

# Содержание

<b>Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE .....</b>	3
<b>Пример настройки триггера на поиск источника DDOS-атаки типа Flood .....</b>	3
<b>Пример настройки триггера на поиск цели DDOS-атаки типа Flood .....</b>	9
<b>Анализ BotNet .....</b>	11
<b>Фиксация перехода абонента на ресурс конкурента .....</b>	12



# Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE

Триггеры используются для поиска данных в QoE Stor по заданным параметрам. После срабатывания триггера возможно одно из действий:

- уведомление в GUI
- HTTP действие
- отправка email

Необходимые опции СКАТ DPI:

- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- Внедрение и администрирование

## Пример настройки триггера на поиск источника DDoS-атаки типа Flood

### Общая информация триггера

Общее			
Название триггера *	Важность	Триггер	
DDoS поиск источника	Информация	<input checked="" type="radio"/> Выключен	
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	1 час	1	
Дата начала	Дата окончания	Время начала	Время окончания
<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>

Название триггера «DDoS поиск источника», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

## Запросы

Запросы								
+								
	Название	Отчет		Период с	Период по			
<input checked="" type="checkbox"/> Вкл.	A	Maxi		▼ сейчас - 15 минут	сейчас			<input type="button" value=""/>

- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Сырой полный сетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 15 минут», период по: «сейчас»



В этом случае будет происходить анализ трафика по выбранной странице в период — последние 15 минут.

## Условия

Условия								
+								
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
<input checked="" type="checkbox"/> Вкл.	И	A	avg		Время жизни <=		20	<input type="button" value=""/>
<input checked="" type="checkbox"/> Вкл.	И	A	avg		Сессии	>=	1500	<input type="button" value=""/>

- Добавить "+" 2 поля
- Связка – И
- Функция – avg
- Серия в 1 поле – Время жизни сессии, мс <= 20
- Серия во 2 поле – Сессии >= 1500



Мы задали условие — для срабатывания триггера необходимо, чтобы были детектированы: И сессии с жизнью меньше или равно 20мс, И с одного IP-хоста было более 1500 сессий.

## Обработка ошибок

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

- В поле "Если нет данных" — нет данных
- В поле "Если есть ошибка или тайм-аут" — сохранить последнее состояние



в этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

## Действия

### E-mail действие

Действия	
<b>E-mail</b>	<b>x</b>
<p>Кому your@email.com</p> <p>Вкл. <input checked="" type="checkbox"/></p>	
<p>Тема Trigger fired: {trigger.name}</p>	
<p>Сообщение</p> <p><b>Font</b> <b>Font Size...</b> <b>Font Family...</b> <b>Font Format...</b> <b>Text Color...</b> <b>Background Color...</b> <b>Link Color...</b> <b>Text Style...</b> <b>Text Alignment...</b> <b>Text Spacing...</b> <b>Text Transformation...</b> <b>Text Underline...</b> <b>Text Overline...</b> <b>Text Strike...</b> <b>Text Emphasis...</b> <b>Text Decoration...</b> <b>Text Font...</b> <b>Text Font Weight...</b> <b>Text Font Style...</b> <b>Text Font Variant...</b> <b>Text Font Size...</b> <b>Text Font Family...</b> <b>Text Font Format...</b> <b>Text Text Color...</b> <b>Text Background Color...</b> <b>Text Link Color...</b> <b>Text Text Style...</b> <b>Text Text Alignment...</b> <b>Text Text Spacing...</b> <b>Text Text Transformation...</b> <b>Text Text Underline...</b> <b>Text Text Overline...</b> <b>Text Text Strike...</b> <b>Text Text Emphasis...</b> <b>Text Text Decoration...</b> <b>Text Text Font...</b> <b>Text Text Font Weight...</b> <b>Text Text Font Style...</b> <b>Text Text Font Variant...</b> <b>Text Text Font Size...</b> <b>Text Text Font Family...</b> <b>Text Text Font Format...</b></p> <p><b>Id:</b> {trigger.id}  <b>Trigger:</b> {trigger.name}  <b>Status:</b> {trigger.state}  <b>Severity:</b> {trigger.severity}</p> <p><b>Queries:</b>  {trigger.queries}</p>	

- Для автоматического заполнения — кликнуть по иконке (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние)

## Нотификация

Действия

E-mail X Нотификация X +

---

Заголовок нотификации  
{trigger.name} Вкл.

