

Содержание

| | |
|----------------|---|
| Триггеры | 3 |
|----------------|---|

Триггеры

Для автоматизации работы с отчетами, используется меню «Триггеры и Нотификация». Инструмент может быть тонко настроен под автоматическое информирование о событиях, связанных с изменением метрики любых состояний фиксируемых в базе данных на основании потоков Clickstream и Netflow.

Создание нового триггера происходит в 5 этапов:

1. Задать общую информацию триггера:

Название (любое уникальное)

Важность (выбор степень важности: информация, предупреждение, средняя/высокая важность)

Дни недели (задать, в какие дни триггер будет работать)

Частота проверки (таймаут между проверками после срабатывания триггера в минутах)

Количество срабатываний перед нотификацией (сколько раз событие должно повториться)

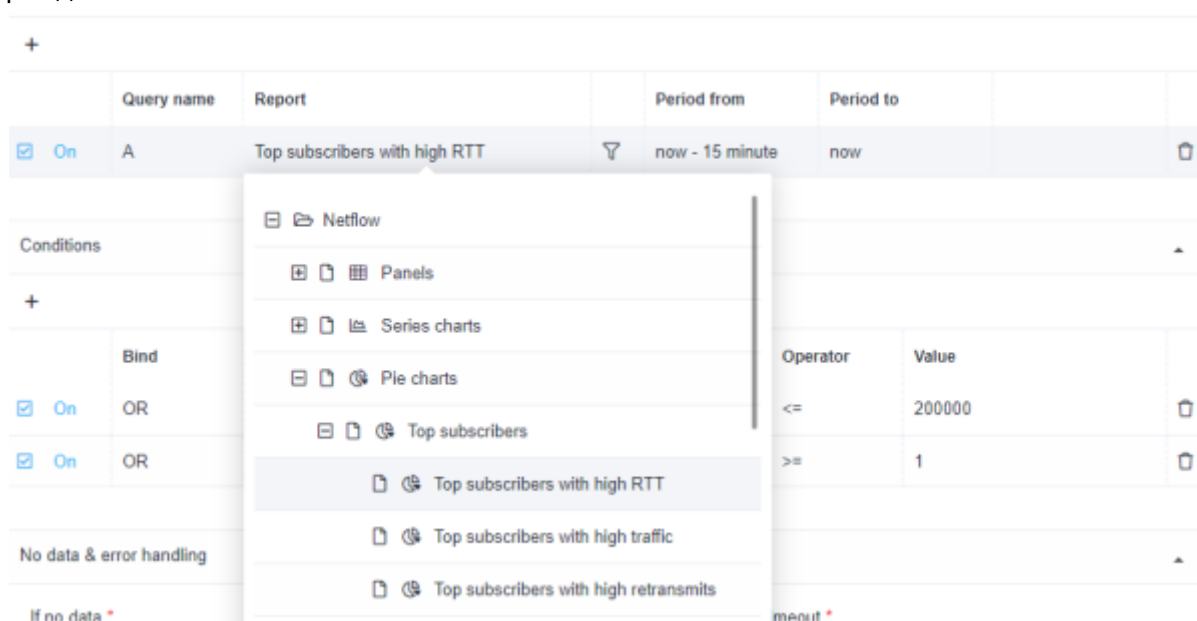
Дата начала/окончания работы триггера

Время начала/окончания работы триггера.

2. Запросы — в этом поле мы выбираем, какую метрику и из какой таблицы сканировать:

Отчет (выбираем из таблиц: Netflow, Clickstream, сырой полный Netflow, сырой полный Clickstream; искомое значение)

Период с/по



3. Условия — что с метрикой должно произойти для срабатывания триггера:

Связь (и/или — сопоставить с названиями запросов на предмет выполнения сразу нескольких условий, или хотя бы одного из заданных)

Название (выбрать один из созданных запросов)

Комбинатор (не/числовое, не/буквенное, нулевое значение)

Оператор (выбрать: =, !=, >, >=, <, <=, between, not between.)

