Application notes

RipEX - SNMP

version 1.2
1/20/2021
# Table of Contents

1. Simple Network Management Protocol ................................................................. 5
   1.1. How does SNMP work? ....................................................................................... 5
   1.2. SNMP communication ....................................................................................... 5
   1.3. MIB database – Management Information Base .................................................. 6
2. SNMP in RipEX ......................................................................................................... 7
   2.1. Limitations ........................................................................................................... 7
   2.2. RipEX SNMP Settings ......................................................................................... 9
   2.3. RipEX Traps/informs Description ....................................................................... 9
3. Network Management System – ZABBIX .............................................................. 11
   3.1. Installation and Documentation ........................................................................ 11
   3.2. Templates ........................................................................................................... 12
   3.3. How to Import Monitored RipEX Stations? ....................................................... 18
   3.4. Value Mappings ................................................................................................. 20
4. How do I Know that Something Has Happened to the RipEX Station? ............... 27
   4.1. Active Querying ................................................................................................. 27
   4.2. SNMP Traps/Informs ......................................................................................... 27
5. What Else does Zabbix Offer? .................................................................................. 36
6. How to Access RipEX GUI from Zabbix ................................................................. 37
   6.1. Map URL ............................................................................................................. 37
   6.2. Trigger URL ......................................................................................................... 37
   6.3. Inventory URL .................................................................................................... 38
7. Zabbix Alerting via e-mail ...................................................................................... 40
   7.1. E-mail Configuration ......................................................................................... 40
   7.2. Users Configuration ........................................................................................... 40
   7.3. Actions ................................................................................................................ 41
8. RipEX Scripts in Zabbix .......................................................................................... 45
   8.1. Zabbix Configuration ......................................................................................... 45
Revision History ........................................................................................................ 51
1. 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/informs).

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 RipEX)
   - 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/informs whenever the monitored values (watched values in RipEX, e.g. temperature) are outside the threshold range. RipEX is capable of sending SNMP traps/informs to up to three SNMP managers (since the firmware release 1.3).

1.2. SNMP communication

In SNMP, each value is uniquely identified using Object Identifier (OID). Standard communication starts by sending a request and then the response is returned. Alternatively, an agent can send an SNMP trap or inform (acknowledged trap).

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

SNMPv3 shall be used if the higher security of the monitoring traffic is required. SNMPv3 provides security with authentication and privacy. The manager is required to know an authentication and encryption methods and common secrets to authenticate itself and decrypt SNMP packets.

A **request** is sent to 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.

An **inform** is sent to the manager without its request and the manager acknowledges its successful delivery.
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 (for example, temperature, voltage, number of transmitted messages or bytes per second, etc.).

Trap/Inform sent from the agent to the manager whenever any monitored value is beyond its thresholds.

SetRequest used to set various parameters (unsupported by RipEX).

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:

RIPEX::serialNumber
serialNumber OBJECT-TYPE
-- FROM RIPEX
SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Product serial number."
 ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) racom(33555) ripex(2) ►
station(1) device(1) 4 }

As you can see, numbers 1.3.6.1.4.1.33555 are the “higher-level” OIDs. The “lower-level” OIDs are .2.1.1.4 which are allocated by RACOM.
2. SNMP in RipEX

RipEX SNMP protocols can be used to:

- Read configuration parameters,
- Read operation statistics (interfaces, ...), and
- Send traps/informs when set thresholds for monitored values are exceeded (TxLost [%], UCC, Temp, PWR, ...)

For detailed description of individual values refer to section RipEX MIB below.

RipEX utilises SNMP versions **SNMPv1, SNMPv2c** (using a configurable **community string** for authentication, which is by default “public”) and **SNMPv3** (using **Security User name**, **Security levels**, **Authentication** and **Encryption mechanisms**). SNMP uses UDP protocol for communication; delivery checks are implemented from version 2 onwards.

**Note**

The RipEX MIB module complies with Severity level 3 validation.

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

RipEX launches SNMP agent automatically on start-up if enabled. RipEX also sends alarm states (traps/informs) to the manager via the port 162 (SNMP TRAP/INFORM). Users can change this port number in RipEX for each destination (up to three). The notifications’ behaviour can be influenced (see **Alarm management settings, RipEX manual, Adv. config.**

When using SNMP over radio channel we recommend setting RipEX to the Router mode. From the point of radio network, SNMP is typically a standalone application sharing the radio channel with others. Thus it causes collisions, which are automatically resolved by the radio channel protocol in the Flexible Router mode. The radio channel uses no protocol in the Bridge mode, meaning two competing applications can only be run at a great risk of collisions and with the knowledge that packets from both applications may be irretrievably lost.

**Note**

Since the firmware 1.6.x, Base Driven Protocol (BDP) has been introduced in the Router mode. SNMP can be, of course, used together with BDP. BDP’s mechanism ensures there is not a single collision on the radio channel.

### 2.1. Limitations

SNMP is primarily designed for Ethernet networks, where generally, bandwidth capacity is not an issue. By contrast, radio bandwidth capacity is very limited and RipEX mostly works over the radio channel. For this reason, special care is recommended while configuring NMS. If badly configured, NMS can take a significant portion of the network capacity or can even overload the network completely.

