Содержание

QoE Триггеры и Нотификация

[GUI v.2.32.70+]
В отчетах, формируемых в данном разделе GUI, улучшены название и обозначение таблиц, названия столбцов таблиц.

Назначение

В разделе "Триггеры и Нотификация" Вы сможете настроить отправку периодических отчетов и оперативных алертов в Telegram или на E-mail с отображением их в самом GUI. При срабатывании триггера будет приходить сообщение с информацией о заданном событии и ссылками на соответствующие отчеты. По умолчанию это 4 отчета в форматах csv, tsv, xlsx, pdf, но шаблон сообщения можно редактировать.

Для работы раздела "Триггеры и Нотификация" требуется активация подписки — лицензия Standard для GUI.

Сделаем настройки на примере двух сценариев:

1. **Периодический отчет для отслеживания задержки RTT от абонента.**
   В отчете будут отображаться абоненты, у которых значение "RTT от абонента" больше либо равно 150000 мс. Он будет приходить по понедельникам и четвергам **в Telegram**.
2. **Алерт об абонентах-участниках ботнета.**
   Настроим проверку таблицы раз в минуту каждый день. **На почту** будет приходить нотификация как только в таблице будет замечен хотя бы один зараженный абонент.

Создание и настройка триггеров

1. В GUI перейти в раздел QoE аналитика → Триггеры и Нотификация.
2. Нажать на **+** на дашборде "Триггеры" для добавления триггера. Откроется окно настройки.

Создание нового триггера происходит в 5 шагов. Настройки триггеров разделены на блоки, необходимо заполнить все из них.

Шаг 1. Расписание работы

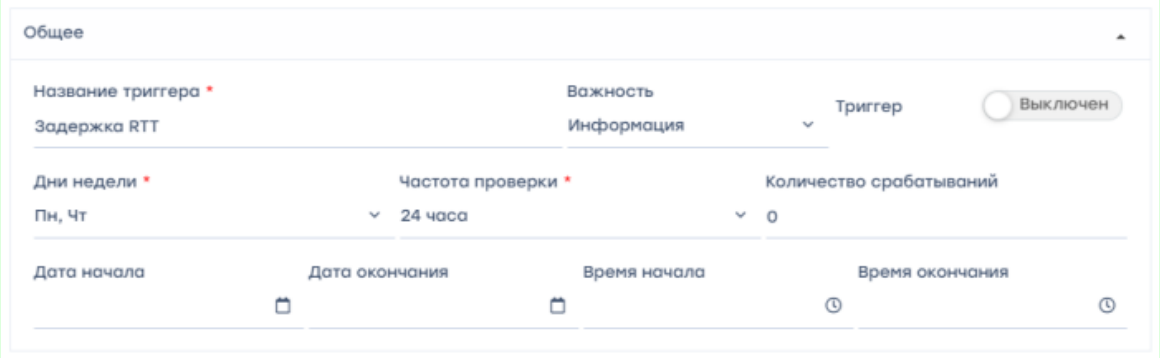
Заполните обязательные поля:

- Название — любое уникальное имя для триггера.
- Важность — выбор степени важности: информация, предупреждение, средняя/высокая

важность. Например, степень "Информация" можно задать для отчета, а все остальные — разным нотификациям по вашему усмотрению. **Необязательное поле.**
- Дни недели проверки — в какие дни недели будет работать триггер.
- Частота проверки — как часто будет запускаться скрипт проверки. Например, если выставлено значение "1 минута" — скрипт проверки будет запускаться в заданные дни недели раз в минуту.
- Дату и время начала и окончания работы триггера. **Необязательные поля.**

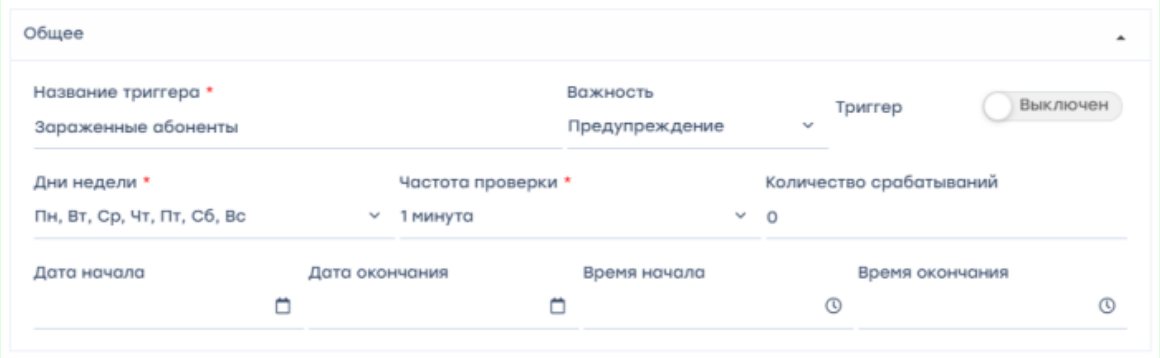
Также в этом блоке расположен переключатель для включения/выключения триггера, **после окончания настройки не забудьте его включить.**

Пример заполнения блока для отчета для отслеживания задержки RTT от абонента:



В этом случае скрипт проверки будет запускаться по заданным дням раз в 24 часа — один раз в понедельник и один раз в четверг.

