

Содержание

| | |
|---|----|
| QoE Триггеры и Нотификация | 3 |
| Назначение | 3 |
| Создание и настройка триггеров | 3 |
| Шаг 1. Расписание работы | 3 |
| Шаг 2. Выбор источника данных и метрики | 4 |
| Шаг 3. Условия | 7 |
| Шаг 4. Обработка ошибок | 8 |
| Шаг 5. Действия | 8 |
| Описание элементов страницы "Триггеры и Нотификация" | 12 |

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 расположена переключатель для включения/выключения триггера, **после окончания настройки не забудьте его включить**.

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

| Общее | | | |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| Название триггера * | Важность | Триггер | |
| Задержка RTT | Информация | <input type="radio"/> Выключен | |
| Дни недели * | Частота проверки * | Количество срабатываний | |
| Пн, Чт | 24 часа | 0 | |
| Дата начала | Дата окончания | Время начала | Время окончания |
| <input type="button" value=""/> | <input type="button" value=""/> | <input type="button" value=""/> | <input type="button" value=""/> |

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:

| Общее | | | |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| Название триггера * | Важность | Триггер | |
| Зараженные абоненты | Предупреждение | <input type="radio"/> Выключен | |
| Дни недели * | Частота проверки * | Количество срабатываний | |
| Пн, Вт, Ср, Чт, Пт, Сб, Вс | 1 минута | 0 | |
| Дата начала | Дата окончания | Время начала | Время окончания |
| <input type="button" value=""/> | <input type="button" value=""/> | <input type="button" value=""/> | <input type="button" value=""/> |

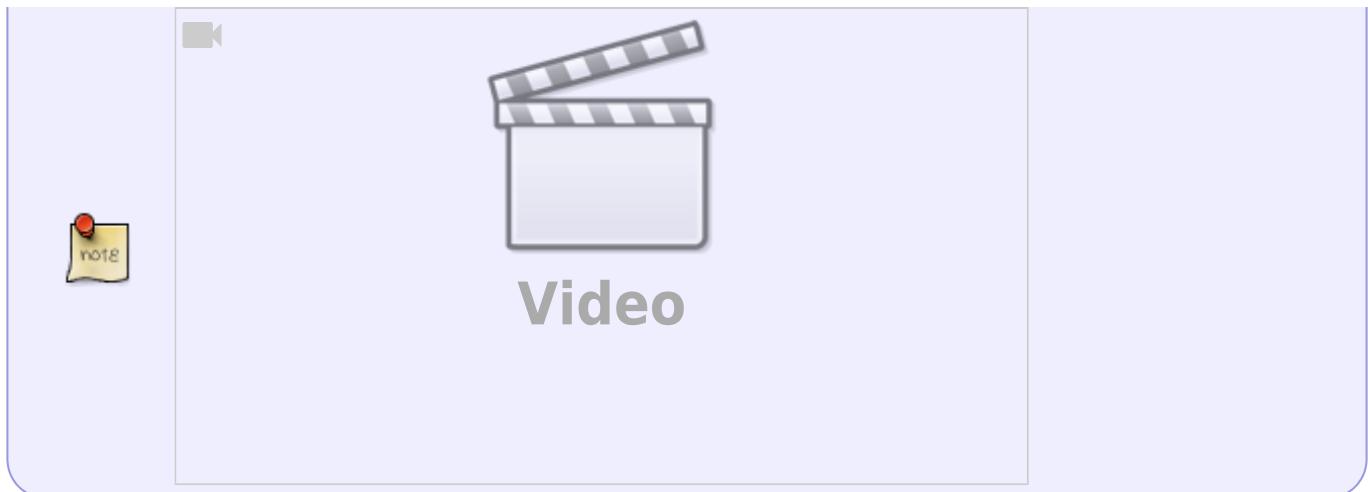
В этом случае скрипт проверки будет запускаться раз в минуту каждый день, то есть работать постоянно.

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:

Запросы

| Название | Отчет | Период с | Период по |
|--|-------------------------------|----------------------------------|-----------|
| <input checked="" type="checkbox"/> Вкл. А | Топ хостов с высоким трафиком | <input type="button" value="▼"/> | |

+ Условия

| Связь | Название | Функция | Комбинатор |
|--|----------|---------|-------------|
| <input checked="" type="checkbox"/> Вкл. И | А | max | если не NaN |

Обработка ошибок

Если нет данных *

Нотификация

Действия

Нотификация

Заголовок нотификации
{trigger.name}

Подзаголовок нотификации
{trigger.id}

Тип нотификации
Предупреждение

Фильтры

| Фильтр | Оператор | Значение | |
|--|----------|------------|---------------------------------------|
| <input checked="" type="checkbox"/> Вкл. Хост | = | google.com | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Абонент | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Логин | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. IP хоста | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Протокол | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Группы прикладных протоколов | in | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Прикладной протокол | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Номер АС источника | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Номер АС получателя | like | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Категория хоста | in | | <input type="button" value="Delete"/> |
| <input type="checkbox"/> Выкл. Категория зараженного трафика | in | | <input type="button" value="Delete"/> |

Отменить

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.