---

1 [https://www.racom.eu/eng/products/m/ripex/h-menu.html](https://www.racom.eu/eng/products/m/ripex/h-menu.html)
2.1.1. Bandwidth Consumption

- **SNMPv2c**
  It is important to realise that the average size of a single request and response to a specific OID is approximately 184 Bytes each. The entire MIB for a single RipEX with one neighbouring RipEX is approximately 48 kilobytes. Based on the limitations and the MIB size, we recommend to query only carefully selected OIDs over the radio channel and not all possible data. Set SNMP query time intervals in your NMS as long as possible. The shortest recommended interval ranges from several minutes to tens of minutes.

- **SNMPv3**
  With SNMPv3 it is more complicated to define bandwidth consumption because several security levels can be configured (NoAuthNoPriv, AuthNoPriv and AuthPriv). Each level requires different approach and number of packets. For each SNMP GET Request packet, SNMP Report is returned by RipEX (to get the current and unique EngineID, Engine Boots and Engine Time). The following steps are different upon the Security level configuration. For each level, there is an SNMP GET Request and SNMP Response.

  - **NoAuthNoPriv:**
    Both messages are sent in plain text. No authentication and no Encryption.

  - **AuthNoPriv:**
    The messages are authenticated, the packet size increases.

  - **AuthPriv:**
    The messages are authenticated and encrypted, the packet size is the highest.

To obtain any SNMP value using v3 consumes approximately two times more bandwidth compared to SNMPv2c. Keep this in mind in case of SNMP traffic over the Radio channel.

Wherever possible, use the RipEX Ethernet interface for SNMP communication to free up the radio channel.

**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.

2.1.2. Bandwidth Efficiency Tip

If you wish to monitor many watched values (VSWR, Temperature, UCC, …) from remote stations connected over the radio channel and you have a star topology network, you can improve bandwidth efficiency by reading OID values only from the Master (Repeater) RipEX station.

The advantage of the above is that the watched values from remote stations are broadcast in regular intervals and saved in the Master (Repeater) RipEX. These values from neighbouring stations have their own OID’s and can be downloaded from the Master (Repeater) RipEX.

In the picture below – Master RipEX station periodically reads watched values from its neighbouring Slave stations. Whenever the NMS requests any value mentioned, the reply is sent only from the Master station (over Ethernet) saving radio bandwidth. SNMP uses radio link only for sending SNMP Traps from any Slave to the NMS.
Note
The diagram is simplified - there are no flows for SNMPv3 PDUs, neither Inform's Acknowledgements.

Fig. 2.1: NMS communication with Slave stations

Note
In such a case, watched values from neighbouring stations are displayed as part of the Master (Repeater) station.

The OID of individual remote stations is based on the order in the Neighbours menu of RipEX web interface (i.e. 1st neighbour has the last OID digit set to 1, 2nd neighbour to 2, etc.). Due to its dynamic character, it may happen that the order might be changed each period (e.g. once a day), keep this in mind!

Important
To avoid this confusion, using Zabbix "dynamic indexes" is suggested. See the Section 3.2.3, "Reading Remote Watched Values" for more details about dynamic indexes and their usage with RipEX units.

2.2. RipEX SNMP Settings

SNMP agent is switched off by default. To enable it, go to the settings menu and click on the SNMP button.

Important
Thresholds for all SNMP traps/informs can be configured in the RipEX web interface, Settings → Alarm management. Since detailed description of RipEX SNMP settings can vary based on the current firmware, please kindly refer to the online Help accessible through the RipEX web interface or see the User manual, Chapter Settings (https://www.racom.eu/eng/products/m/ripex/h-menu.html#settings).

2.3. RipEX Traps/informs Description

The traps/informs are sent whenever any of the following watched values are beyond their threshold ranges:
• RSS (Received Signal Strength)
• DQ (Data Quality)
• TX Lost (The probability of a transmitted frame being lost)
• UCC (Power voltage [V])
• Temperature [C]
• RF Power [W]
• VSWR (Voltage Standing Wave Ratio, 1.0 = the best ratio, 1.0 – 1.8 = acceptable ratio, > 2.5 = indicates a serious problem in antenna or feeder)
• Ethernet RX/TX Packets ratio (Ratio between received and sent packets over Ethernet)
• COM1/2 RX/TX Packets ratio (Ratio between received and sent packets over COM ports)
• HW Alarm input
• Hot-Standby (SNMP trap containing active station identity – sent by the active station)
• Backup paths system (Backup path state and Alternative path state changes)
• Unit ready (the hardware alarm output or the SNMP trap indicates that the RipEX radio is ready to operate)
• Nomadic remote device is offline (A notification to indicate that Nomadic remote device is offline/online; i.e. status of connection to Nomadic base)
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.

The Zabbix website provides the following short description: 
Zabbix is the ultimate enterprise-level software designed for real-time monitoring of millions of metrics collected from tens of thousands of servers, virtual machines and network devices. 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 RipEX 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 5.0.x. 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. Contact us for access details.

