

Содержание

12 QoE Аналитика	3
-------------------------	-------	---

12 QoE Аналитика

Не забудте настроить подключение к [QoE Stor](#).

Для удобства использования раздел разделен на несколько подразделов.

[QoE Дашборд](#)

[QoE Нефлоу](#)

[QoE Кликстриим](#)

[QoE Абоненты](#)

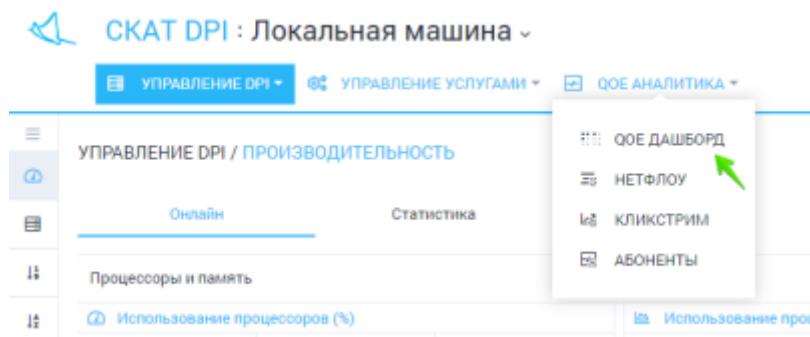
[QoE Триггеры и нотификации](#)

Представленные разделы содержат наборы отчетов (табличных и графических) и фильтров. Каждый отчет позволяет проводить анализ данных под разным углом зрения.

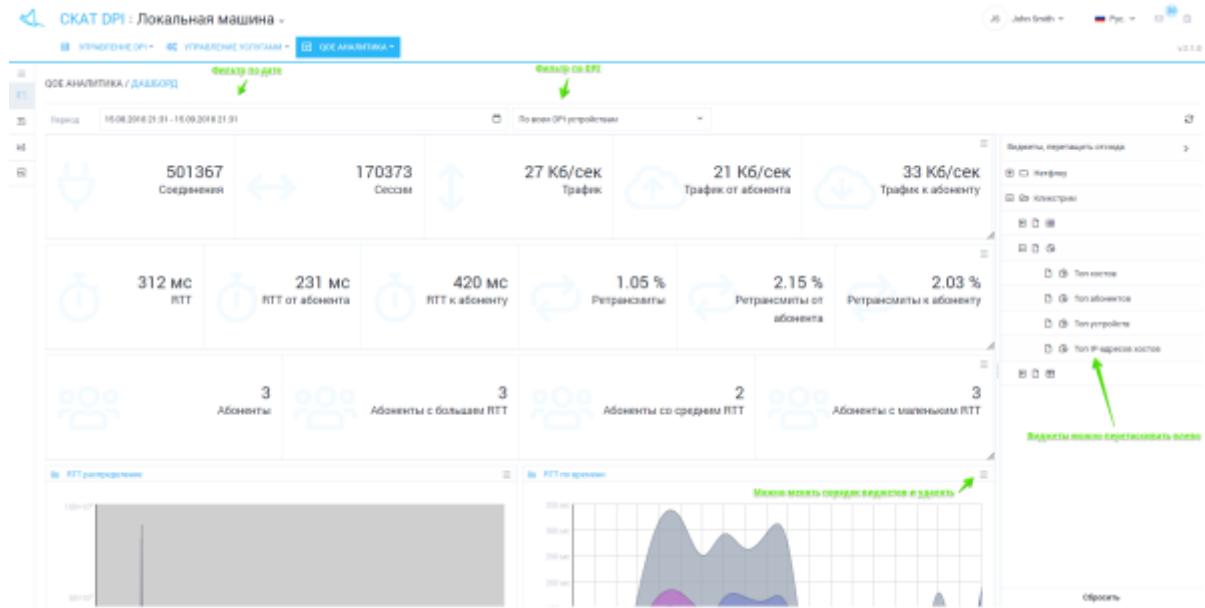
QoE Дашборд

В данном разделе собран набор всех отчетов-виджетов, имеющихся в системе. Виджеты можно перемещать, добавлять (путем переноса из правой части в левую), удалять.

Для перехода в раздел откройте меню QoE Аналитика и нажмите Дашборд.



