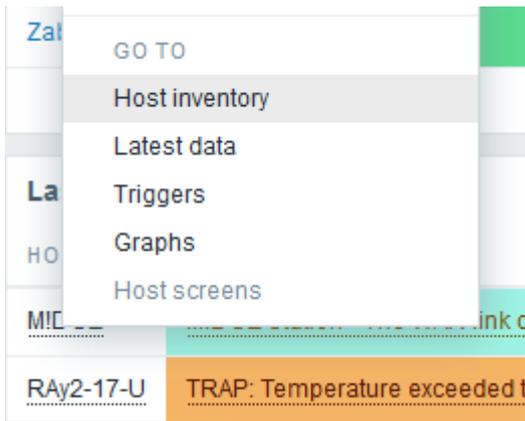
Fig. 1.19: Inventory URL definition

Every host's Inventory can be opened from the Dashboard's "Last 20 Issues" window. And in the Details, there is the configured URL displayed.
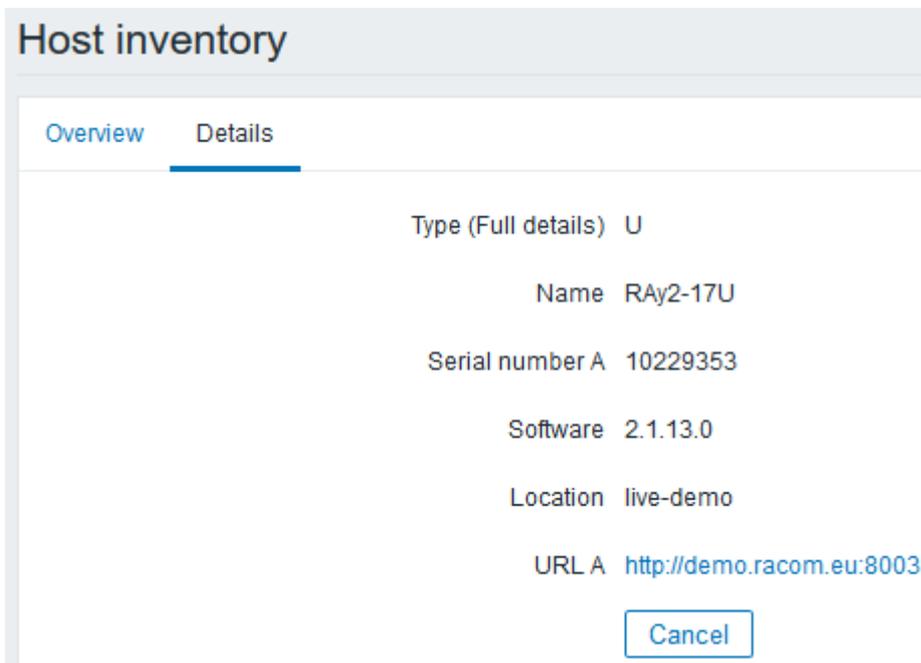
Fig. 1.20: RAy2 URL link in the Inventory

1.2.8. What Else does Zabbix Offer?

There are many features provided by the Zabbix software. They are described in the Zabbix Documentation. Below are just a few of them.

You can create Screens. A Screen is a set of various graphs on one page for better overview of your network (temperature, UCC, RF power, …).

You can create Maps. If you administer many stations in many locations, a Map can be a good choice. You can define the background picture (e.g. real maps), various station pictures, station status, various statistics, etc. You can import any icon or background picture you want to use.
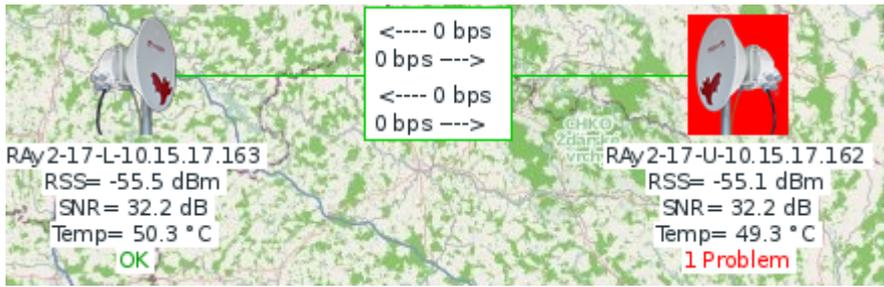
Fig. 1.21: Basic map with two RAy2 stations

A short example of RAy2 station configuration in Maps:

```
{HOSTNAME}
RSS= {{HOSTNAME}:rss.last(0)}
SNR= {{HOSTNAME}:snr.last(0)}
Temp= {{HOSTNAME}:temperatureModem.last(0)}
```


Fig. 1.22: Definition of RAy2 station in maps

For the link, you can define the throughput variables to be displayed.