3.1. 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:

- Linux
- IBM AIX
- IBM Power8
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows: all desktop and server versions since 2000 (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 RipEX SNMP functionality into the Zabbix software.

---

2 https://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
3 https://www.racom.eu/eng/products/remote-access.html#load(product=zabbix)
Note
The following guide requires the use of MySQL database (mariadb) 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 CentOS7 and CentOS8 operating systems; some tasks may require a different approach in other systems.

3.1.1. 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.

3.2. 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 (RipEX) and you can have access to the desired values very quickly.

3.2.1. What Templates do we Provide?

The Templates list:

- Name: RipEX Template
  o Consists of all specific OIDs provided by RACOM
  o Implements one neighbouring RipEX monitoring
- Name: RipEX – RFC1213 Template
  o Consists of supported RFC1213 OIDs
- Name: RipEX – RS232 Template
  o Consists of supported RS232 OIDs
- Name: RipEX – SNMP Trapper Template
  o Consists of SNMP traps
- Name: PING Template
  o Pings a defined host and triggers whenever the host is unreachable

All templates can be downloaded from the RipEX Download site at https://www.racom.eu/download/hw/ripex/free/eng/3_fw/RipEX_Zabbix_templ.zip.

How do I Import the RipEX 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.
Important

Since Zabbix 3, Value mappings can be imported together with the template. We highly recommend to do that. Check the option "Value mapping" while uploading the templates.

Select the RipEX template file and Import that file. Repeat this step for each template or import the `zbx_export_templates-RipEX-ALL.xml` template with all templates in one file.

![Import file](Procházek.png)

Now you can see the RipEX template in the Template list window along with 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 overwritten. The checkbox for Updating existing template must be checked.

Each Item has its Description, SNMP OID number, community string, UDP port (161), key, update interval and other parameters. One of the key parameter is the update interval, because it defines how
often Zabbix will request various replies from the RipEX stations. This interval is predefined to 30 minutes, but you should consider changing it to suit your radio network infrastructure.

The individual items can be in an active or disabled state. By default, only some items are active based on their importance – see the next chapter for more information. If you wish to monitor more values, activate the desired ones. But as already mentioned, preferably use the RipEX Ethernet interface for SNMP communication to free up the radio channel. If this is not possible, consider carefully whether monitoring other values is necessary.

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

The items are divided into the usage groups, called Applications in Zabbix. These applications serve for 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 it. 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, …).

We also provide several triggers within the templates. Triggers defined in templates cannot be edited within individual hosts, which means you cannot define various threshold ranges for hosts and each host would have the same threshold range. Please define your own triggers within each individual host.

**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 some basic watched values like temperature, UCC etc.

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 them at all and you can create your own set of monitored values/items.

### 3.2.2. Which Values/Items Should I Monitor?

The templates themselves are fully scalable and consist of many items. However, monitoring all of them is not required in a routine situation. Pre-activated items in RipEX default templates are:

- **RipEX Template**
  - Pre-activated Items: 5
  - Modem temperature (°C), RF power (W), TX lost (%), UCC (V), VSWR
- **RipEX – RFC1213 Template**
  - All items are disabled by default
- **RipEX – RS232 Template**
  - All items are disabled by default
- **RipEX – SNMP Trapper Template**
  - Five SNMP trap items and triggers are enabled by default. DQ and RSS triggers need to be cloned for individual hosts, because we cannot predefine remote hosts IP addresses. See **Section 4.2, “SNMP Traps/Informs”** for more information.
- **PING Template**
- Pre-activated Items: 1
- Default Update Time: 30 minutes
- The only active item checks the host reachability and triggers an alarm if the host is not reachable.

**Note**

If you need to monitor more than one remote RipEX station, you need to “clone” existing items for the remote station watched values.

### 3.2.3. Reading Remote Watched Values

Remote Watched values are read by Zabbix using the Dynamic indexes. This works on a basis of "snmpwalk" through all available remote units (neighbours) of specific RipEX (host). When it finds the correct neighbour (correct IP), it reads the watched value for this neighbour. E.g. local RipEX has 3 neighbours (10.10.10.1, .2 and .3) and we need to know the RSS level for the 10.10.10.2 host. Zabbix sends several "snmpgetnext" requests until it reaches the end of this SNMP branch (in our example, 4 snmpgetnext requests are sent). Thanks to this, Zabbix finds out that 10.10.10.2 has for example ID "2" and thus, Zabbix knows how to ask for the RSS value of this particular neighbour and sends the correct snmpget request. All values are readable by OID ending with this previously "unknown" ID.

**Note**

Without dynamic indexes, values for several remote units could be mixed together, because each History period, the IDs can be different for particular neighbours.

**Note**

Do not read remote watched values and remote statistic values from RipEX unit which is not reachable via Ethernet. If you read it from RipEX reachable via the Radio channel, it could send too much of data over the Radio channel and cause a decrease of available bandwidth for this link. Do it on your own risk and requirements (it is supported).