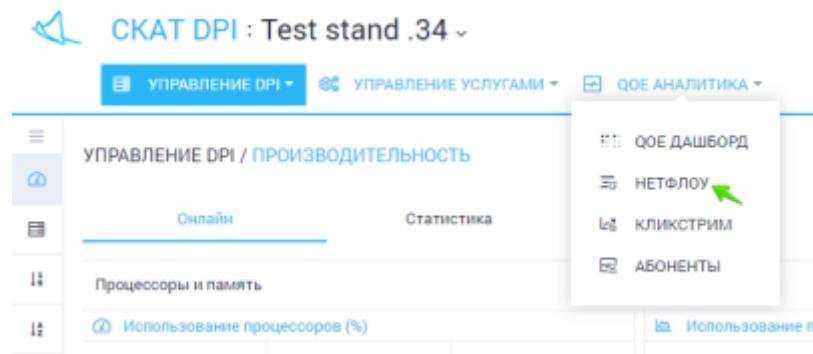
Откроется раздел как на картинке ниже.



QoS Нефлоу

В данном разделе собраны отчеты для анализа нетфлоу.

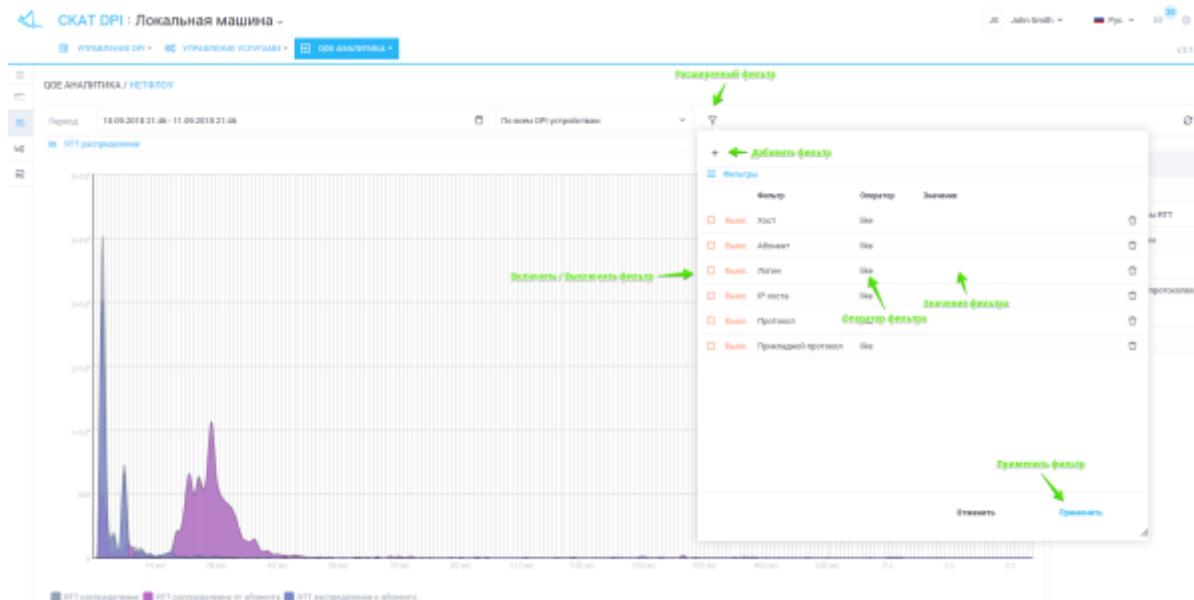
Для перехода в раздел откройте меню QoS Аналитика и нажмите Нетфлоу.



Откроется раздел как на картинке ниже.



Для расширенного анализа имеется возможность устанавливать фильтры.