Пример заполнения блока для нотификации об абонентах с киберугрозами:

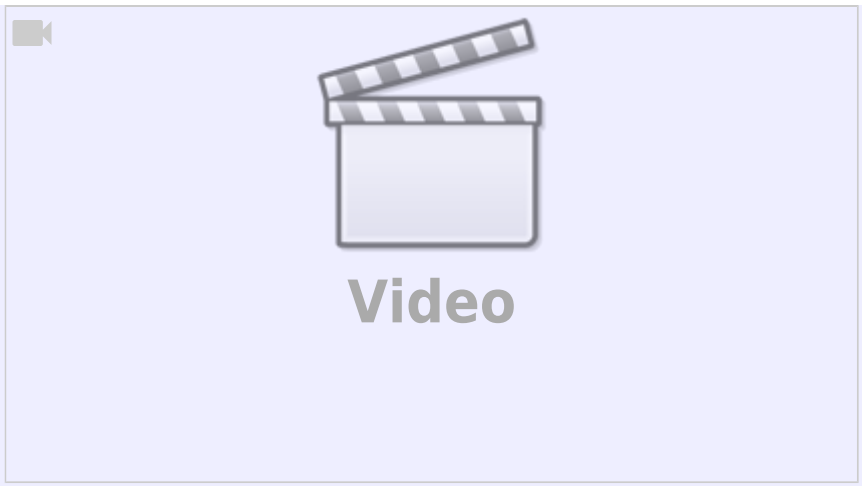


В этом случае скрипт проверки будет запускаться раз в минуту каждый день, то есть работать постоянно.

Шаг 2. Выбор источника данных и метрики

Выбрать метрику и таблицу данных. Триггеры работают только с готовыми таблицами, которые находятся в разделах "Нетфлоу" и "Кликстрим", для начала настройки нужно найти таблицу, где есть необходимая метрика.

Подсказка к выбору таблицы в видео:

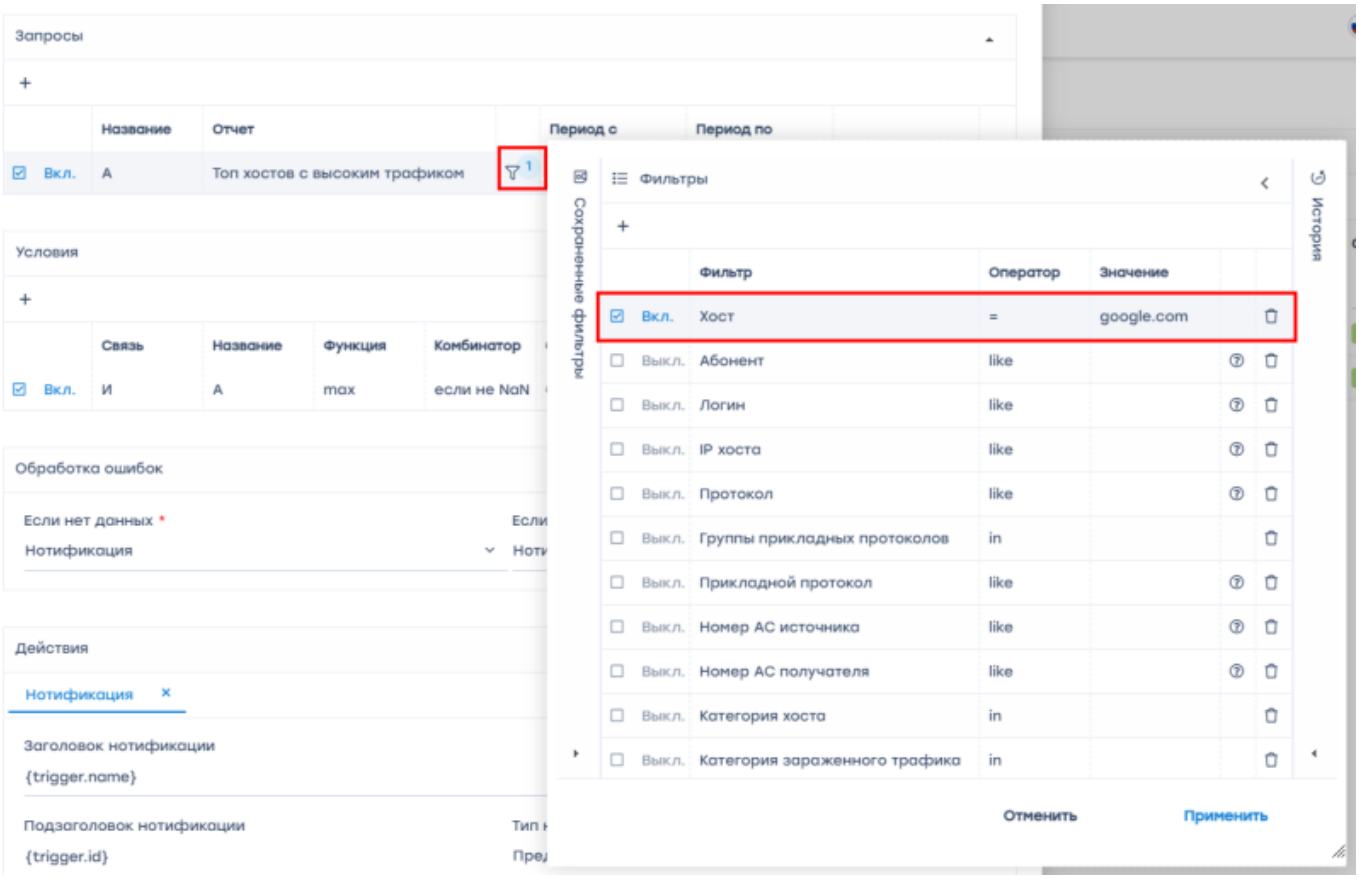


Для создания запроса нажать на **+** под названием блока.