Запросы

| Название | Отчет | Период с | Период по |
|--|--|----------------------------------|------------------|
| <input checked="" type="checkbox"/> Вкл. А | Топ зараженных абонентов с ботнет трафиком | <input type="button" value="▼"/> | сейчас - 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:

| Условия | | | | | | | |
|--|-------|----------|---------|-------------|---------------------|----------|----------|
| + | | | | | | | |
| | Связь | Название | Функция | Комбинатор | Серия | Оператор | Значение |
| <input checked="" type="checkbox"/> Вкл. | И | A | any | если не NaN | RTT от абонента, мс | \geq | 150000 |

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:

| Условия | | | | | | | |
|--|-------|----------|---------|-------------|---------|----------|----------|
| + | | | | | | | |
| | Связь | Название | Функция | Комбинатор | Серия | Оператор | Значение |
| <input checked="" type="checkbox"/> Вкл. | И | A | count | если не NaN | Абонент | \geq | 1 |

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:



| Обработка ошибок | |
|-------------------|---------------------------------------|
| Если нет данных * | Если ошибка выполнения или тайм-аут * |
| Ok | Нотификация |

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.

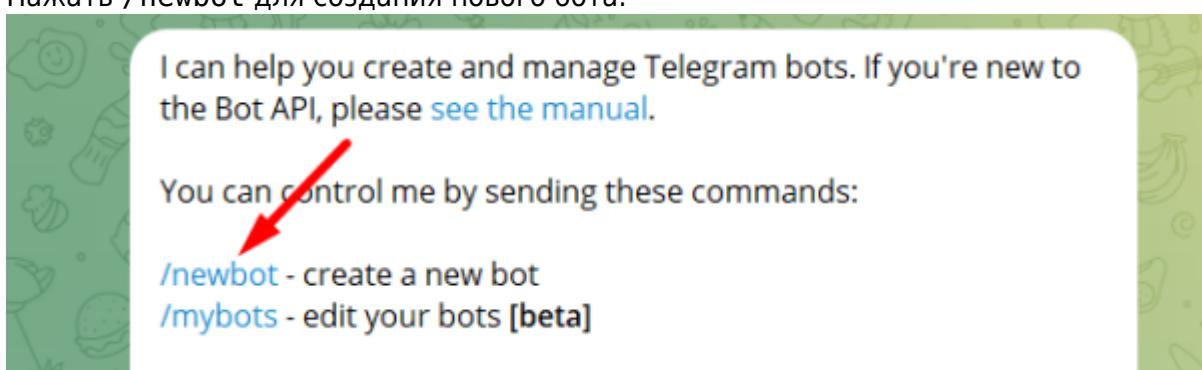
Для создания действия нажать на + под названием блока.

Для удаления действия нажать на X 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.

Alright, a new bot. How are we going to call it? Please choose a name for your bot.

15:05

Триггеры 15:05 ✓

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

Sorry, the username must end in 'bot'. E.g. 'Tetris_bot' or 'Tetrisbot'

15:06

TriggerVASEbot 15:06 ✓

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).

The screenshot shows the VAS Experts application interface. On the left, there's a sidebar with various menu items like 'Управление DPI', 'Управление PCRF', 'QoE аналитика', 'Сервисы VAS cloud', 'Администратор' (which has a red arrow pointing to it), 'Оборудование', 'Пользователи', 'Роли', 'Конфигурация GUI' (which is highlighted in blue and has a red arrow pointing to it), 'Логи GUI', 'Обновление GUI', 'Конфигурация QoE Stor', 'Логи QoE Stor', 'Конфигурация CAPTCHA', and 'Темплейт CAPTCHA'. The main panel shows a 'Конфигурация GUI' section with tabs for 'Настройки' and 'Настройки Telegram'. Under 'Настройки', there are several options like 'Общие', 'Интервалы джобов', 'QoE Stor: Соединение с БД (Clickhouse)', etc. Under 'Настройки Telegram', the 'Токен API Telegram бота (TELEGRAM_BOT_API_TOKEN)' field contains the value '5995002635 : AAGdSR0udY9K9uxEnaPu2HF4azmpsKQq98X'. A red arrow points from the 'Настройки Telegram' tab to this token field.

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".

Действия

Telegram

Идентификатор чата

222455434

Вкл.

E-Mail действие

Создает уведомление и посыпает его на выбранный адрес электронной почты.