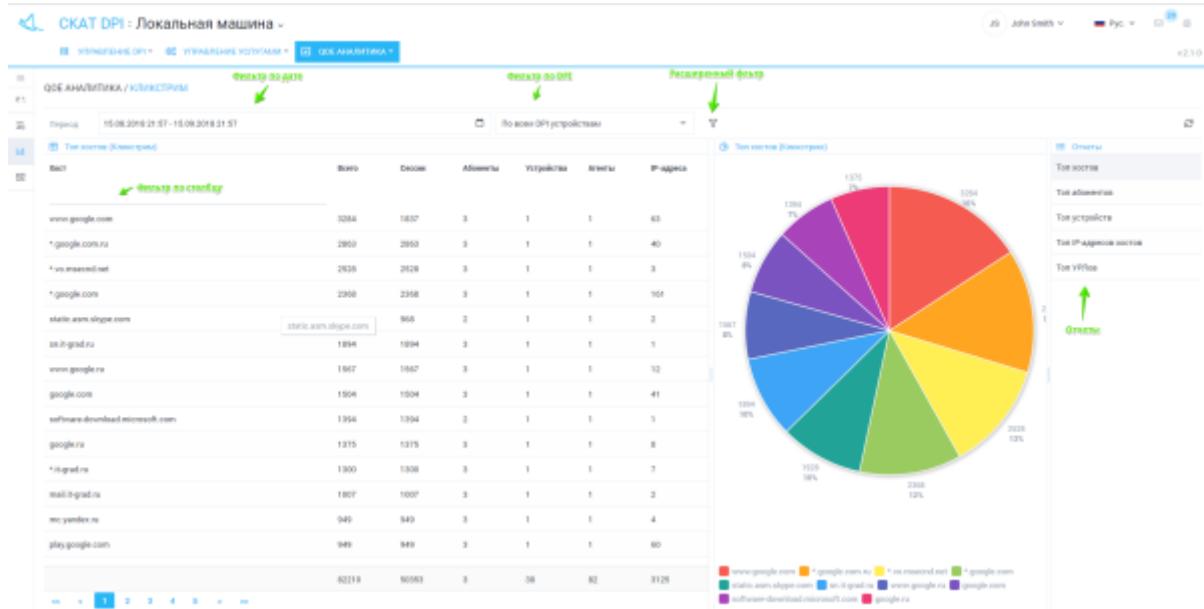
QoE Кликстрим

В данном разделе собраны отчеты для анализа клистрим.

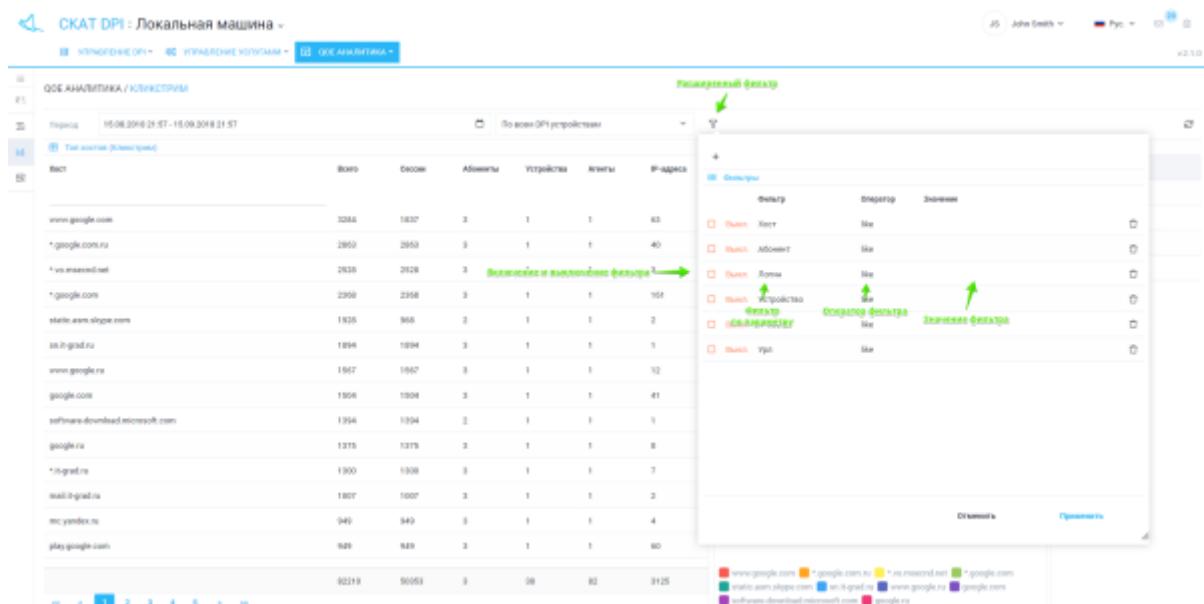
Для перехода в раздел откройте меню QoS Аналитика и нажмите Кликстрим.

СКАТ DPI : Test stand .34

Откроется раздел как на картинке ниже.



Для расширенного анализа имеется возможность устанавливать фильтры.