Each Host linked with a RipEX template automatically obtains {$NEIGHBOUR.1} user MACRO needed for reading remote watched values. This MACRO defines the IP address of the first RipEX neighbour of the particular "local" RipEX (host). If the monitored RipEX has more than one neighbour, you need to add additional neighbours to its MACRO list. Go to the Configuration -> Hosts -> choose the particular RipEX -> Macros -> Inherited and host macros -> Click on the "Add" button and define other neighbours.
Fig. 3.3: Host MACROs

Each Neighbour IP can be set as required. The default value for the first one is 192.168.169.169.

The \{$NEIGHBOUR.1\} user MACRO is also used for reading statistics of particular neighbours. The IP addresses are the same (since the firmware 1.6.x) and thus they do not need to be set separately. The only difference is that you also have a "RADIO BROADCAST" line is Statistics which is NOT in the Neighbours menu (RipEX GUI). Configure it as a separate neighbour MACRO, but do not use it for remote watched values.

By default, reading the watched values is disabled. To enable it, go to the Configuration -> Hosts -> choose the host -> Go to the Applications -> Choose "Watched values - Remotes" and enable required values. If more than one neighbour is required, you need to "Clone" the existing Items and change the ID of the specific Neighbour. For example, if you have 3 neighbours, for each Item (RSS, DQ, Temperature, ...) you need to:

- Open this particular Item within the Host's (local RipEX) watched values Items
- Click on the "Clone" button
- Change the ID from 1 to X, where X is the neighbour's ID (2, 3, ...), in the Name, Key and SNMP OID parameters!
- Click on the "Update" button
- Repeat the steps for the third neighbour as well
- Repeat the steps for all required Items
Fig. 3.4: Remote Watched values - Item Cloning

The same procedure must be done for Radio Statistics. By default, only the first neighbour and Total numbers are pre-defined. Broadcast and other hosts must be defined manually.

Values from any neighbour can now be displayed in the Latest data menu.

Fig. 3.5: Remote watched values - Latest values

3.2.4. MACROs

Macros are variables, identified by a specific syntax: \{MACRO\}. MACROs resolve to a specific value depending on the context. Effective use of MACROs allows to save time and make Zabbix configuration more transparent.

With our templates, each RipEX automatically obtains the following MACROs:

- \{$HOST.SSHKEY\} - Full path to a stored admin SSH key to access the unit (by default "/home/zabbix/.ssh/id_rsa"). See more details in Chapter 8, RipEX Scripts in Zabbix.
- \{$HOST.SSHPORT\} - SSH port to access the unit (by default "22")
- \{$NEIGHBOUR.1\} - Radio IP address of the first Neighbour (usage described in the previous paragraphs, by default "192.168.169.169")
- \{$SNMP.PORT\} - UDP port for SNMP queries (by default "161")
- \{$SNMP_COMMUNITY\} - SNMPv2c community string (security parameter in SNMP version 2, by default "public")
- \{$SNMP_PRIV\} - The encryption passphrase used in SNMPv3 (by default "racom")
- \{$SNMP_USER\} - User name used for authentication in SNMPv3 (by default "racom")

Note

SNMPv3 MACROs are not defined in SNMPv2c templates.
You can edit the values in Configuration -> Hosts -> choose the particular RipEX -> Macros -> Inherited and host macros. Edit any value and all Items will be automatically updated. Note that SNMPv3 Authentication (MD5, SHA), Encryption (DES, AES) and Security level (NoAuthNoPriv, AuthNoPriv, AuthPriv) methods cannot be defined by MACROs and must be edited within individual Items. Select all Items within the Template and use the "Mass update" button. Edit the parameters as required and all Hosts' parameters will be changed as well.

Note

If you need to have different Authentication and Encryption (or other) parameters in various network parts, you might Clone the templates and use particular Template for particular Group of Hosts.

3.3. How to Import Monitored RipEX Stations?

Now you have a working template, but you need to define hosts (RipEX stations). Each RipEX 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.

Fig. 3.6: 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.

Fig. 3.7: Host template
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 RipEX units. This feature enables sending multiple SNMP queries within one UDP datagram.

![Fig. 3.8: Defining the SNMP interface](image-url)

**Note**

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

Do not forget to edit the Host MACROs (e.g. Neighbours' IP addresses, SNMPv3 authentication, ...), see the previous section for details.

### 3.3.1. Where can I See the RipEX Monitored Values?

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

![Fig. 3.9: RipEX latest data](image-url)

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.
3.4. Value Mappings

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

Example 3.1. deviceMode

- “1” stands for “bridge” mode.
- “2” stands for “router” mode.

Unfortunately, by default, you can see only the numeric values at the Zabbix front-end. The Value mappings are automatically imported with the RipEX 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 RipEX 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).

Note

There are also several value mappings used at RFC1213 and RS232.