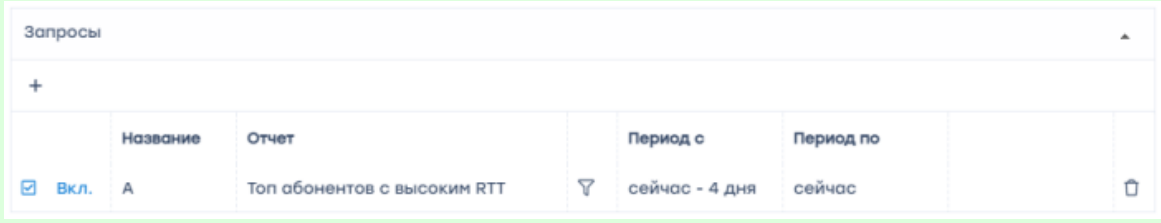
- Отчет — выбор таблицы с данными из готовых отчетов системы, по которым производится поиск.
- "Период с" и "-по". Например, если нужно анализировать данные за последние сутки, задайте "Период с" — 24 часа, "Период по" — сейчас.

"Сейчас" в периоде с/по в запросе означает момент запуска триггера. Он складывается из дней недели работы триггера и верхней границы частоты проверки (из блока настроек "Общее").

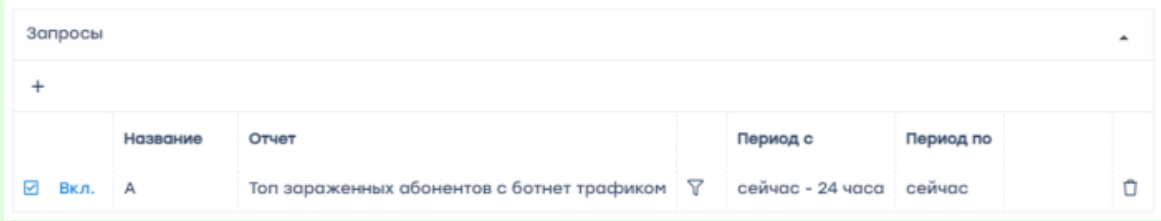
Для каждого запроса можно создать фильтр, где можно задать значение IP хоста, логина абонента и т.д. Например, можно настроить формирование отчета или нотификации по одному конкретному хосту, если задать такой фильтр:



Пример заполнения блока для отчета для отслеживания задержки RTT от абонента. Здесь нужно выбрать отчет "Топ абонентов с высоким RTT", в нем есть нужные метрики для данного триггера. Так как нужно, чтобы отчет приходил по понедельникам и четвергам, "Период с" выставить равным промежутку между этими днями — "Сейчас - 4 дня", будут анализироваться данные за последние 4 дня.



Пример заполнения блока для нотификации об абонентах с киберугрозами. Здесь нужно выбрать отчет "Топ зараженных абонентов с ботнет трафиком", в нем есть нужные метрики для данного триггера. В данном случае будут анализироваться данные за последние 24 часа.

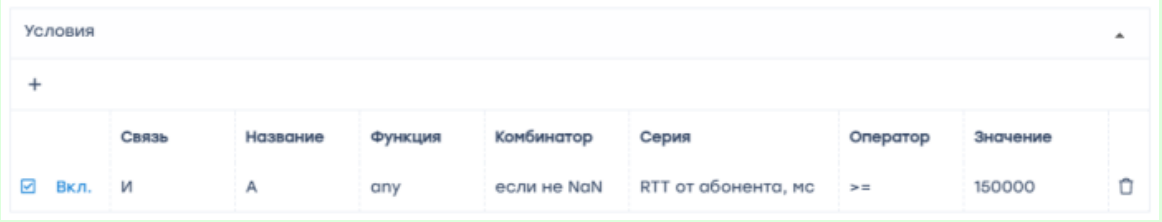


Шаг 3. Условия

Задать условия — что должно произойти с метрикой для срабатывания триггера.
Для создания условия нажать на **+** под названием блока.
Для каждого условия нужно настроить следующие параметры:

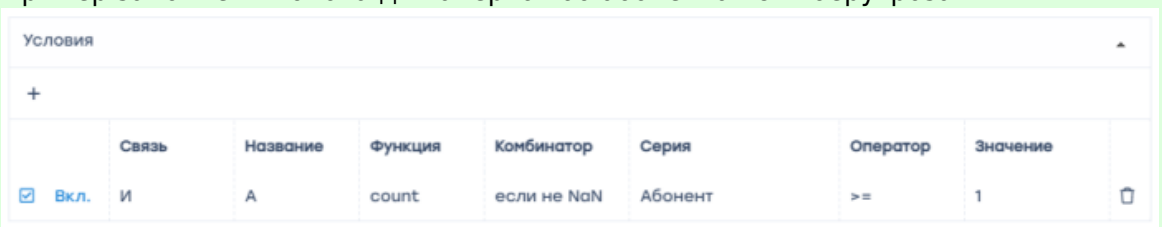
- Связь И/ИЛИ — сопоставить с названиями запросов на предмет выполнения либо сразу нескольких условий, либо хотя бы одного из заданных.
- Название — выбрать один из созданных запросов.
- Функция — выбрать тип агрегатной функции, которая будет применена к значениям в условии:
  - "count" считает количество элементов или записей в наборе данных,
  - "any" возвращает любое значение из доступных в наборе данных,
  - "anyLast" возвращает последнее значение из доступных в наборе данных,
  - "avg" вычисляет среднее значение числовых данных в наборе,
  - "min" возвращает минимальное значение из доступных в наборе данных,
  - "max" возвращает максимальное значение из доступных в наборе данных,
  - "sum" вычисляет сумму числовых данных в наборе,
  - "uniq" возвращает уникальные значения в наборе данных, удаляя дубликаты.
- Комбинатор — выбрать нечисловое/ненулевое/числовое/нулевое значение или оставить пустым.
- Серия — выбрать нужную метрику из отчета.
- Оператор — выбрать: =, !=, >, >=, <, <=, between *(будет возвращать записи, где выражение находится в диапазоне значений value1 и value2 включительно)*, not between *(возвращает все записи, где выражение НЕ находится в диапазоне между value1 и value2 включительно)*.
- Значение — присвоить необходимое значение для условия.

Пример заполнения блока для отчета для отслеживания задержки RTT от абонента:



В этом случае триггер будет срабатывать, если в таблице из шага 2 появится значение RTT от абонента больше либо равное 150000 мс.

Пример заполнения блока для алертов об абонентах с киберугрозами:



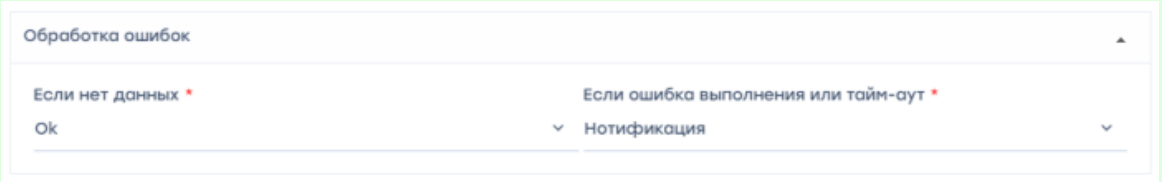
В этом случае триггер будет срабатывать, если в таблице из шага 2 будет хотя бы один абонент.

Шаг 4. Обработка ошибок

Задать поведение триггера при ошибках.
В полях "Если нет данных" и "Если есть ошибка выполнения или тайм-аут" выбрать одно из значений:

- "Нотификация" — условие, заданное в триггере, выполнено.
- "Нет данных" — при обработке отчетов, заданных в триггере, не найдено данных.
- "Сохранить последнее состояние" — не нужно предпринимать никаких действий.
- "Ок" — условия, заданные в триггере, не сработали, все в порядке и никаких действий выполнять не нужно.

Пример заполнения блока для отчета и для алертов:



В обоих случаях если нет данных — триггер не будет срабатывать и сообщение не будет приходить, если возникла ошибка или тайм-аут — будет приходить нотификация.

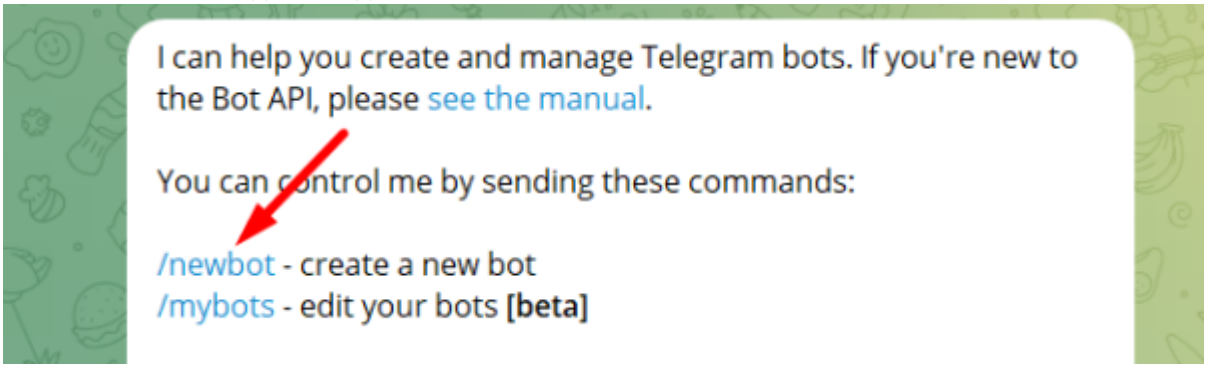
Шаг 5. Действия

Настройка действия позволит в случае срабатывания триггера получать сообщение на E-mail или в Telegram.
Для создания действия нажать на **+** под названием блока.
Для удаления действия нажать на × напротив названия действия.