Значение (присвоить уникальное значение)

Common

Trigger name * Severity Information Trigger Disabled
 DDos find who

Days of the week * Check frequency * Number of positives
 Mon, Tue, Wed, Thu, Fri, Sat, Sun 1 minute 0

Start date End date Start time End time

Queries

+

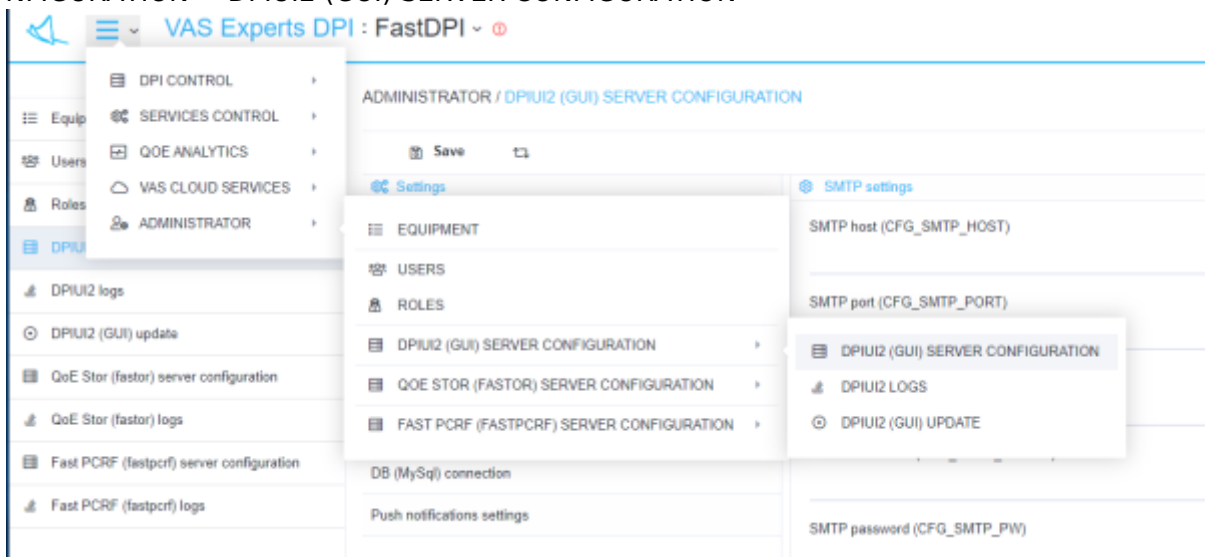
| | Query name | Report | | Period from | Period to | |
|--|------------|-------------------------------|--------------------------|-----------------|-----------|--------------------------|
| <input checked="" type="checkbox"/> On | A | Top subscribers with high RTT | <input type="checkbox"/> | now - 15 minute | now | <input type="checkbox"/> |

Conditions

+

| | Bind | Query name | Function | Combinator | Serie | Operator | Value | |
|--|------|------------|----------|------------|------------------|----------|--------|--------------------------|
| <input checked="" type="checkbox"/> On | OR | A | avg | | Session lifetime | <= | 200000 | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> On | OR | A | avg | | Sessions | >= | 1 | <input type="checkbox"/> |

4. Обработка ошибок. В полях «Если нет данных», «Если есть ошибка или таймаут» присвоить значение: создать нотификацию, сохранить последнее состояние, ок.
5. Действия. Создать E-Mail/HTTP действие, нотификацию:
 E-Mail действие — создает уведомление и посылает его на выбранный адрес электронной почты (автоматическое письмо о событии можно редактировать).
 Для настройки SMTP: перейти MAIN MENU → ADMINISTRATOR → DPIUI2 (GUI) SERVER CONFIGURATION → DPIUI2 (GUI) SERVER CONFIGURATION



Перейти в раздел настройки SMTP: SMTP SETTINGS

The screenshot shows the 'SMTP settings' configuration page. On the left is a sidebar with a 'Save' button and a list of settings categories: Settings, Common, Jobs intervals and periods, QoEStor DB (Clickhouse) connection, QoEStor DB lifetime settings, SMTP settings (selected), System, DB (MySQL) connection, and Push notifications settings. The main area is titled 'SMTP settings' and contains the following fields:

- SMTP host (CFG_SMTP_HOST)
- SMTP port (CFG_SMTP_PORT): 587
- SMTP encryption type (CFG_SMTP_SECURE): tls
- SMTP username (CFG_SMTP_UNAME)
- SMTP password (CFG_SMTP_PW)
- Sender (CFG_SMTP_FROM)
- Tech. support email (CFG_SEND_ERROR_EMAIL): sd@vas.expert
- Send copy to (CFG_SEND_COPY_EMAIL)