3.4.1. Value Mappings List

<table>
<thead>
<tr>
<th>RipEX.AlmState</th>
<th>Items:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1 ⇒ unknown</td>
<td>Alarm state - COM1 interface Rx to Tx packets ratio</td>
</tr>
</tbody>
</table>
### RipEX.AlmState

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>inactive</td>
</tr>
<tr>
<td>1</td>
<td>active</td>
</tr>
</tbody>
</table>

**Items:**
- Alarm state - COM2 interface Rx to Tx packets ratio
- Alarm state - Device temperature
- Alarm state - DQ
- Alarm state - ETH interface Rx to Tx packets ratio
- Alarm state - HW Input
- Alarm state - RF Power
- Alarm state - RSS
- Alarm state - Tx lost
- Alarm state - UCC
- Alarm state - Unit ready
- Alarm state - VSWR

### RipEX.BackupPathsState

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>unknown</td>
</tr>
<tr>
<td>1</td>
<td>up</td>
</tr>
<tr>
<td>2</td>
<td>down</td>
</tr>
</tbody>
</table>

**Items:**
- Backup Paths 1 - Alternative Paths - Currently passive paths State
- Backup Paths 2 - Alternative Paths - Currently passive paths State
- Backup Paths 1 - Alternative Paths - Currently used path State
- Backup Paths 2 - Alternative Paths - Currently used path State

### RipEX.comProtocol:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>3</td>
<td>AsyncLink</td>
</tr>
<tr>
<td>4</td>
<td>Modbus</td>
</tr>
<tr>
<td>5</td>
<td>IEC101</td>
</tr>
<tr>
<td>6</td>
<td>DNP3</td>
</tr>
<tr>
<td>7</td>
<td>UNI</td>
</tr>
<tr>
<td>8</td>
<td>Comli</td>
</tr>
<tr>
<td>9</td>
<td>DF1</td>
</tr>
<tr>
<td>10</td>
<td>Profibus</td>
</tr>
<tr>
<td>12</td>
<td>C24</td>
</tr>
<tr>
<td>13</td>
<td>RP570</td>
</tr>
<tr>
<td>14</td>
<td>Cactus</td>
</tr>
<tr>
<td>15</td>
<td>ITT Flygt</td>
</tr>
<tr>
<td>18</td>
<td>SLIP</td>
</tr>
<tr>
<td>19</td>
<td>Siemens 3964 (R)</td>
</tr>
<tr>
<td>20</td>
<td>PR2000</td>
</tr>
</tbody>
</table>

**Items:**
- COM1 - Protocol
- COM2 - Protocol
- TS 1 COM user protocol type
- TS 2 COM user protocol type
- TS 3 COM user protocol type
- TS 4 COM user protocol type
- TS 5 COM user protocol type
RipEX.deviceMode
1 ⇒ bridge
2 ⇒ router

RipEX.eDhcp
0 ⇒ off
1 ⇒ server
2 ⇒ client

RipEX.eSpeed
0 ⇒ auto
1 ⇒ s-100baseTX-Full
2 ⇒ s-100baseTX-Half
3 ⇒ s-10baseT-Full
4 ⇒ s-10baseT-Half

RipEX.ifTmATM
0 ⇒ mask
1 ⇒ table

RipEX.IOState
-1 ⇒ unknown
0 ⇒ off
1 ⇒ on

RipEX.RelayContactType
0 ⇒ off
1 ⇒ normally-closed
2 ⇒ normally-open

RipEX.rEncryption
0 ⇒ off
1 ⇒ aes256

RipEX.rRfPwr
0 ⇒ mE-100mW
1 ⇒ mEr-200mW
2 ⇒ mE-500mW
3 ⇒ mE-1W
4 ⇒ mE-2W
5 ⇒ mE-3W
6 ⇒ mE-4W
7 ⇒ mE-5W
RipEX.rRfPwr

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>mE-10W</td>
</tr>
<tr>
<td>9</td>
<td>mE-8W</td>
</tr>
<tr>
<td>17</td>
<td>mL-200W</td>
</tr>
<tr>
<td>18</td>
<td>mL-500mW</td>
</tr>
<tr>
<td>19</td>
<td>mL-1W</td>
</tr>
<tr>
<td>20</td>
<td>mL-2W</td>
</tr>
</tbody>
</table>

RipEX.SettingState

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>1</td>
<td>on</td>
</tr>
</tbody>
</table>

RipEX.tsEthProtType

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>tcp</td>
</tr>
<tr>
<td>1</td>
<td>udp</td>
</tr>
</tbody>
</table>

RFC1213.ifType

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>other</td>
</tr>
<tr>
<td>2</td>
<td>regular1822</td>
</tr>
<tr>
<td>3</td>
<td>hdh1822</td>
</tr>
<tr>
<td>4</td>
<td>ddn-x25</td>
</tr>
<tr>
<td>5</td>
<td>rfc877-x25</td>
</tr>
<tr>
<td>6</td>
<td>ethernet-csmacd</td>
</tr>
<tr>
<td>7</td>
<td>iso88023-csmacd</td>
</tr>
<tr>
<td>8</td>
<td>iso88024-tokenBus</td>
</tr>
<tr>
<td>9</td>
<td>iso88025-tokenRing</td>
</tr>
<tr>
<td>10</td>
<td>iso88026-man</td>
</tr>
<tr>
<td>11</td>
<td>starLan</td>
</tr>
<tr>
<td>12</td>
<td>proteon-10Mbit</td>
</tr>
</tbody>
</table>
Items: RFC1213.ifType
13 ⇒ proteon-80Mbit
14 ⇒ hyperchannel
15 ⇒ fddi
16 ⇒ lapb
17 ⇒ sdlc
18 ⇒ ds1
19 ⇒ e1
20 ⇒ basicISDN
21 ⇒ primaryISDN
22 ⇒ propPointToPointSerial
23 ⇒ ppp
24 ⇒ softwareLoopback
25 ⇒ eon
26 ⇒ ethernet-3Mbit
27 ⇒ nsip
28 ⇒ slip
29 ⇒ ultra
30 ⇒ ds3
31 ⇒ sip
32 ⇒ frame-relay