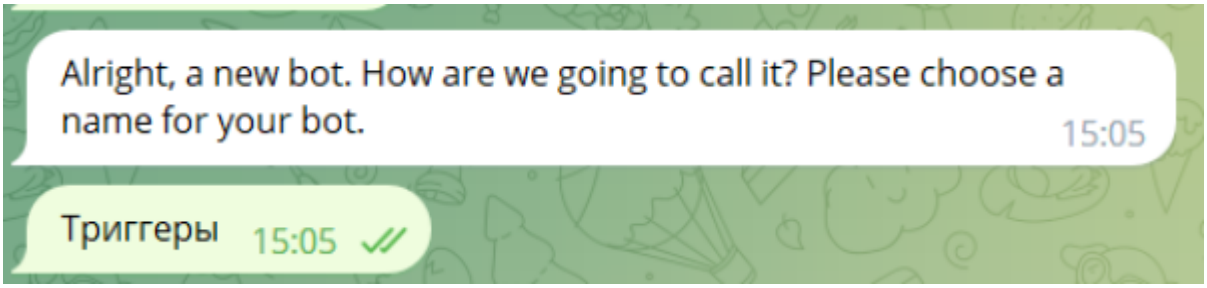
Telegram действие

Шаг 1. Регистрация своего бота через https://t.me/BotFather

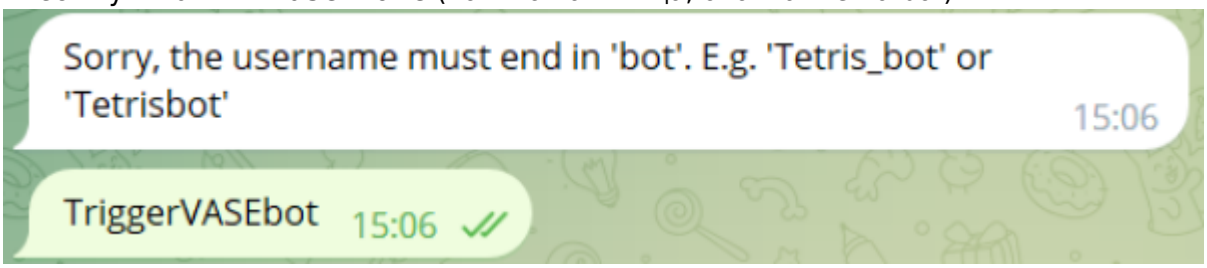
1. Запустить BotFather командой `/start`.
2. Нажать `/newbot` для создания нового бота.



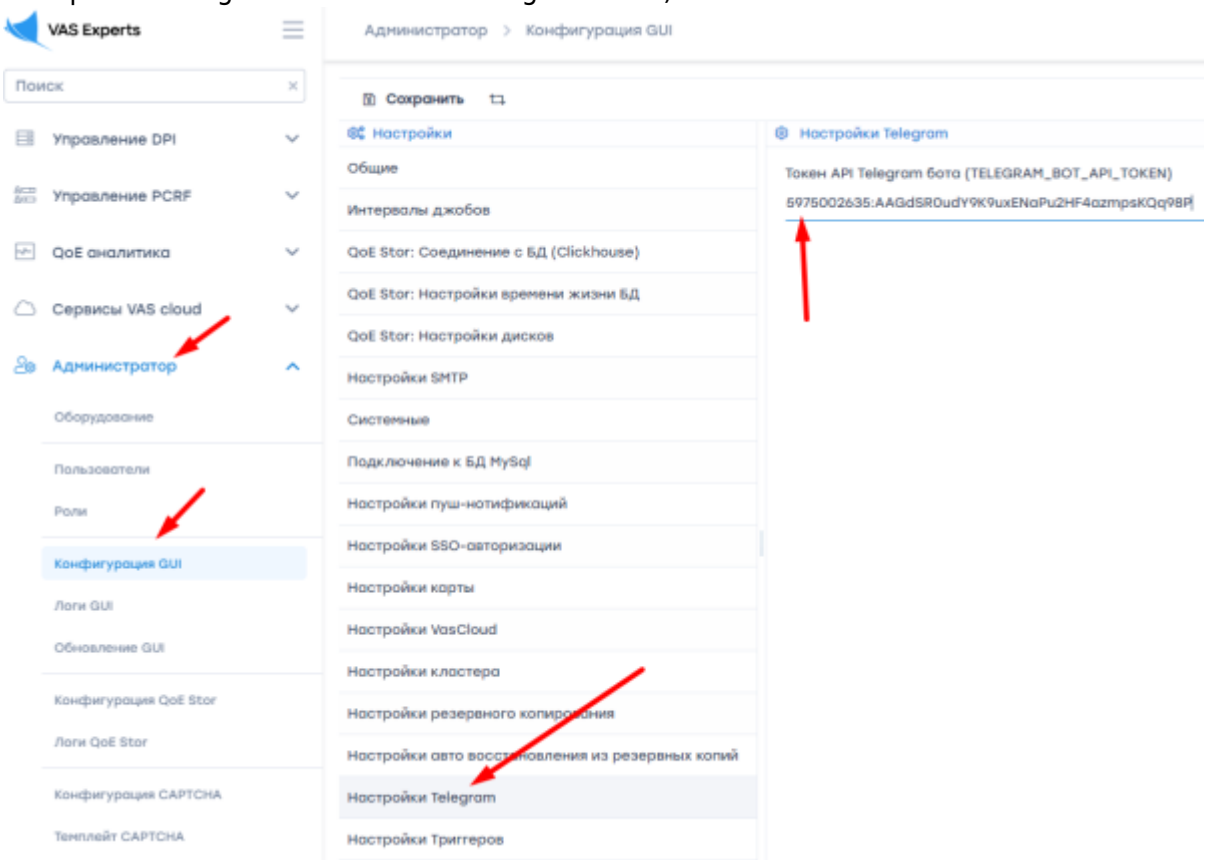
3. Ввести название бота.



