

# Содержание

|   |    |
|---|----|
| <b>Triggers in QoE</b> .....  | 3  |
| <i>Trigger configuration example: Finding the source of a Flood DDOS attack</i> ..... | 3  |
| <i>Trigger configuration example: Finding the target of a Flood DDOS attack</i> ..... | 9  |
| <i>BotNet Analysis</i> .....  | 10 |
| <i>Subscriber's interest in competitor resources</i> .....                            | 11 |



# Triggers in QoE

Triggers are used to search for data in QoE Stor according to the specified parameters. After the trigger is fired, one of the following actions is possible:

- GUI notification
- HTTP action
- sending email

Required SSG options:

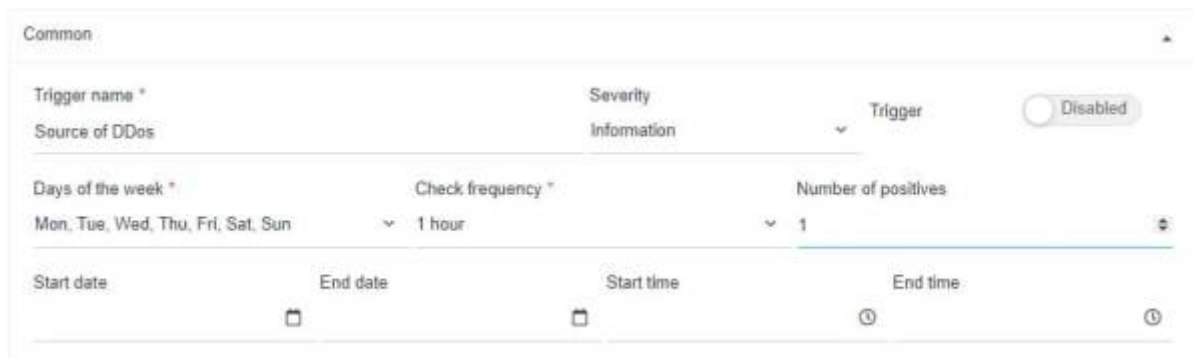
- [Statistics gathering and analysis on protocols and directions](#)
- [Subscriber notifications](#)

Required additional modules:

- [DPIUI2 \(GUI - Graphical User Interface\)](#)
- [QoE Stor \(Statistics collection module\)](#)

## Trigger configuration example: Finding the source of a Flood DDOS attack

### General Information



The screenshot shows a configuration form for a trigger named 'Source of DDos'. The form is titled 'Common' and includes the following fields:

- Trigger name \***: Source of DDos
- Severity**: Information
- Trigger**: Disabled (toggle)
- Days of the week \***: Mon, Tue, Wed, Thu, Fri, Sat, Sun
- Check frequency \***: 1 hour
- Number of positives**: 1
- Start date**: (calendar icon)
- End date**: (calendar icon)
- Start time**: (clock icon)
- End time**: (clock icon)

Trigger name «Source of DDoS», days of week – all, check frequency – every hour, number of positives – once, time and date of start/end - not specified.



Every day, once an hour, a check will be carried out according to the conditions described below.

### Queries

| Queries                                |            |        |  |                 |           |  |
|--|------------|--------|--|-----------------|-----------|--|
| +                                      |            |        |  |                 |           |  |
|  | Query name | Report |  | Period from     | Period to |  |
| <input checked="" type="checkbox"/> On | A          | Maxi   |  | now - 15 minute | now       |  |

- Add a field
- Name: A
- Choose a table to be scanned: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Set the period from: «now - 15minute», until : «now»



In this case, the traffic analysis for the selected page will be carried out for the period of the last 15 minutes.

## Conditions

| Conditions                             |      |            |          |            |                  |          |       |
|--|------|------------|----------|------------|------------------|----------|-------|
| +                                      |      |            |          |            |                  |          |       |
|  | Bind | Query name | Function | Combinator | Serie            | Operator | Value |
| <input checked="" type="checkbox"/> On | AND  | A          | avg      |            | Session lifetime | <=       | 20    |
| <input checked="" type="checkbox"/> On | AND  | A          | avg      |            | Sessions         | >=       | 1500  |

- Add "+" 2 fields
- Bind - AND
- Function - avg
- Serie in the 1 field - session timeout <= 20(ms)
- Serie in the 2 field - number of sessions >= 1500



We have set a condition — the trigger will fire when it detects both signs: sessions with lifetime equal or less than 20ms AND more than 1500 sessions from one IP-host.