Items: RFC1213.ipForwarding
1 ⇒ forwarding
2 ⇒ not-forwarding

Items: RFC1213.snmpEnableAuthenTraps
1 ⇒ enabled
2 ⇒ disabled

Items: RS232.rs232AsyncPortParity
1 ⇒ none
2 ⇒ odd
3 ⇒ even
4 ⇒ mark
5 ⇒ space

Items: RS232.rs232AsyncPortStopBits
1 ⇒ one
2 ⇒ two
Note

Two value mappings should already be included in the Zabbix itself, see "SNMP interface status (ifAdminStatus)" and "SNMP interface status (ifOperStatus)" in the Value mapping menu. Four Items from the RFC1213 template use these mappings.

3.4.2. 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: RipEX.eDhpc
Fig. 3.11: Linking a value map to an item
4. How do I Know that Something Has Happened to the RipEX Station?

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

4.1. 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.

![Image](image.png)

Fig. 4.1: Displaying of RipEX issue

4.2. SNMP Traps/Informs

The key aspect of the SNMP are the TRAPS/INFORMS. These OID objects are not actively monitored by the Zabbix manager but by the RipEX itself. This behaviour is described in the on-line help on RipEX web Settings page or in the User manual\(^1\).

4.2.1. How to configure SNMPv2c Traps/Informs 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**
  
  Other approaches could be using SNMPTT functionality.

- **Important**
  
  The following section will explain the SNMPv2c Traps only. The SNMPv3 or SNMP Informs differences and requirements are explained at the end of this section.

---

\(^1\) [https://www.racom.eu/eng/products/m/ripex/h-menu.html\#SNMP](https://www.racom.eu/eng/products/m/ripex/h-menu.html\#SNMP)
You have to install an snmptrapd, a daemon which receives SNMP traps and pass them into the Zabbix front-end. Keep in mind to start it automatically after the system start, e.g. via the command:

```
# systemctl enable snmptrapd
```

You can use the script (`snmptrap.sh`) which is included in the RipEX_Zabbix_templ.zip file downloadable from *Firmware section* on RACOM 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.

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

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

**Note**

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

For a correct snmptrap.sh script functionality, RipEX MIB must be configured in the Zabbix server. First, copy the MIB file `RACOM-RipEX-<version>.mib` to your MIB directory (on CentOS7, it is `/usr/share/snmp/mibs/`). Afterwards, you need to edit the SNMP configuration file (`/etc/snmp/snmp.conf`) with a text editor (e.g. "vim").

```
# vim /etc/snmp/snmp.conf
```

Add the RipEX MIB via the following line and save the changes.

```
mibs +/usr/share/snmp/mibs/RACOM-RipEX-<version>.mib
```

Reboot the Zabbix server. The RipEX OIDs, Value mapping etc. should now be correctly translated and understood.

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

If you have not yet done so, import the RipEX templates. One application is called TRAPS and it consists of all traps. Link the templates 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: RipEX1
SNMP interface: 192.168.10.1, port 161, IP

Along with this template, 16 new items and triggers appear at each used host. That is exactly the number of SNMP traps defined at the RipEX. Each trap should be recognized and the Zabbix should display the correct information message at the dashboard.

Fig. 4.2: Definition of RipEX traps

RipEX 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 or in the OK state.

RSS and DQ trap items are disabled in the template by default. The reason is that we need to define remote RipEX IP addresses first. See the following example for enabling a DQ trap:

Go to the Zabbix web front-end and select a RipEX host for which you want to process DQ traps. Click on the Items button and find an item with the following key: trpDqX.Y.Z.W.
Fig. 4.3: Default DQ trap item

Click on the item and then click on the Clone button. Now you can edit the item. Replace the "X.Y.Z.W" string in the item Name with the remote RipEX radio IP address (e.g. 192.168.131.55). Do the same in the Key field and select the Enabled option in the Status field. See the following example:
How do I Know that Something Has Happened to the RipEX Station?

Save the changes and open the host Triggers list. Repeat the above steps for the DQ trigger and save the changes. You should see the trigger with the enabled status.

Follow the same procedure (DQ and RSS) for other remote RipEX units as needed.
How do I Know that Something Has Happened to the RipEX Station?

You can also define Zabbix to send you an e-mail whenever any trap is triggered. See the Zabbix Documentation or Section *Chapter 7, 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 /bin/bash /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. Note that you should not define this line for security reasons.

```
disableAuthorization yes
```

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.