Fig. 1.23: Definition of RAy2 link in maps

Each map can be divided into several sub-maps. It can be useful for various levels of detail.

1.3. Zabbix Alerting via e-mail

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. The following example will show just one procedure, other ways are possible (e.g. via the script).

1.3.1. E-mail Configuration

The e-mail can be set in the 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. 1.24: E-mail configuration

1.3.2. Users Configuration

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. 1.25: 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).

1.3.3. Actions

The last step is to configure the action – configure which issue causes the e-mail to be sent. Go the Configuration – Actions menu and create a new Action.

Fig. 1.26: Action

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

If the issue is fixed, we also send a recovery message. It is the same message, but saying "OK" instead of "PROBLEM".

Fig. 1.27: Action conditions

The action is executed if it meets the conditions, e.g. the trigger value is "PROBLEM" and the host is a RipEX (or RAy2 unit). The conditions can be combined with AND or OR statements.

Fig. 1.28: Action Operation

The operation does not need to be just an e-mail, but it can consist of sending SMS or jabber messages. Or based on the issue duration, it can perform different tasks. In the example above, we send the e-mail to the user "servis" immediately when the issue occurs. There are no additional steps.

1.4. RAy2 Firmware upgrade and other Useful Scripts

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 RAy2 template, we already prepared several examples:

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

Note

If you have troubles running scripts or making your own, contact us on `<support@racom.eu>`.

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 now realise, 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 RAy2 unit.

1.4.1. Zabbix Configuration

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 CentOS 7 operating system with Zabbix 3 installed via packaging system.

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

Zabbix Server Configuration File

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=/home/zabbix/.ssh
```

This is the location of the RSA private SSH key which will be used to access the RAy2 units.

Restart the Zabbix server afterwards.

```
# systemctl restart zabbix-server
```

Uploading the Template Scripts

The scripts must be uploaded manually to a correct directory manually. 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/
total 48
-rw-r--r--. 1 zabbix zabbix   933 Mar 14 15:40 cli_upgrade_ray.sh
-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    77 Mar 15 08:31 script-log.txt
-rwxr-xr-x. 1 zabbix zabbix 17200 Mar  1 13:24 snmptrap.sh
```

There are three executable scripts via the Zabbix web interface (starting with "ray_") and one additional script "cli_upgrade_ray.sh" which is used by one of the previous script. 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/*
```

Zabbix User Configuration

The Zabbix user cannot login to the bash by default. We need modify the /etc/passwd file as follows:

```
# chsh -s /bin/bash zabbix
# cat /etc/passwd
zabbix:x:996:994:Zabbix Monitoring System:/home/zabbix:/bin/bash
```

Make sure that the last part after the ":" has a correct path to the bash binary.

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

```
# usermod -m -d /home/zabbix zabbix
# chown zabbix:zabbix /home/zabbix
# chmod 700 /home/zabbix
```

> **ℹ Note**
>
> You may need to run the "usermod" command once again.

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

```
# mkdir /home/zabbix/configuration-backup
# mkdir /home/zabbix/firmware
# mkdir /home/zabbix/configuration-backup/ray
# mkdir /home/zabbix/firmware/ray
# chown zabbix:zabbix -R /home/zabbix/
```

SSH Access to RAy2 units

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

```
# su zabbix
```

A new prompt appears. Because, we cannot access the RAy2 units using their password via scripts, 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

```
bash-4.2$ ssh-keygen -t rsa
```

Follow the guide of the ssh-keygen application and leave the passphrase empty.

To copy our RSA key into the RAy2 units, run the following command:

```
bash-4.2$ ssh-copy-id admin@10.250.2.225
```

Just replace 10.250.2.225 with the correct RAy2 IP address. The prompt will ask for the Admin password, fill it in and click Enter. Now, you should have the access into the unit without using a password. Check it via this command:

```
bash-4.2$ ssh admin@10.250.2.225
```

You should be logged in the RAy2 unit without writing the password.

Scripts in the Zabbix Web Interface

The script files can be downloaded within the template ZIP file[3]. Save them in the correct directory (/usr/lib/zabbix/externalscripts/) of your Zabbix distribution. Then, the scripts must be manually created in the Zabbix Administration - Scripts menu. See the example below and create Zabbix scripts for all RAy2 scripts.
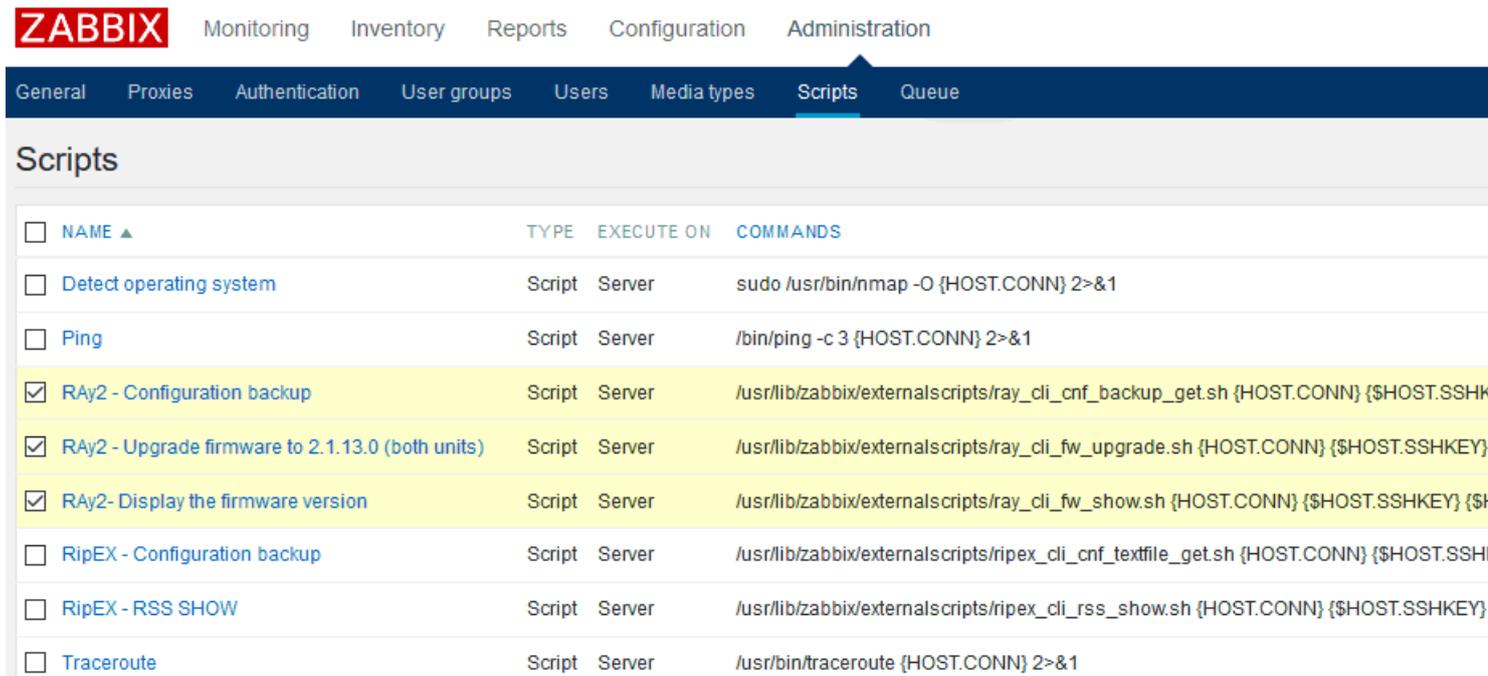
Fig. 1.29: RAy2 script

If you open one of them, you can modify them as required.

Scripts

Name	RAy2 - Configuration backup
Type	Script ▾
Execute on	Zabbix agent Zabbix server
Commands	/usr/lib/zabbix/externalscripts /ray_cli_cnf_backup_get.sh {HOST.CONN} {$HOST.SSHKEY} {$HOST.SSHPORT} 2>>/var /log/zabbix/scripts.log
Command	
Description	
User group	All ▾
Host group	Selected ▾
	RAy2 ✕ Select
Required host permissions	Read ▾
Enable confirmation	☐
Confirmation text	Test confirmation

Update   Clone   Delete   Cancel