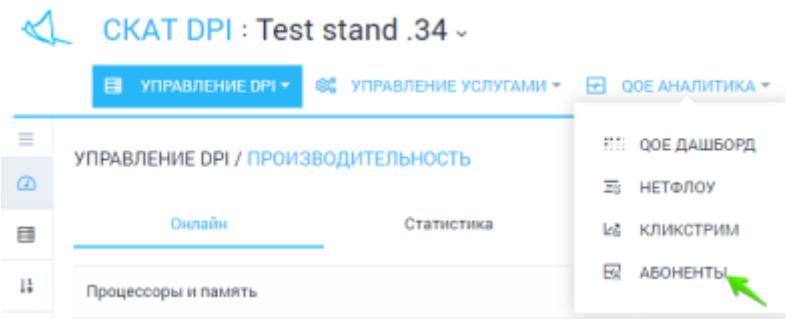


QoS Абоненты

В данном разделе собраны отчеты для анализа нетфлоу и кликстрим в разрезе абонентов.

Особенностью данного раздела является то, что имеется возможность сформировать пользовательский список именованных фильтров (шаблонов поиска): поиск абонентов, посещающих сайты конкурентов; поиск абонентов, использующих IPTV или телефонию; поиск результатов измерения скорости интернета абонентами...

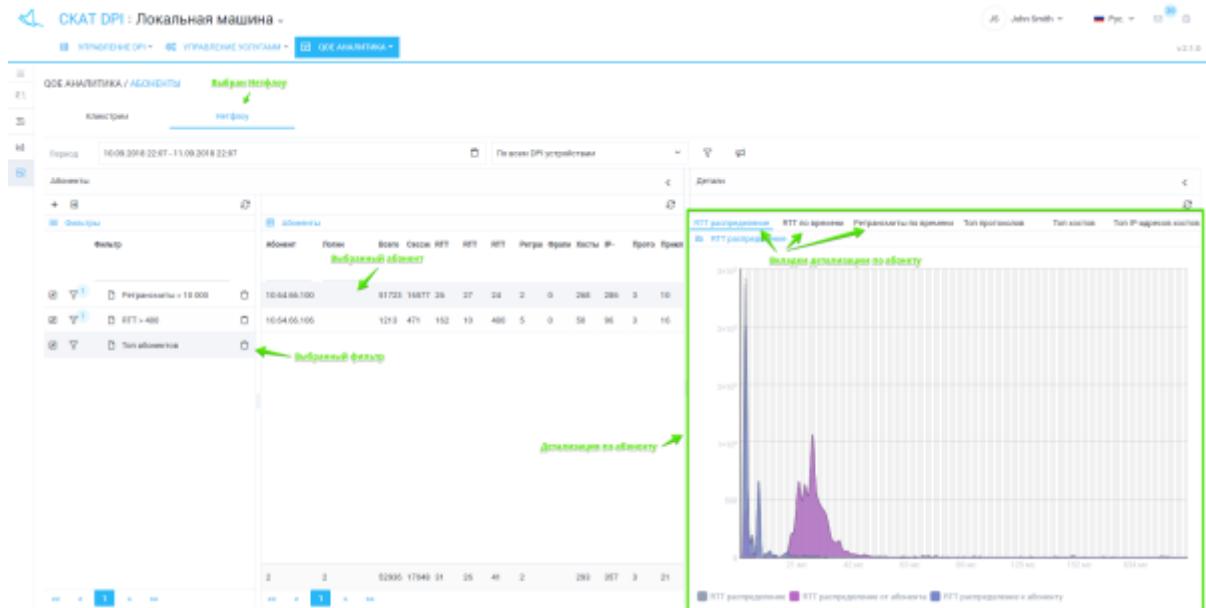
Для перехода в раздел откройте меню QoE Аналитика и нажмите Абоненты.



Откроется раздел как на картинке ниже.

The screenshot shows the 'АБОНЕНТЫ' section of the SKAT DPI interface. On the left, a sidebar displays a list of filters: 'Результаты запросов', '64.235.195.136', 'по клиентам', 'по устройствам', 'ядро', 'топ-абонентов', 'лок.', 'тест'. A green box highlights this sidebar. Several green arrows point to specific items: 'Выбранный объект' (highlighting a selected device), 'Фильтр по IP', 'Фильтр по устройствам', 'Создание реестровой кампании', 'Выбранный фильтр' (highlighting the 'по клиентам' filter), 'Детализация по объекту' (highlighting the device details table), and 'Сохранение фильтра' (highlighting the 'Сохранить' button). The main table lists devices with columns: Имя устройства, Агенты, Хосты, IP-адреса хостов, УРЛы, IP-адреса хостов. The table includes rows for 'Локальная машина', 'Маршрутизатор', 'Миниатюрный ПК', 'НСС', 'Microsoft BTB', 'QE', 'Microsoft CryptowAPI', 'Avast NOC', 'Windows Update Agent', 'RF-Нагрузчик', and 'Samsung Android v7.0, samsung_hen20'. The table has a green border.