## Error handling

| No data & error handling |                                 |
|--------------------------|---------------------------------|
| If no data *             | If execution error or timeout * |
| No data                  | Keep last state                 |

- In the field "If no data" — No data

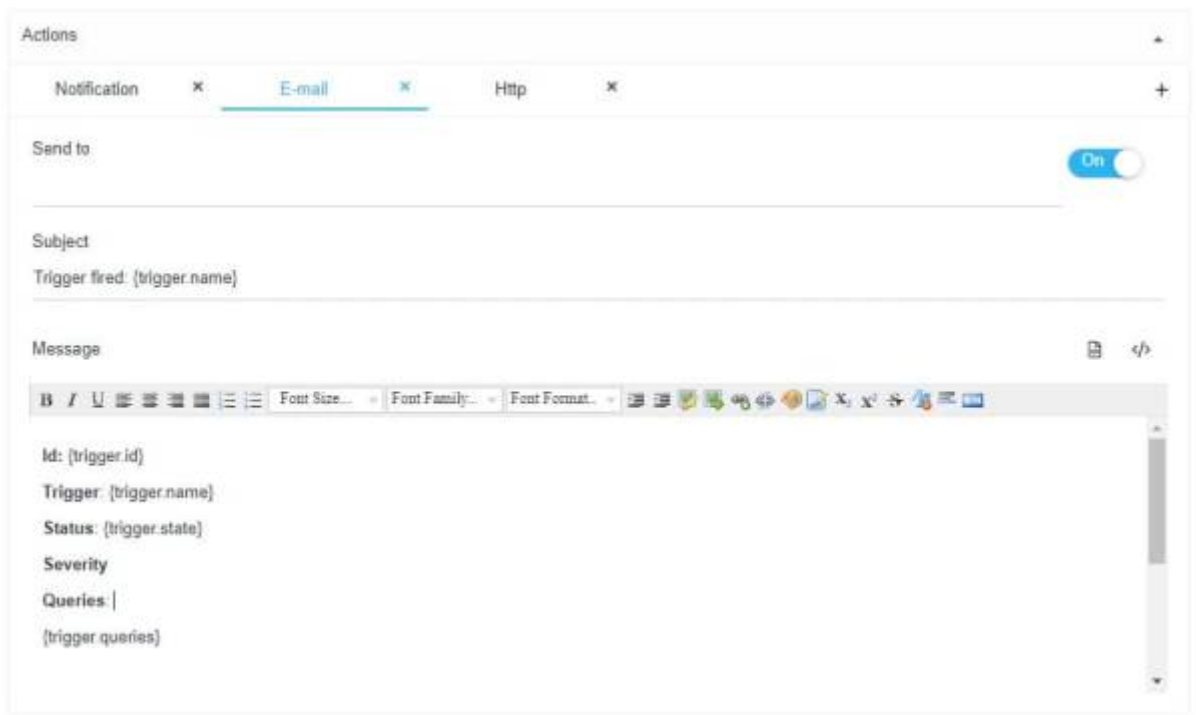
- In the field "If execution error or timeout" — Keep last state



In this configuration — if there are no errors, no data will be saved; if any, information will be saved in the form of a table containing suspicious sessions.

## Actions

### E-mail

A screenshot of a web interface for configuring an "E-mail" action. The interface has a tabbed view with "Notification", "E-mail", and "Http" tabs. The "E-mail" tab is active. It includes a "Send to" field with a blue "On" toggle switch to its right. Below is a "Subject" field containing the text "Trigger fired: {trigger.name}". The "Message" field is a rich text editor with a toolbar and contains the following text: "Id: {trigger.id}", "Trigger: {trigger.name}", "Status: {trigger.state}", "Severity", "Queries |", and "{trigger.queries}".