4. Ввести уникальный `username` (только латиница, окончание на bot).



5. Скопировать токен для доступа к HTTP API из сообщения при регистрации бота, выглядит вот так: `5995002635:AAGdSR0udY9K9uxENaPu2HF4azmpsKQq98X`
6. Скопированный токен вставить в настройки GUI (Администратор → Конфигурация GUI → Настройки Telegram → Токен API Telegram бота).



Шаг 2. Получение id чата для своего персонального Telegram-аккаунта через https://t.me/RawDataBot

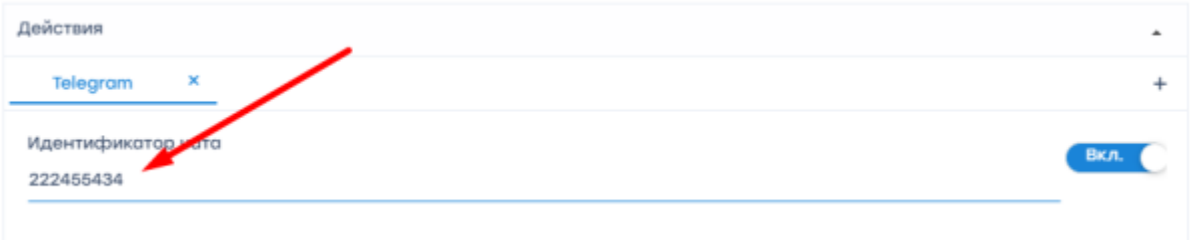
Для получения `id` чата у пользователя в Telegram-профиле должен быть задан `username`!

1. Запустить Telegram Bot Raw командой `/start`.
2. Скопировать `id`, выглядит так:

```
"chat": {
      "id": 222455434,
      "first_name": "Ivan",
      "last_name": "Nat",
      "username": "HardNat",
      "type": "private"
},
```

Шаг 3. Подключение Telegram к настроенному триггеру

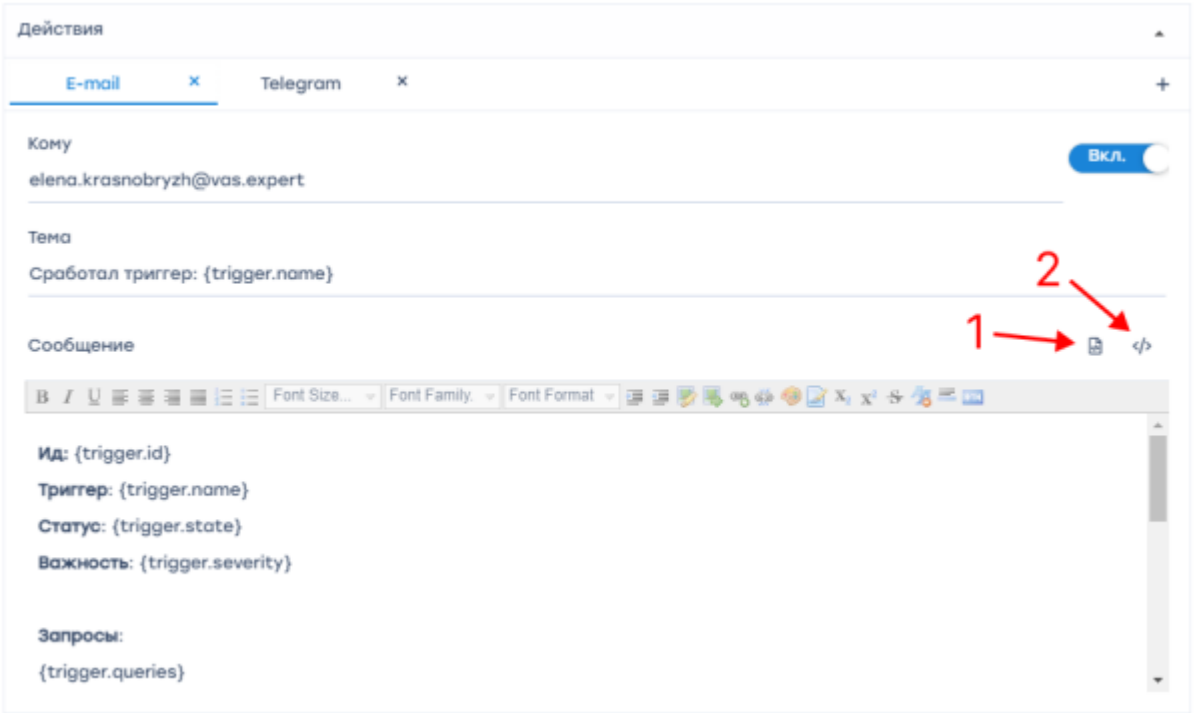
Добавить `id` из шага 2 в Telegram действие в поле "Идентификатор чата".



E-Mail действие

Создает уведомление и посылает его на выбранный адрес электронной почты.