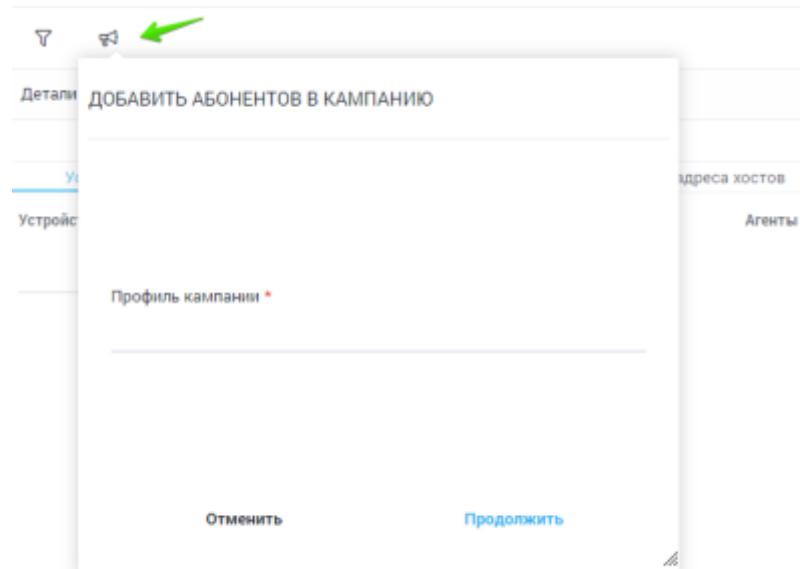
Для анализа абонентов в разрезе нетфлоу, откройте вкладку Нетфлоу.



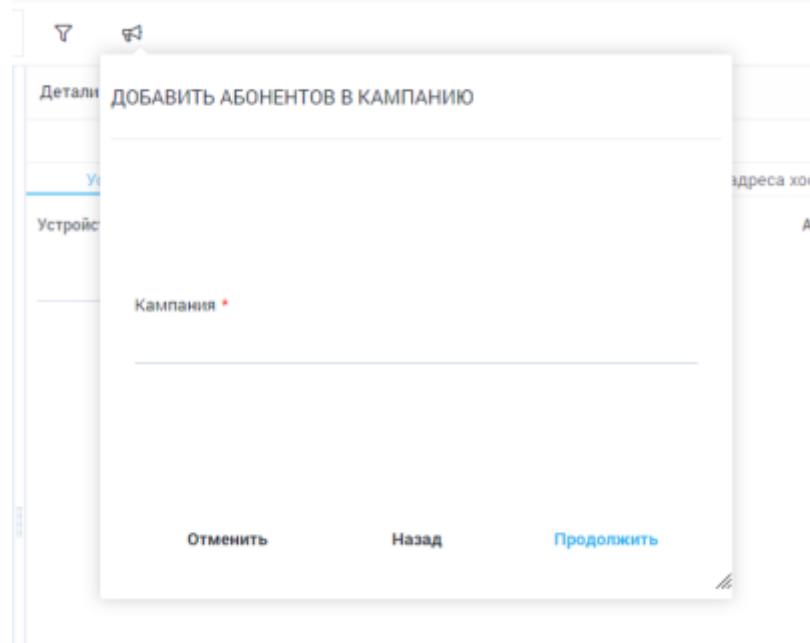
Экспорт QoE абонентов в рекламную кампанию

В разделе “QoE Абоненты” имеется возможность создать рекламную кампанию и экспортовать список отфильтрованных абонентов.

Перейдите в раздел QoE Абоненты. Выберите фильтр. Нажмите кнопку “Добавить абонентов в кампанию”.



Введите профиль кампании (будет создан новый, если профиля еще нет). На следующем шаге введите название кампании (будет создана новая, если кампании еще нет).