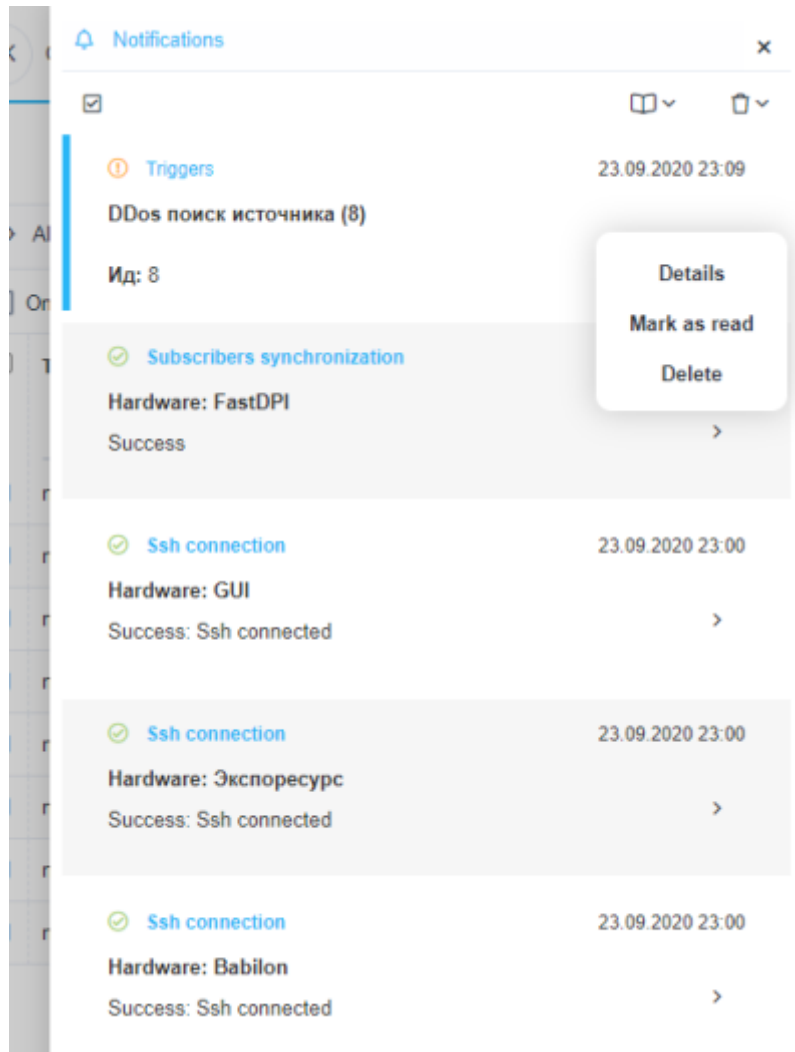
- For automatic filling - click on the "</>" icon (automatic filling of the form)
- In the field "Send to" — specify email address



With this setting, when the trigger is fired, all information about the event will be sent to the specified email: ID, trigger name, status, link to the report (saved state).

### Notification





Select notification  
Select - "Details"

Notifications x

---

← Triggers

---

|                   |   |
|-------------------|---|
| Status            | Read  |
| Notification date | 23.09.2020 23:09                              |
| Notify type       | <span style="color: orange;">ⓘ</span> Warning |

---

Notification content

---

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostsIpsWidget

Причины возникновения нотификации:

avg(avg\_ses\_lifetime) <= 200000 is true in query A  
avg(sessions\_uniq) >= 1 is true in query A

Ссылки на отчеты:

A: [https://192.168.88.11/#QoEAnyReport/report\\_id=rMeFuKSp316vU1b](https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b)

Follow the link to the report - it will open in a new tab.

**HTTP**



Actions

Notification × E-mail × Http × +

Method: POST    Url: https://your\_redmine\_host/issues.xml?key=your\_redmine\_api\_key    On

Headers <    Body >

| Name         | Value           |  |
|--------------|-----------------|--|
| Content-Type | application/xml |  |

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Сработал триггер: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Ид: {trigger.id}
  Триггер: {trigger.name}
  Статус: {trigger.state}
  Важность: {trigger.severity}