1. Если поле "Сообщение" не заполнено — нажать на кнопку "Установить шаблон по умолчанию" (1) для заполнения полей действия значениями по умолчанию. При необходимости все значения можно отредактировать.
2. При нажатии на кнопку "Параметры шаблона" (2) Откроется меню с идентификаторами, которые можно использовать для составления сообщения.



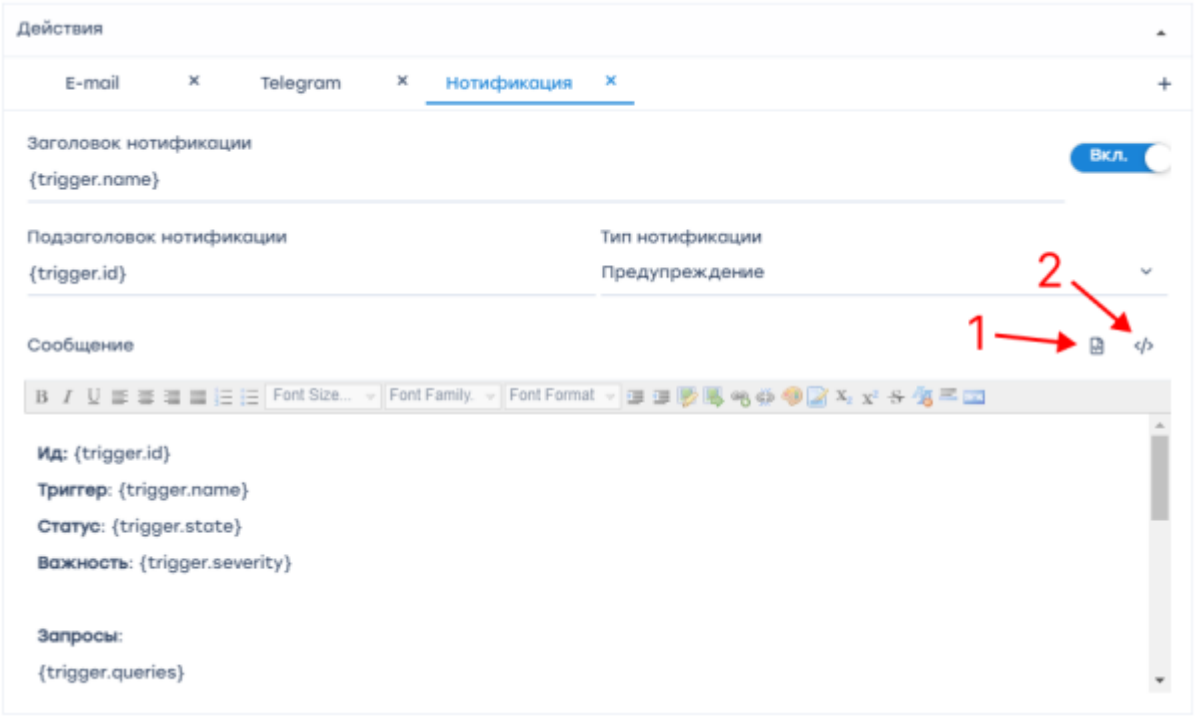
Для работы E-mail действия нужно настроить SMTP. Перейти в раздел Администратор →

Конфигурация GUI, выбрать "Настройки SMTP".

Нотификация в GUI

Нотификацию можно использовать для проверки работоспособности триггеров.

1. Нажать на кнопку "Установить шаблон по умолчанию" (1) для заполнения полей действия значениями по умолчанию. При необходимости все значения можно отредактировать.
2. При нажатии на кнопку "Параметры шаблона" (2) Откроется меню с идентификаторами, которые можно использовать для составления сообщения.



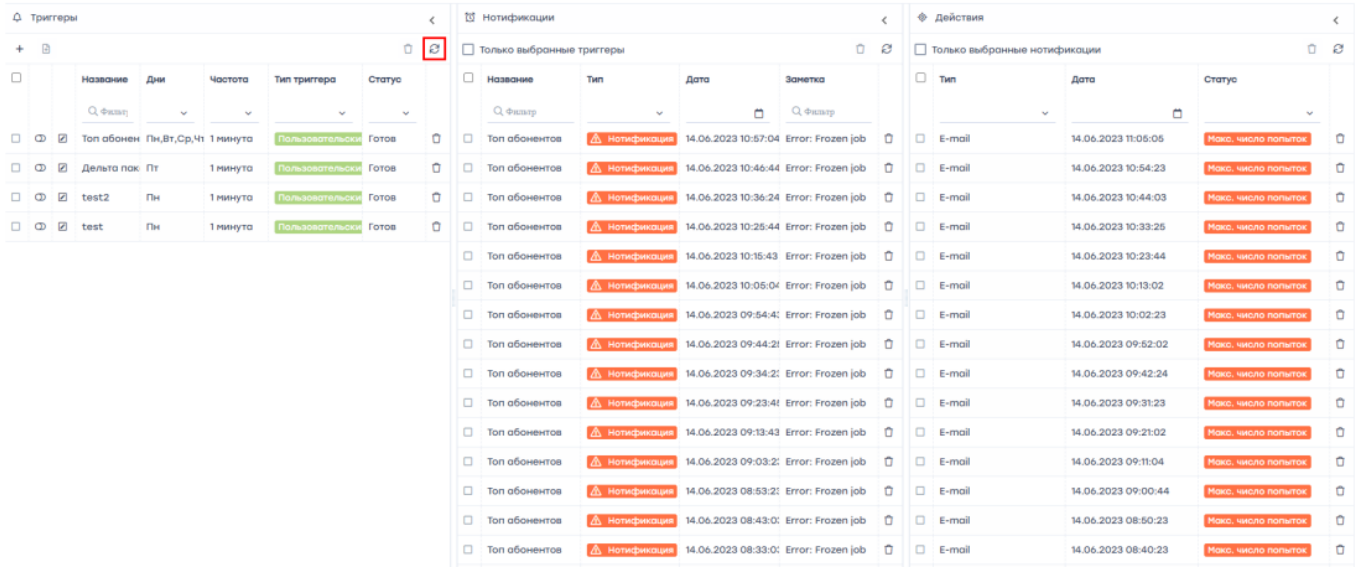
[GUI v.2.32.70+]
В меню "Параметры шаблона" добавлены новые идентификаторы:

- `{trigger.report.csv.as_file}` - прикрепить CSV файл (только для email)
- `{trigger.report.csv.as_file.zip}` - прикрепить архив с CSV файлом (только для email)

Раньше такие файлы можно было добавлять в сообщение только в формате ссылки, теперь можно добавлять файлы.
Также появилась возможность объединить в один PDF файл несколько отчетов, добавив в сообщение следующие новые идентификаторы:

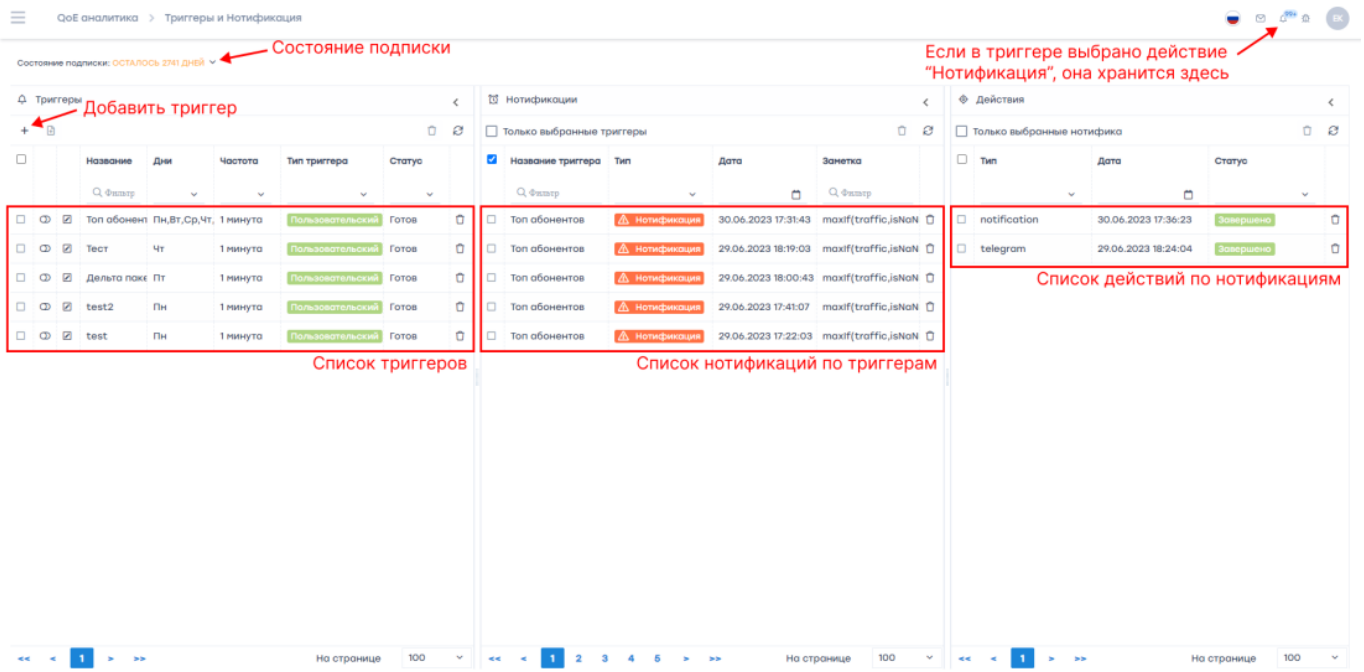
- `{trigger.report.merged_pdf}` - ссылка на PDF файл со всеми отчетами
- `{trigger.report.merged_pdf.as_file}` - прикрепить PDF файл со всеми отчетами (только для email)
- `{trigger.report.merged_pdf.as_file.zip}` - прикрепить архив с PDF файлом со всеми отчетами (только для email)

После создания триггера нажать "Сохранить". На дашборде "Триггеры" включить необходимые триггеры. Если страница GUI не обновлялась — обновить страницу в браузере или нажать на кнопку "Обновить".



Описание элементов страницы "Триггеры и Нотификация"

Перейти в раздел QoE Аналитика → Триггеры и Нотификация.
Откроется раздел как на картинке ниже.



В данном разделе отображены три секции:

- Список триггеров.
- Список нотификаций по триггерам.

- Список действий, выполненных триггерами в результате возникших нотификаций.

Типы триггеров:

- Системные. Задаются вендором и их можно только включить/выключить.
- Пользовательские. Задаются пользователем и могут свободно настраиваться.

Подробное описание настройки триггера смотрите в разделе Создание и настройка триггеров.