- 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.
- При нажатии на кнопку "Параметры шаблона" (2) Откроется меню с идентификаторами, которые можно использовать для составления сообщения.

Действия

E-mail

Кому

elena.krasnobryzh@vas.expert

Тема

Сработал триггер: {trigger.name}

Сообщение

Ид: {trigger.id}
Триггер: {trigger.name}
Статус: {trigger.state}
Важность: {trigger.severity}

Запросы:
{trigger.queries}

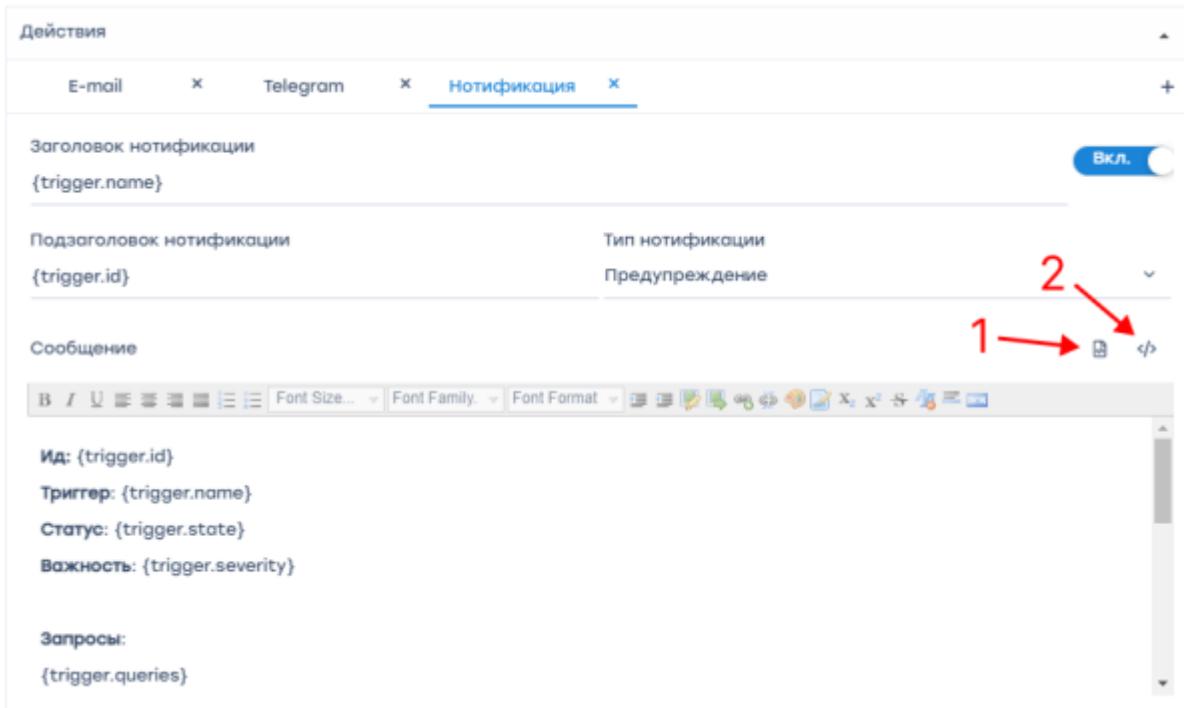
Для работы E-mail действия нужно настроить SMTP. Перейти в раздел Администратор →

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".

The screenshot shows three tables side-by-side:

- Триггеры (Triggers):** Shows a list of triggers with columns: Название (Name), Дни (Days), Частота (Frequency), Тип триггера (Trigger Type), and Статус (Status). One trigger is selected.
- Нотификации (Notifications):** Shows a list of notifications with columns: Название (Name), Тип (Type), Дата (Date), and Заметка (Note). One notification is selected.
- Действия (Actions):** Shows a list of actions with columns: Тип (Type), Дата (Date), and Статус (Status). One action is selected.

Описание элементов страницы "Триггеры и Нотификация"

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

The screenshot shows the same three tables with additional annotations:

- Состояние подписки:** Осталось 2741 дней (Subscription status: 2741 days left) with an arrow pointing to the top right of the first table.
- Список триггеров (List of triggers):** Shows the list of triggers with one selected.
- Список нотификаций по триггерам (List of notifications by triggers):** Shows the list of notifications corresponding to the selected trigger.
- Список действий (List of actions):** Shows the list of actions corresponding to the selected notification.
- Если в триггере выбрано действие "Нотификация", она хранится здесь (If the trigger selects the "Notification" action, it is stored here):** An arrow points to the 'notification' entry in the 'Actions' table.
- Список действий по нотификациям (List of actions by notifications):** A red box highlights the 'notification' entry in the 'Actions' table.

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](#).