Fig. 1.30: Script configuration

The Type must be set to "Script" and the Execute on parameter to "Zabbix server". The command can be modified as required. There is a full path to the script saved on the server and the parameters. The script output is appended to the mentioned log file.

The script can apply to ALL hosts or just one group – in our example, the group name is "RAY2".

The parameters are MACROs which should be enabled by default due to our Template. Each RAy2 unit uses the SSH port 22 and the SSH key saved in /home/zabbix/.ssh/id_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 (Inherited and host macros submenu).
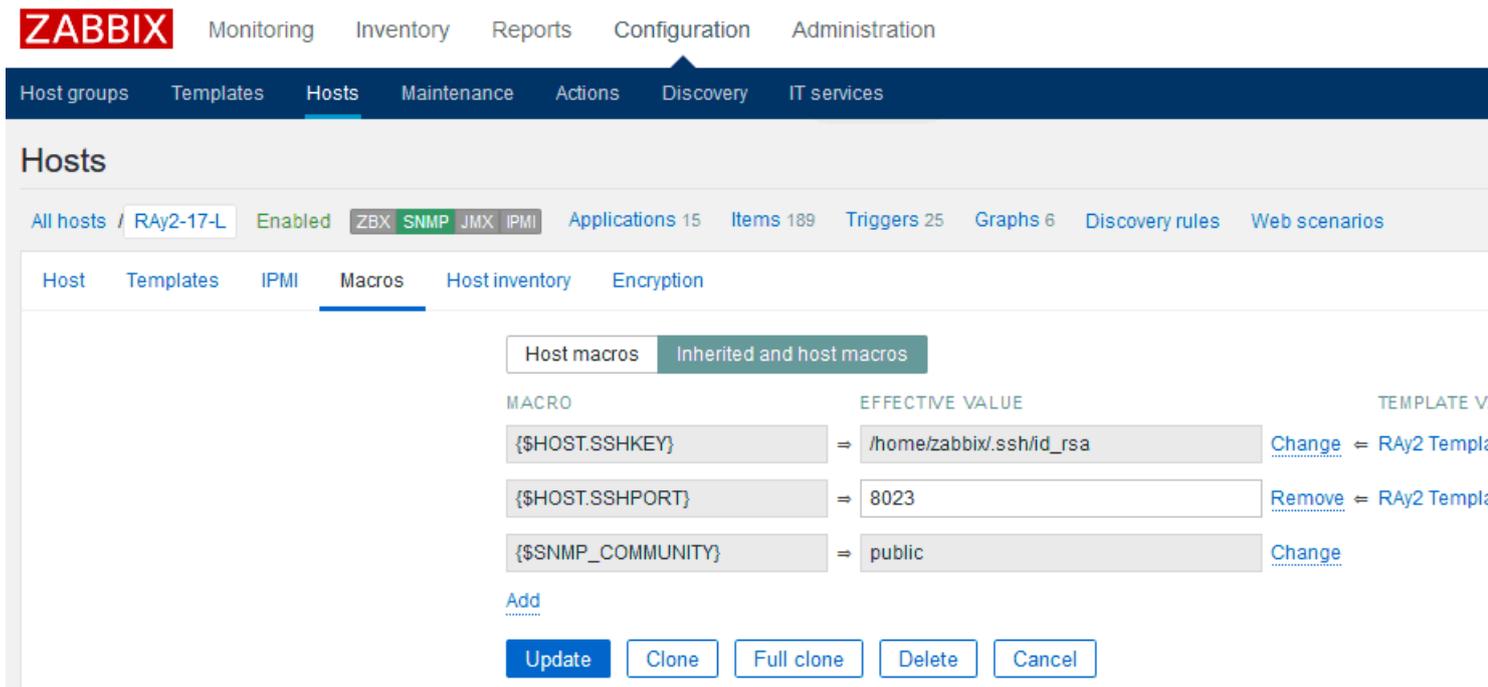
Fig. 1.31: Host MACROs

To edit any of the parameters, click on the "Change" button and Update the Host.

SELinux Restrictions

If the operating system is CentOS 7 and has the SELinux security option enabled, the scripts will not run properly due to these restrictions.

If you run the script, but it will not run properly, check the following output via the command line:

```
# ausearch -m avc|tail -n 3
```

It can display a similar output:

```
time->Tue Mar  8 14:12:31 2016
type=SYSCALL msg=audit(1457442751.052:8277): arch=c000003e syscall=42 success=no exit=-13 ▶
a0=3 a1=7f11466de620 a2=10 a3=56decfbf items=0 ppid=4929 pid=2936 auid=4294967295 uid=996 ▶
gid=994 euid=996 suid=996 fsuid=996 egid=994 sgid=994 fsgid=994 tty=(none) ses=4294967295 ▶
comm="ssh" exe="/usr/bin/ssh" subj=system_u:system_r:zabbix_t:s0 key=(null)
type=AVC msg=audit(1457442751.052:8277): avc:  denied  { name_connect } for  pid=2936 ▶
comm="ssh" dest=8021 scontext=system_u:system_r:zabbix_t:s0 ▶
tcontext=system_u:object_r:zope_port_t:s0 tclass=tcp_socket
```

The issue here is that the SSH cannot be run from the Web interface. To enable it, you can run the following commands. Note that the first command installs some binaries to control SELinux rules. If already installed, you do not need them.

```
# yum install policycoreutils-devel
# mkdir -p /root/local-policy-modules/zabbix
# cd /root/local-policy-modules/zabbix
# grep "denied" /var/log/audit/audit.log|tail -n 2 > avc.log
```

```
# audit2allow -M zabbix_script_ssh -R -i avc.log
# semodule -i zabbix_script_ssh.pp
```

⚠️ **Important**

Do not rush with SELinux rules, if you understand SELinux, make the required changes. If not, please consult us.

A similar approach is required for the Bash, SNMP traps, logging the script output, etc.

Testing Scripts

The scripts can be tested via clicking on the Hosts in the Web interface. You can click on them when they are displayed within the Last 20 Issues on your Dashboard, or within Maps where they are always displayed.
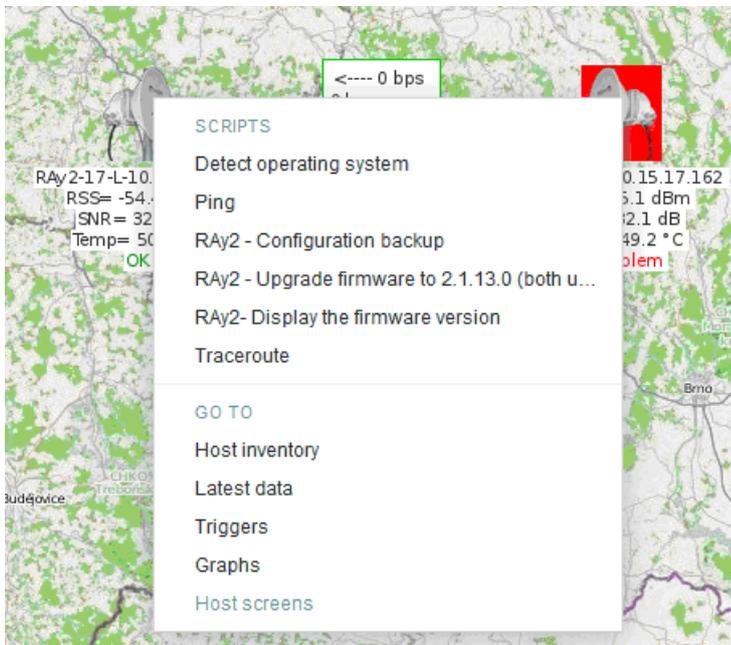
Fig. 1.32: Scripts in the Maps

If you click on any of the scripts, the corresponding script runs and the output is displayed in the pop-up window. You can test the Zabbix general ones such as "Ping" or "Traceroute" first.

ℹ️ **Note**

You may be required to change the SELinux rules or to install "traceroute" application via the command line (yum install).

The easiest script displays the current firmware version. The version should be displayed within several seconds in the pop-up window.

Another script is the Configuration backup. The expected output should display a full path to the stored file (in the /home/zabbix/configuration-backup/ray directory).

The last scripts makes the Firmware upgrade. The script copies the firmware and another script into the unit and if successfully transmitted, it displays the information in the pop-up window. Due to Zabbix

functionality, there is no way to wait for the upgrade to be finished and be informed about it within this pop-up window. Check the Firmware version after several minutes (e.g. 10 minutes) to check whether the upgrade was successful. Note that the script upgrades both units of the selected link! If the upgrade was not finished successfully, check the LOG file or login to the unit via SSH and check the internal log files (/var/log/) and the script log in the /tmp directory. You may also need to check the SELinux rules.

Once configured correctly, running the scripts is easy. If you need to add a new host, just copy the SSH key and you are ready to use it. And if a new script is required, see these examples and create your own scripts or consult creating them with our technical support at `<support@racom.eu>`.

Appendix A. Revision History

Revision 1.1   2013-11-19
First issue – Simple Network Management Protocol in RAy Units

Revision 1.2   2013-11-19
adjustments in section Value Mappings

Revision 1.3   2014-09-09
Added Section 1.2.7, "How to Access RAy2 GUI from Zabbix"

Revision 1.4   2015-05-15
Updates for RAy2

Revision 1.5   2016-07-01
Added Section 1.3, "Zabbix Alerting via e-mail" and Section 1.4, "RAy2 Firmware upgrade and other Useful Scripts"