**Note**

RipEX default Community string name is “public”, however it can be changed (since firmware release 1.3). All RipEX stations within the network must have the same Community string. Otherwise disableAuthorization has to be set to “yes” (or set authCommunity variables for all allowed Community string names).

### 4.2.2. How to Configure SNMPv3 Traps/Informs in Zabbix?

Now, the system is ready to receive SNMPv2c traps and informs (see the previous section). If you configure SNMPv3 in the network, several additional steps are required.

Snmptrapd deamon needs to decrypt the incoming traps/informs. To successfully authenticate itself and decrypt the message, correct Users with correct secrets must be configured in the `/etc/snmp/snmptrapd.conf` file.

In this file, you already have the similar lines:
For SNMPv3 Inform (not traps), you need to create the user via `createUser` command. Stop the snmptrapd daemon:

```
# systemctl stop snmptrapd
```

Now, edit the `/etc/snmp/snmptrapd.conf` file and add this line:

```
createUser racom MD5 "racom1234" DES "racom5678"
```

This command should add the User "racom" with MD5 and DES secrets. Save the changes and run the snmptrapd daemon.

```
# systemctl start snmptrapd
```

Check if the addition was successful via

```
# cat /var/lib/net-snmp/snmptrapd.conf
```

You should see a line similar to the following one:

```
usmUser 1 3 0x80001f8880a9b9e400d6e8b55900000000 "racom" "racom" NULL .1.3.6.1.6.3.10.1.1.3 0x40d2c90a2f4ee04d30eb4e207ale4ab507ce8d1 .1.3.6.1.6.3.10.1.2.2 0x40d2c90a2f4ee04d30eb4e207ale4ab ""
```

Now, the SNMPv3 informs can be successfully received and used.

SNMPv3 Traps need a bit different command. Everything is the same, but the EngineID must be configured. In the RipEX web interface, create the unique EngineID within SNMP configuration page. This value is static and unique. For each RipEX unit, you need to create a separate User in the snmptrap configuration file. Stop the snmptrapd daemon again and add a similar line in the `/etc/snmp/snmptrapd.conf` file:

```
createUser -e 0000831304199430ac1077ab racom MD5 "racom1234" DES "racom5678"
```

This creates a "racom" user the same way as for the Informs, but the EngineID 0000831304199430ac1077ab is fixed and must correspond to that created in the RipEX web interface.

Start the daemon and check the procedure:

```
# cat /var/lib/net-snmp/snmptrapd.conf
```

```
usmUser 1 3 0x000831304199430ac1077ab "racom" "racom" NULL .1.3.6.1.6.3.10.1.1.3 0x3fcdada23b84853de23e8838d96e985d9 .1.3.6.1.6.3.10.1.2.4 0x3fcdada23b84853de23e8838d96e985d9 ""
```

A similar line should be there - check the EngineID parameter. If succesful, Informs and Traps should now be working correctly. If not, try to check all the mentioned steps and verify your procedure.

**Note**

The same procedure must be met for any other SNMPv3 devices and their SNMPv3 traps/informs (not just RipEX).
4.2.3. Basic Trap/Inform Functionality Tests

Now Zabbix is ready to receive SNMP traps/informs from all RipEX stations and enter them into the database properly. In order to test it, force the trap to be sent from any RipEX 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 trpTemp -o "trpTemp, ALARM: ON"
```

The IP address of your RipEX station is 192.168.10.1, key is "trpTemp" and the message for the Zabbix server is "trpTemp, ALARM: ON". The command should trigger the host's "temperature 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/inform would not match the trigger. See more KEY values with their description below:

- `trpRssIPAddress` - Remote station RSS value out of range (Replace the IPAddress with a real remote RipEX IP address)
- `trpDqIPAddress` - Remote station DQ value out of range (Replace the IPAddress with a real remote RipEX IP address)
- `trpTxLost` - TX Lost value out of range
- `trpUcc` - UCC value out of range
- `trpTemp` - Modem temperature value out of range
- `trpRfpwr` - RF power value out of range
- `trpLanPr` - Ethernet RX/TX packet ratio out of range
- `trpCom1Pr` - COM1 RX/TX packet ratio out of range
- `trpCom2Pr` - COM2 RX/TX packet ratio out of range
- `trpHwIn` - HW input in the alarm state
- `trpHotStby` - Modem becomes active in a Hot-Standby mode
- `trpBpath` - Backup path state has changed
- `trpBpathAlt` - Alternative path state has changed
- `trpUnitReady` - Unit ready signal has changed
- `trpNomadOffline` - Nomadic remote device is offline/online (i.e. status of connection to Nomadic base)

If you want to clear the trap/inform alarm, just repeat the same zabbix_sender command, but change the message to contain the word "OFF". E.g. "ALARM OFF".
Fig. 4.6: Zabbix dashboard – Status of units

You can also see Trap's output in Monitoring → Latest Data → TRAPS of your RipEX station → History. The displayed information differs based on the trap received. See the detailed description in the respective Zabbix item.
5. 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. 5.1: Basic map with two RipEX stations

A short example of RipEX station configuration in Maps:

```
{HOSTNAME}
Temp = {{HOSTNAME}:wvTempAvg.last(0)}
RSS = {{HOSTNAME}:wvRemRssAvg[$NEIGHBOUR.1].last(0)}
DQ = {{HOSTNAME}:wvRemDqAvg[$NEIGHBOUR.1].last(0)}
```

**Map element**

<table>
<thead>
<tr>
<th>Type</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>RipEX-239</td>
</tr>
<tr>
<td>Temp</td>
<td>{{HOSTNAME}:wvTempAvg.last(0)}</td>
</tr>
<tr>
<td>RSS</td>
<td>{{HOSTNAME}:wvRemRssAvg[$NEIGHBOUR.1].last(0)}</td>
</tr>
<tr>
<td>DQ</td>
<td>{{HOSTNAME}:wvRemDqAvg[$NEIGHBOUR.1].last(0)}</td>
</tr>
</tbody>
</table>

Fig. 5.2: Definition of RipEX station in maps

Each map can be divided into several sub-maps. It can be useful for various levels of detail. Links can also be added - just select both Hosts and click on the "Add link" button at the top of the Network maps menu.
6. How to Access RipEX GUI from Zabbix

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

Note
This chapter consists of RAy2 screenshots, but the procedure is completely the same for RipEX as well.

6.1. Map URL

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

<table>
<thead>
<tr>
<th>URL Name</th>
<th>URL</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAy2-234 URL</td>
<td><a href="http://10.250.2.234">http://10.250.2.234</a></td>
<td>Remove</td>
</tr>
</tbody>
</table>

Add

Apply  Remove  Close

Fig. 6.1: 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. 6.2: RAy2 URL Link in maps

6.2. 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.
How to Access RipEX GUI from Zabbix

6.3. 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.
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.

![Host inventory]

Fig. 6.6: RAy2 URL link in the Inventory
7. 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).

7.1. 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.

![Media types](image)

Fig. 7.1: E-mail configuration

7.2. 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. 7.2: 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).

7.3. 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. 7.3: 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”.

```plaintext
Trigger: \{TRIGGER.NAME\}
Trigger status: \{TRIGGER.STATUS\}
Trigger severity: \{TRIGGER.SEVERITY\}
Trigger URL: \{TRIGGER.URL\}
```

```plaintext
Item values:
1. \{ITEM.NAME1\} \{ITEM.KEY1\} \{ITEM.VALUE1\}
```

```plaintext
RipEX - SNMP – © RACOM s.r.o.
```
Fig. 7.4: 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.

<table>
<thead>
<tr>
<th>Conditions</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger value = PROBLEM</td>
<td>Remove</td>
</tr>
<tr>
<td>Host = RipEX_TP238</td>
<td>Remove</td>
</tr>
</tbody>
</table>

Fig. 7.5: 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.
Additional steps can be set as required. E.g. one can send e-mail immediately as the Problem occurs, and if the Problem is still active, send the e-mail every additional day (once per 24 hours).
8. RipEX 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 RipEX template, we already prepared several examples:

- Configuration backup
- Displaying the current RSS

Note

If you have troubles running those 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 two scripts. As you know 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 RipEX unit.

8.1. 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.

8.1.1. 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 RipEX units.

Restart the Zabbix server afterwards.

`# systemctl restart zabbix-server`

8.1.2. 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`
There are two executable scripts via the Zabbix web interface (starting with "ripex_"), 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/INFORM 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/*
```

### 8.1.3. 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.

Do not edit the UID and GID, these are created by CentOS automatically and can be different in your installation.

**Note**

You might need to install "util-linux-user" for the "chsh" command.

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
```

**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/ripex
# mkdir /home/zabbix/firmware/ripex
# chown -R zabbix:zabbix /home/zabbix/
```

### 8.1.4. SSH Access to RipEX 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.
A new prompt appears. Because, we cannot access the RipEX 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 RipEX 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 RipEX 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
```

**Note**

You might need to define the key manually with `-i` parameter.

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

### 8.1.5. Scripts in the Zabbix Web Interface

The script files can be downloaded within the template ZIP file. 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 RipEX scripts.

Fig. 8.1: RipEX scripts

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

---

Fig. 8.2: 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 “RipEX”.

The parameters are MACROs which should be enabled by default due to our Template. Each RipEX 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. 8.3: Host MACROs

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

8.1.6. SELinux Restrictions

If the operating system is CentOS and has the SELinux security option enabled, the scripts will not run properly due to these restrictions. Please consult this with your IT department or contact RACOM technical support.

⚠️ Important

Do not rush with SELinux rules.

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

8.1.7. 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. 8.4: Scripts in the Maps

If you click on any of the script, 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.

**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 RSS level. The level (in dBm) 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/ripex directory).

Reading the watched values script is working in a different manner. It is used as an external check Item. If you open the Application called "Watched value via script", you will see 17 readable watched values.

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>.
Revision History

Revision 1.0  2017-11-27
First issue.

Revision 1.1  2018-03-20
Nomadic trap added (RipEX FW 1.8.2.0).

Revision 1.2  2021-01-20
Small changes regarding CentOS8 and Zabbix5.