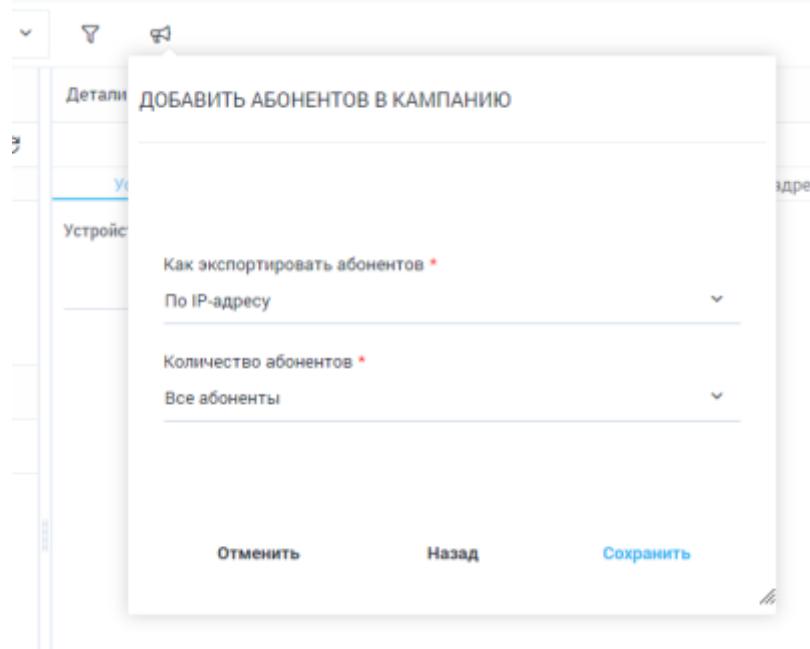


На следующем шаге откроется форма редактирования кампании. Можете заполнить или отредактировать данные.

Настройки кампании			Данные кампании		
Название *	test_campaign		+ Добавить параметр	По умолчанию	
Ответственный	Стрелок С.С.		param1	Строка	value1
Период кампании *	07.07.2018 - 30.09.2018		param2	Строка	value2
Время с *	00:00	Время по *	22:55		
Дни недели *	Пн, Вт, Ср, Чт, Пт, Сб, Вс				
URL перенаправления *	https://ап.уадекс.ru/?param1				
Состояние кампании	Кампания остановлена (по умолчанию)				

Отменить Сохранить

На последнем шаге нужно выбрать как экспортитьировать абонентов: по ip адресу или логину. При необходимости ограничить количество абонентов.



QoE Триггеры и нотификации

В данном разделе можно управлять триггерами системы. Триггеры в фоном режиме по расписанию обрабатывают статистику и при определенных условиях, заданных пользователем формируют нотификации и выполняют определенные действия, заданные пользователем.

Для перехода в раздел откройте меню QoE Аналитика и нажмите Триггеры и нотификации.

SKAT DPI : miniDPI ~

УПРАВЛЕНИЕ DPI УПРАВЛЕНИЕ УСЛУГАМИ QOE АНАЛИТИКА СЕРВИСЫ

QOE АНАЛИТИКА / ТРИГГЕРЫ И НОТИФИКАЦИЯ

Триггеры

Название	Дни недели	Частота	Тип
ssh bruteforce	Пн,Вт,Ср,Чт,Г	10 минут	Смс
Test	Пн,Вт,Ср,Чт,Г	0 минут	Пол

QOE ДАШБОРД
НЕТФЛОУ
КЛИКСТРИМ
АБОНЕНТЫ
СЫРОЙ ПОЛНЫЙ НЕТФЛОУ
СЫРОЙ КЛИКСТРИМ
ТРИГГЕРЫ И НОТИФИКАЦИЯ
АДМИНИСТРАТОР

Откроется раздел как на картинке ниже.

СОСТОЯНИЕ ПОДПИСКИ

Список триггеров

Список нотификаций по триггерам

Список действий по нотификациям

В данном разделе отображены три секции:

- Список триггеров слева
- Список нотификаций по центру
- Список действий выполненных триггерами в результате возникших нотификаций

Триггеры могут быть пользовательскими и системными. Системные триггеры задаются вендором и их можно только отключить / подключить. Пользовательские триггеры задаются пользователем. Для работы пользовательских триггеров требуется активация подписки (лицензия Standart для dpii2).

Нотификации бывают нескольких типов:

- “Нотификация” – означает, что выполнено условие, заданное в триггере
- “Нет данных” – означает, что при обработке отчетов, заданных в триггере , не найдено данных
- “Сохранить последнее состояние” – означает, что не нужно принимать никаких действий
- “Ок” – означает, что условия заданные в триггере, не сработали, все в порядке и никаких действий выполнять не нужно

Действия по нотификациям бывают двух типов:

- E-mail – отправляется e-mail на один или несколько заданных адресов с определенным шаблоном
- Http – вызывается http ресурс методом GET или POST. На ресурс передаются xml- или json- данные, заданные в шаблоне.

Чтобы добавить триггер нажмите кнопку Плюс. Откроется форма, как на картинках ниже.