  Запросы:
  {trigger.queries}
</issue>
```

REDMINE JSON  
REDMINE XML

- For automatic filling - click on the "</>" icon (automatic filling of the form)
- Choose the method most suitable for your ticket system and enter the URL



It is important to understand: the number of established sessions, the number of incoming packets, etc. are averaged. More precise configuration should be made taking into account the specifics of your network.

## Trigger configuration example: Finding the target of a Flood DDOS attack

It differs from the previous example in setting 2 and 3 stages (Queries and Conditions).

### Queries

In the "Report" field choose Raw full netflow → Tables → Attacks detection → Top subscribers → Maxi

### Conditions

| Bind | Query name | Function | Combinator | Serie                      | Operator | Value |
|------|------------|----------|------------|----------------------------|----------|-------|
| AND  | A          | avg      |            | Flow volume to subscribers | >=       | 10000 |

Serie — "Flow volume to subscribers", >= 10000



It is important to understand: the number of established sessions, the number of incoming packets, etc. are averaged. More precise configuration should be made taking into account the specifics of your network.

## BotNet Analysis

It differs from the previous example in setting 2 and 3 stages (Queries and Conditions).

### Queries

| Queries                                |            |              |  |                 |           |  |  |
|--|------------|--------------|--|-----------------|-----------|--|--|
| +                                      |            |              |  |                 |           |  |  |
|  | Query name | Report       |  | Period from     | Period to |  |  |
| <input checked="" type="checkbox"/> On | A          | Maxi         |  | now - 15 minute | now       |  |  |
| <input checked="" type="checkbox"/> On | B          | Full raw log |  | now - 15 minute | now       |  |  |

- Choose Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi for the "A" value
- Raw full network → Tables → Raw log → Full raw log for the "B" value

## Conditions

| Conditions                             |      |            |          |            |                  |          |       |
|--|------|------------|----------|------------|------------------|----------|-------|
| +                                      |      |            |          |            |                  |          |       |
|  | Bind | Query name | Function | Combinator | Serie            | Operator | Value |
| <input checked="" type="checkbox"/> On | OR   | B          | avg      |            | Destination port | =        | 6667  |
| <input checked="" type="checkbox"/> On | OR   | B          | avg      |            | Source port      | =        | 6667  |
| <input checked="" type="checkbox"/> On | OR   | B          | avg      |            | Destination port | =        | 1080  |
| <input checked="" type="checkbox"/> On | OR   | B          | avg      |            | Source port      | =        | 1080  |
| <input checked="" type="checkbox"/> On | AND  | A          | avg      |            | Flow, Pkts/s     | >=       | 2000  |

Most often, BotNet uses ports 6667 and 1080 — add each destination/source port by selecting query "B" with value "OR" and choose Flow Pcts/s equal or more than 2000.



With this configuration, if at least on one of the ports (6667/1080) the number of passing packets is more than 2000 per second, the trigger will fire.



It is important to understand: the number of established sessions, the number of incoming packets, etc. are averaged. More precise configuration should be made taking into account the specifics of your network.

## Subscriber's interest in competitor resources

### General information

Trigger name «Subscriber's interest in competitor resources», days of week - all, check frequency - every hour, number of positives - once, time and date of start/end - not specified.