HTTP действие — создает уведомление и отправляет его в выбранную ticket-систему (автоматическое уведомление о событии можно редактировать)

The screenshot shows the 'Actions' configuration dialog for an HTTP action. The 'Http' tab is active. The configuration is as follows:

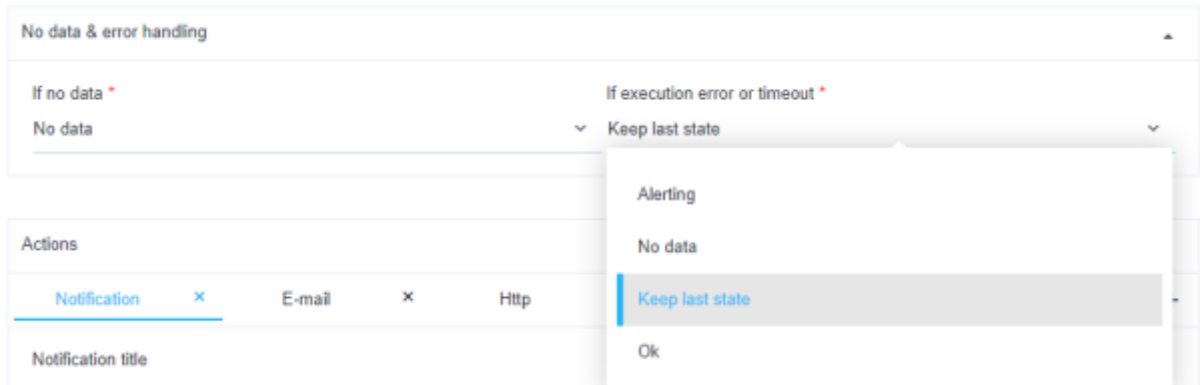
- Method:** POST
- Url:** `https://your_redmine_host/issues.xml?key=your_redmine_api_key`
- Headers:** Content-Type: application/xml
- Body:**

```
<?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}
  ...
```

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Нотификация — создает нотификацию в DPIUI (автоматическое уведомление о событии можно редактировать)



После создания триггера, нажать «Сохранить». В окне «Триггеры и нотификация» включить необходимые триггеры. Если страница DPIUI2 не обновлялась — обновить или нажать на иконку refresh, аналогично с меню действий.

QOE ANALYTICS / TRIGGERS & ALERTS Subscription status: REMAINS 500 DAYS

| Triggers | | | | | | Alerts | | | | Alerts actions | | |
|------------|---------------|------------|--------------|-------|--|-------------------|----------|------------------|-------------------|----------------|---------------------|----------|
| Trigger | Days of | Check | Trigger type | State | | Trigger name | Type | Date | Note | Type | Date | State |
| DDos scan | Mon, Tue, ... | 1 minute | Custom | Ready | | Ddos | Alerting | 14.08.2020 13:50 | avgflow_vol_to_s | notification | 14.08.2020 13:59:03 | Complete |
| Ddos | Mon, Tue, ... | 1 minute | Custom | Ready | | DDos noise action | Alerting | 14.08.2020 13:50 | avg(ang_ses_flow) | notification | 14.08.2020 13:50:23 | Complete |
| ssh-brute! | Mon, Tue, ... | 10 minutes | System | Ready | | DDos noise action | Alerting | 14.08.2020 13:55 | avgflow_vol_to_s | notification | 14.08.2020 13:55:43 | Complete |
| | | | | | | DDos noise action | Alerting | 14.08.2020 13:55 | avg(ang_ses_flow) | notification | 14.08.2020 13:56:05 | Complete |
| | | | | | | Ddos | Alerting | 14.08.2020 13:54 | avgflow_vol_to_s | notification | 14.08.2020 13:54:25 | Complete |
| | | | | | | Ddos | Alerting | 14.08.2020 13:52 | avgflow_vol_to_s | notification | 14.08.2020 13:52:22 | Complete |
| | | | | | | DDos noise action | Alerting | 14.08.2020 13:51 | avg(ang_ses_flow) | notification | 14.08.2020 13:50:25 | Complete |
| | | | | | | Ddos | Alerting | 14.08.2020 13:50 | avgflow_vol_to_s | | | |