Общее

Название триггера *	Test table	Важность	Триггер	<input checked="" type="checkbox"/> Выключен
Дни недели *	Пн, Вт, Ср, Чт, Пт, Сб, Вс	Частота проверки *	0 минут	Количество срабатываний
Дата начала	Дата окончания	Время начала	Время окончания	
<input type="button" value=""/>				

Общие параметры триггера

Кнопка включения

Запросы

Список отчетов, обрабатываемых триггером

Название	Отчет	Период с	Период по
<input checked="" type="checkbox"/> Вкл. А	Топ абонентов с высоким трафиком	<input type="button" value="▼"/> сейчас - 1 час	сейчас

Условия

Список условий для срабатывания триггера

Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
<input checked="" type="checkbox"/> Вкл. И	А	avg	если не NaN	Трафик, бит/с	>=	1

Обработка ошибок

Поведение триггера при возникновении ошибок

Если нет данных *	Если ошибка выполнения или тайм-аут *
Нет данных	Сохранить последнее состояние

Действия

[Отменить](#) [Сохранить](#)

The screenshot shows the 'Trigger Editor' interface with several sections:

- Конфигурация триггера** (Trigger Configuration) at the top.
- Условия** (Conditions) section with a table:

Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
<input checked="" type="checkbox"/> Вкл.	И	А	avg	если не NaN	Трафик, Бит/с	>=	1
- Обработка ошибок** (Error Handling) section with dropdowns for 'Если нет данных' (If no data) and 'Если ошибка выполнения или тайм-аут' (If execution error or timeout).
- Действия** (Actions) section, highlighted with a green border:
 - E-mail** and **Http** buttons with 'Добавить действие' (Add action) and 'Вкл.' (Enabled) switch.
 - Вызов http ресурса** (Call http resource) button with a green arrow pointing to it.
 - Отправка на e-mail** (Send via e-mail) button with a green arrow pointing to it.
 - Сработал триггер: (trigger.name)** (Trigger triggered: (trigger.name)) message.
 - Настройка действий при срабатывании триггера** (Action settings when trigger fires) section with a rich text editor toolbar.
 - Text fields for **Ид: {trigger.id}**, **Триггер: {trigger.name}**, **Статус: {trigger.state}**, and **Важность: {trigger.severity}**.
 - Запросы:** (Requests:) section.
- Buttons at the bottom: **Отменить** (Cancel) and **Сохранить** (Save).

В форме редактирования триггеров несколько блоков.

В блоке Общее можно задать общие параметры триггера: название, включен/выключен, частота проверки, расписание проверки

В блоке Запросы задается список отчетов, обрабатываемых триггером. Для каждого отчета можно установить фильтр и период.

В блоке Условия задается список условий для срабатывания триггера. Каждое условие привязано к определенному отчету. Набор параметров, определяемых в условии зависит от отчета, к которому условие привязано.

В блоке Обработка ошибок можно задать поведение триггера в ситуациях, когда нет данных или когда в процессе работы триггера возникла ошибка.

В блоке Действия можно задать действия при срабатывании условий в триггере: либо отправка e-mail, либо вызов http ресурса.

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

The screenshot shows the configuration interface for a trigger. On the left, there's a sidebar with sections like 'Conditions' and 'Bind'. The main area has tabs for 'Report' and 'Period from/to'. A dropdown menu under 'Report' shows 'Top subscribers with high RTT'. The 'Period from' is set to 'now - 15 minute' and 'Period to' is 'now'. Below this, the 'Conditions' section is expanded, showing a list of available metrics: 'Netflow', 'Panels', 'Series charts', 'Pie charts', 'Top subscribers', 'Top subscribers with high RTT' (which is currently selected), 'Top subscribers with high traffic', and 'Top subscribers with high retransmits'. To the right of the list is a table for defining conditions with columns 'Operator' and 'Value'. Two rows are present: one with ' \leq ' operator and value '200000', and another with ' \geq ' operator and value '1'. At the bottom, there's a section for 'If no data'.

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: $=$, \neq , $>$, \geq , $<$, \leq , between, not between.)