Every day, once an hour, a check will be carried out according to the conditions described below.

## Queries

| Queries                             |            |                 |   |              |           |    |
|-------------------------------------|------------|-----------------|---|--------------|-----------|----|
| +                                   |            |                 |   |              |           |    |
|                                     | Query name | Report          |   | Period from  | Period to |    |
| <input checked="" type="checkbox"/> | On A       | Raw clickstream | ▼ | now - 1 hour | now       | 🗑️ |
| <input checked="" type="checkbox"/> | On B       | Maxi            | ▼ | now - 1 hour | now       | 🗑️ |

- Add "+" field
- Name A  
Choose a table to be scanned: Raw clickstream → Tables → Raw clickstream
- Name B  
Choose a table to be scanned: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Set the period from: "now - 1 hour", until : "now"



In this case, the traffic analysis for the selected tables will be carried out every hour.

## Conditions

| Conditions                             |      |            |          |            |                 |          |             |  |
|--|------|------------|----------|------------|-----------------|----------|-------------|--|
| +                                      |      |            |          |            |                 |          |             |  |
|  | Bind | Query name | Function | Combinator | Serie           | Operator | Value       |  |
| <input checked="" type="checkbox"/> On | OR   | A          | avg      |            | Host            | =        | *megafon.ru |  |
| <input checked="" type="checkbox"/> On | AND  | B          | avg      |            | Flow volume fro | >=       | 800         |  |
| <input checked="" type="checkbox"/> On | OR   | A          | avg      |            | Host            | =        | *mts.ru     |  |

- Add "+" 3 fields
- First field — choose table "A"; Bind - "OR"; Function - "avg"; Serie Host = \*megafon.com (or any other competitor ISP)
- Second field — choose table "B"; Bind "AND"; Function - "avg"; Serie Flow volume from subscriber, Pct/s >= 800



We have set a condition — the trigger will fire at least 800 packets (not an accidental but meaningful visits) from a subscriber to a competitor's site.

## Error handling

| No data & error handling |                                 |
|--------------------------|---------------------------------|
| If no data *             | If execution error or timeout * |
| No data                  | Keep last state                 |

- In the field "If no data" — No data
- In the field "If execution error or timeout" — Keep last state



In this configuration — if there are no errors, no data will be saved; if any, information will be saved in the form of a table containing suspicious sessions.

## Actions

### E-mail

- For automatic filling - click on the "</>" icon (automatic filling of the form)
- In the field "Send to" — specify email address



With this setting, when the trigger is fired, all information about the event will be sent to the specified email: ID, trigger name, status, link to the report (saved state).

## Notification

- For automatic filling - click on the "</>" icon (automatic filling of the form)

- Choose the notification type — "Warning"
- With this setting, a notification will be created in the SSG

| Alerts                 |          |                  |                   |  | Alerts actions              |                     |          |  |
|------------------------|----------|------------------|-------------------|--|-----------------------------|---------------------|----------|--|
| Only selected triggers |          |                  |                   |  | Only selected notifications |                     |          |  |
| Trigger name           | Type     | Date             | Note              |  | Type                        | Date                | State    |  |
| Ddos                   | Alerting | 14.08.2020 13:58 | avg(flow_vol_to_s |  | notification                | 14.08.2020 13:59:03 | Complete |  |
| DDos поиск исто-       | Alerting | 14.08.2020 13:58 | avg(avg_ses_lifet |  | notification                | 14.08.2020 13:58:23 | Complete |  |
| Ddos                   | Alerting | 14.08.2020 13:56 | avg(flow_vol_to_s |  | notification                | 14.08.2020 13:56:43 | Complete |  |
| DDos поиск исто-       | Alerting | 14.08.2020 13:55 | avg(avg_ses_lifet |  | notification                | 14.08.2020 13:56:05 | Complete |  |
| Ddos                   | Alerting | 14.08.2020 13:54 | avg(flow_vol_to_s |  | notification                | 14.08.2020 13:54:23 | Complete |  |
| Ddos                   | Alerting | 14.08.2020 13:52 | avg(flow_vol_to_s |  | notification                | 14.08.2020 13:52:22 | Complete |  |
| DDos поиск исто-       | Ok       | 14.08.2020 13:51 | avg(avg_ses_lifet |  | notification                | 14.08.2020 13:50:25 | Complete |  |
| Ddos                   | Alerting | 14.08.2020 13:50 | avg(flow_vol_to_s |  |                             |                     |          |  |

You can get a link to the report in the notification menu

**Notifications**

**Triggers** 23.09.2020 23:09

DDos поиск источника (8)

Ид: 8

**Subscribers synchronization**

Hardware: FastDPI

Success

**Ssh connection** 23.09.2020 23:00

Hardware: GUI

Success: Ssh connected

**Ssh connection** 23.09.2020 23:00

Hardware: Экспересурс

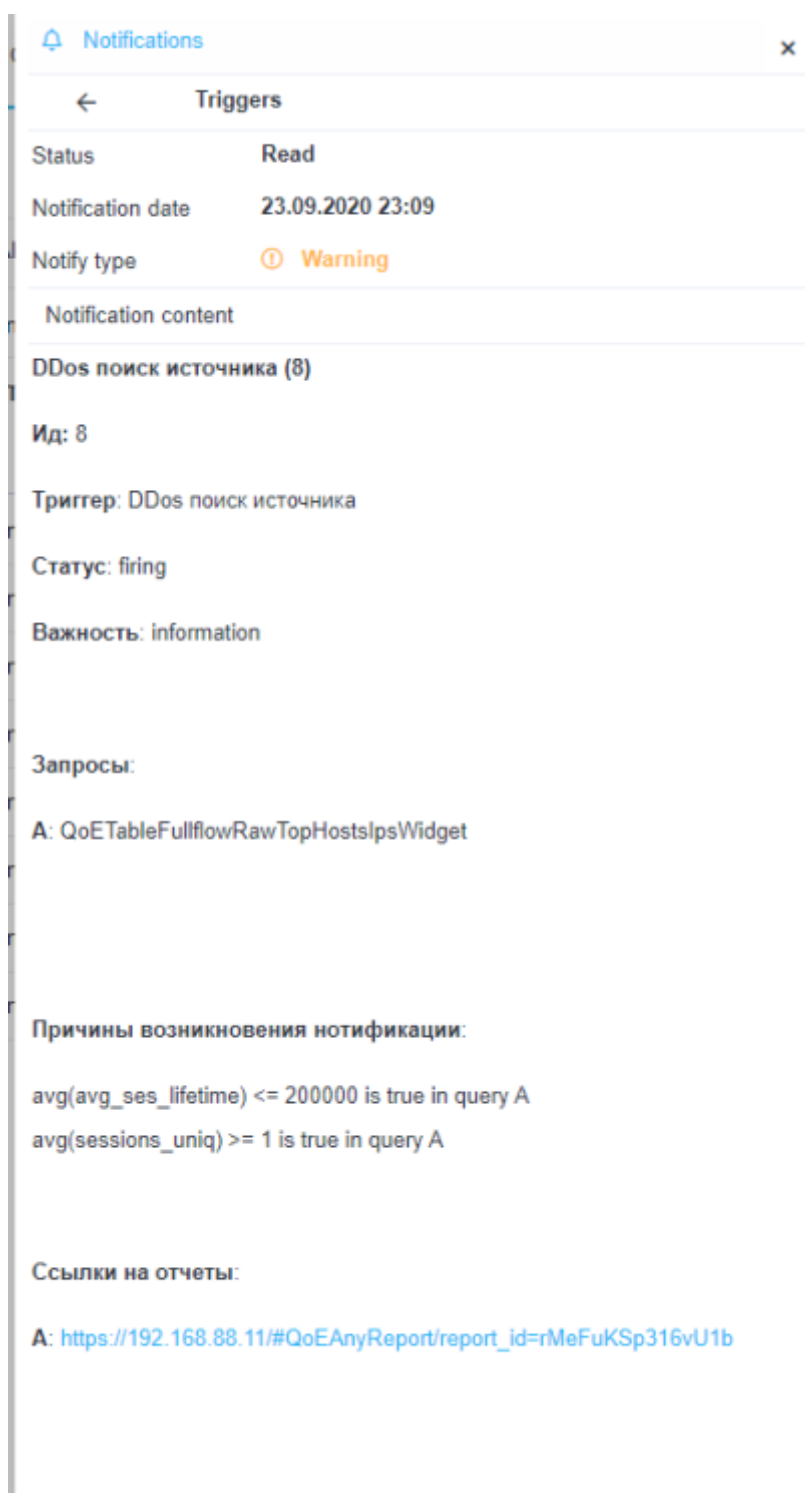
Success: Ssh connected

**Ssh connection** 23.09.2020 23:00

Hardware: Babilon

Success: Ssh connected

Select notification  
Select — "Details"



The screenshot shows a notification details page. At the top, there is a header with a bell icon, the word "Notifications", and a close button (x). Below this is a sub-header with a back arrow and the word "Triggers". The main content area is divided into several sections:

- Status:** Read
- Notification date:** 23.09.2020 23:09
- Notify type:** Warning (indicated by an orange warning icon)
- Notification content:**
  - DDos поиск источника (8)**
  - Ид:** 8
  - Триггер:** DDoS поиск источника
  - Статус:** firing
  - Важность:** information
  - Запросы:**
    - A:** QoETableFullflowRawTopHostsIpsWidget
  - Причины возникновения нотификации:**
    - avg(avg\_ses\_lifetime) <= 200000 is true in query A
    - avg(sessions\_uniq) >= 1 is true in query A
  - Ссылки на отчеты:**
    - A:** [https://192.168.88.11/#QoEAnyReport/report\\_id=rMeFuKSp316vU1b](https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b)

Follow the link to the report — it will open in a new tab.

**HTTP**



Actions

Notification × E-mail × Http × +

Method POST Url  On  
 https://your\_redmine\_host/issues.xml?key=your\_redmine\_api\_key

Headers < Body >

| Name         | Value           |  |
|--------------|-----------------|--|
| Content-Type | application/xml |  |

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Сработал триггер: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Ид: {trigger.id}
  Триггер: {trigger.name}
  Статус: {trigger.state}
  Важность: {trigger.severity}

  Запросы:
  {trigger.queries}
</issue>
```

REDMINE JSON  
REDMINE XML

- For automatic filling — click on the "</>" icon (automatic filling of the form)
- Choose the method most suitable for your ticket system and enter the URL



It is important to understand: the number of established sessions, the number of incoming packets, etc. are averaged. More precise configuration should be made taking into account the specifics of your network.