Значение (присвоить уникальное значение)

Common

Trigger name *	Severity information	Trigger	
DDos find who		<input checked="" type="radio"/> Disabled	
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	now - 15 minute	now	

Conditions

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

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 посыпает 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

The screenshot shows the VAS Experts DPI : FastDPI interface. The left sidebar has a tree view with nodes like EQUIPMENT, USERS, ROLES, and DPIUI2. Under DPIUI2, there are sub-nodes for logs, update, and server configurations for QoS Stor, Fast PCRF, and DPIUI2 GUI. The main panel shows the 'ADMINISTRATOR / DPIUI2 (GUI) SERVER CONFIGURATION' screen. A dropdown menu is open over the 'Settings' button, showing options like EQUIPMENT, USERS, ROLES, and various SERVER CONFIGURATION sections. The 'DPIUI2 (GUI) SERVER CONFIGURATION' section is currently selected. Within this section, there are sub-options for logs and update. To the right of the dropdown, there are fields for SMTP host, port, and password, along with their corresponding configuration keys (CFG_SMTP_HOST, CFG_SMTP_PORT, CFG_SMTP_PW).

Перейти в раздел настройки SMTP: SMTP SETTINGS

The screenshot shows the 'SMTP settings' section of the configuration interface. On the left, there is a sidebar with various settings categories: Common, Jobs intervals and periods, QoEStor DB (Clickhouse) connection, QoEStor DB lifetime settings, SMTP settings (which is currently selected), System, DB (MySQL) connection, and Push notifications settings. The main panel displays 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)
ed@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' section with an 'Http' tab selected. It displays the following configuration:

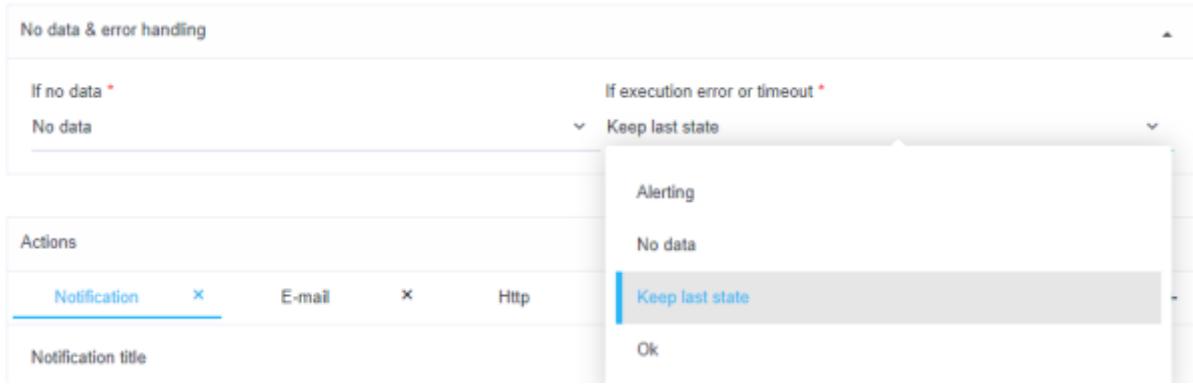
- Method:** POST
- Url:** https://your_redmine_host/issues.xml?key=your_redmine_api_key
- On:** On (switch is turned on)
- Headers:** Content-Type: application/xml
- Body:**

```
<?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 right, there 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: REMAIN 360 DAYS

Triggers					Alerts					Alerts actions				
Trigger	Days of	Check	Trigger type	State	Trigger name	Type	Date	Note	Type	Date	Note			
<input checked="" type="checkbox"/> DDoS	Mon,Tue,...	1 minute	Custom	Ready	Ddos	Alerted	14.08.2020 13:58:	avg(flow.vol_to_5)	notification	14.08.2020 13:59:03	Complete			
<input checked="" type="checkbox"/> DDoS	Mon,Tue,...	1 minute	Custom	Ready	DDos новая искрив.	Alerted	14.08.2020 13:58:	avg(avg_see_blei)	notification	14.08.2020 13:58:23	Complete			
<input checked="" type="checkbox"/> ssh brutef.	Mon,Tue,...	10 minute	Custom	Ready	DDos	Alerted	14.08.2020 13:59:	avg(flow.vol_to_5)	notification	14.08.2020 13:59:43	Complete			
					DDos	Alerted	14.08.2020 13:54:	avg(flow.vol_to_5)	notification	14.08.2020 13:56:05	Complete			
					DDos	Alerted	14.08.2020 13:52:	avg(flow.vol_to_5)	notification	14.08.2020 13:52:22	Complete			
					DDos новая искрив.	Alerted	14.08.2020 13:51:	avg(avg_see_blei)	notification	14.08.2020 13:50:26	Complete			
					DDos	Alerted	14.08.2020 13:50:	avg(flow.vol_to_5)						