---

Подзаголовок нотификации  
{trigger.id} Тип нотификации  
Предупреждение ▼

---

Сообщение

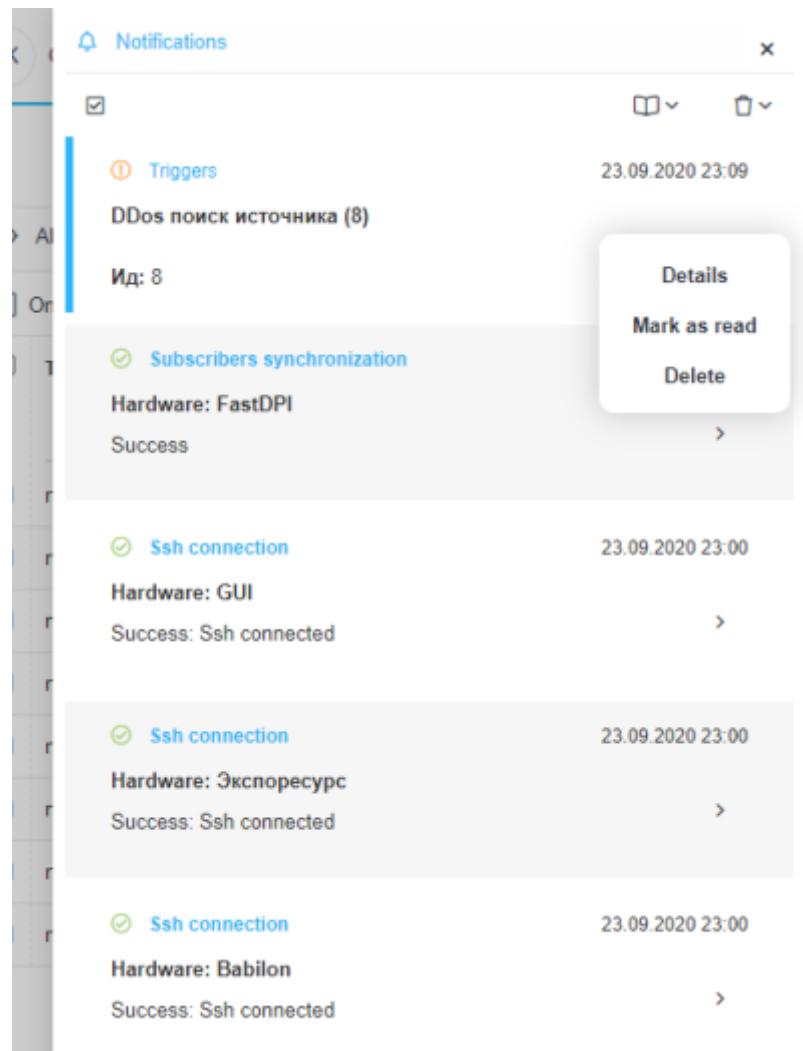
Ид: {trigger.id}  
Триггер: {trigger.name}  
Статус: {trigger.state}  
Важность: {trigger.severity}

Запросы:  
{trigger.queries}

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ

Alerts					Alerts actions				
<input type="checkbox"/> Only selected triggers					<input type="checkbox"/> Only selected notifications				
Trigger name	Type	Date	Note		Type	Date	State		
Ddos	 Alerting	14.08.2020 13:58:	avg(flow_vol_to_s	<input type="checkbox"/>	notification	14.08.2020 13:59:03	Complete	<input type="checkbox"/>	
DDos поиск источ-	 Alerting	14.08.2020 13:58:	avg(avg_ses_lifeti	<input type="checkbox"/>	notification	14.08.2020 13:58:23	Complete	<input type="checkbox"/>	
Ddos	 Alerting	14.08.2020 13:56:	avg(flow_vol_to_s	<input type="checkbox"/>	notification	14.08.2020 13:56:43	Complete	<input type="checkbox"/>	
DDos поиск источ-	 Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti	<input type="checkbox"/>	notification	14.08.2020 13:56:05	Complete	<input type="checkbox"/>	
Ddos	 Alerting	14.08.2020 13:54:	avg(flow_vol_to_s	<input type="checkbox"/>	notification	14.08.2020 13:54:23	Complete	<input type="checkbox"/>	
Ddos	 Alerting	14.08.2020 13:52:	avg(flow_vol_to_s	<input type="checkbox"/>	notification	14.08.2020 13:52:22	Complete	<input type="checkbox"/>	
DDos поиск источ-	 Ok	14.08.2020 13:51:	avg(avg_ses_lifeti	<input type="checkbox"/>	notification	14.08.2020 13:50:25	Complete	<input type="checkbox"/>	
Ddos	 Alerting	14.08.2020 13:50:	avg(flow_vol_to_s	<input type="checkbox"/>					

Получить ссылку на отчет можно через меню нотификаций



Выбрать нотификацию Выбрать — "Детали"

**Notifications**

**Triggers**

Status	Read
Notification date	23.09.2020 23:09
Notify type	Warning

Notification content

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostslpsWidget

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)

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

#### HTTP действие

Действия

E-mail	×	Нотификация	×	Http	+
Метод	Урл	<input checked="" type="checkbox"/> Вкл.			
POST	https://your_redmine_host/issues.xml?key=your_redmine_api_key				
Заголовки		<		Тело	>
+					
Имя	Значение	<pre>&lt;?xml version="1.0"?&gt; &lt;issue&gt;   &lt;project_id&gt;1&lt;/project_id&gt;   &lt;subject&gt;Trigger fired: {trigger.name}&lt;/subject&gt;   &lt;priорity_id&gt;1&lt;/priority_id&gt;   &lt;description&gt;Id: {trigger.id}\nTrigger: {trigger.name}\nStatus: {trigger.state}\nSeverity: {trigger.severity}\nQueries: {trigger.queries}\nReasons for the occurrence of notification: {trigger.notification.notes}\nLinks to reports:\n{trigger.report.link}\n\nLinks to files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report.xlsx}\n\n{trigger.report.xlsx}&lt;/description&gt; &lt;/issue&gt;</pre>			
Content-Type	application/xml	<input type="checkbox"/>			

Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)  
 Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

## Пример настройки триггера на поиск цели DDoS-атаки типа Flood

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

### Запросы

Запросы

	Название	Отчет	Период с	Период по	
<input checked="" type="checkbox"/> Вкл.	A	Maxi	сейчас - 15 минут	сейчас	<input type="button" value="Удалить"/>

Условия

Связь	Поле	Оператор	Значение	
<input checked="" type="checkbox"/> Вкл.	Сырой полный нетфлоу	<=	20	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/> И	Таблицы	>=	1500	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/> И	Сырой лог			
	Обнаружение атак			
	Топ прикладных протоколов			
	Топ групп прикладных протоколов			
	Топ абонентов			
	По трафику			
	По флоу			
	По времени жизни сессии			
	По абонентам и хостам			
	Maxi			

Обработка ошибок

Если нет данных \*  
Нет данных

Действия

Нотификация

Кому

в поле отчет выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ абонентов → Maxi

## Условия

Условия

Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
<input checked="" type="checkbox"/> Вкл.	И	A	avg	Флоу к абоне	>=	10000	<input type="button" value="Удалить"/>

Серия — "Объем Flow к абонентам, Пак",  $\geq 10000$



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

# Анализ BotNet

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

## Запросы

Запросы							
		Название		Отчет		Период с	
+ <input checked="" type="checkbox"/>		Вкл.		Maxi		сейчас - 15 минут	
							<input type="button" value=""/>
							<input type="button" value=""/>

- Выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ прикладных протоколов → Maxi для значения "A"
- Сырой полный нетфлоу → Сырой лог → Полный сырой лог для значения "B"

## Условия

Условия							
		Связь		Название		Функция	
+ <input checked="" type="checkbox"/>		Вкл.		B		avg	
						Порт получат =	6667
						Порт источни =	6667
						Порт получат =	1080
						Порт источни =	1080
						Флоу >=	2000

Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "B" со значением "ИЛИ", и Флоу больше или равно 2000.



При этой конфигурации в случае если: хоть на одном из портов (6667/1080) количество проходящих пакетов будет более 2000 в секунду — сработает триггер.



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

# Фиксация перехода абонента на ресурс конкурента

## Общая информация триггера

Общее			
Название триггера *	Интерес к конкурентам	Важность	Триггер
Информация		Выключен	
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	1 час	1	
Дата начала	Дата окончания	Время начала	Время окончания
<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value=""/>

Название триггера «Интерес к конкурентам», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

## Запросы

Запросы						
+						
	Название	Отчет		Период с	Период по	
<input checked="" type="checkbox"/>	Вкл.	A	Сырой кликстрим	<input type="button" value="▼"/>	сейчас - 1 час	<input type="button" value=""/>
<input checked="" type="checkbox"/>	Вкл.	B	Maxi	<input type="button" value="▼"/>	сейчас - 1 час	<input type="button" value=""/>

- Добавить "+" поле
- Название А  
Выбрать таблицу для сканирования: Сырой кликстрим → Таблицы → Сырой кликстрим
- Название В  
Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 1 час», период по : «сейчас»
- В этом случае будет происходить анализ трафика каждый час по выбранным таблицам.

## Условия

Условия								
+								
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
<input checked="" type="checkbox"/> Вкл.	ИЛИ	A	avg		Хост	=	*megafon.ru	
<input checked="" type="checkbox"/> Вкл.	И	B	avg		Объем флоу	>=	800	
<input checked="" type="checkbox"/> Вкл.	ИЛИ	A	avg		Хост	=	*mts.ru	

- Добавить "+" 3 поля
- Первое поле — выбрать таблицу "A"; Связка - "Или"; Функция - "avg"; Серия Хост = \*megafon.ru (или ваш любимый конкурент)
- Второе поле — выбрать таблицу "B"; связка "И"; Функция – "avg"; Серия Объем флоу от абонентов >= 800
- Третье поле — выбрать таблицу "A"; Связка – "Или"; Функция – "avg"; Серия Хост = \*mts.ru



Мы задали условие — для срабатывания триггера необходимо, чтобы было детектировано: не менее 800 пакетов (не случайный а осмысленный переход) от абонента к сайту конкурента.

## Обработка ошибок

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

- В поле "Если нет данных" — Нет данных
- В поле "Если ошибка выполнения или тайм-аут" — Сохранить последнее состояние.



В этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

## Действия

### E-mail действие

**Действия**

**E-mail**

Кому  
your@email.com Вкл.

Тема  
Trigger fired: {trigger.name}

Сообщение

Font Size... Font Family... Font Format...

Id: {trigger.id}  
Trigger: {trigger.name}  
Status: {trigger.state}  
Severity: {trigger.severity}

Queries:  
{trigger.queries}

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты



При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние).

## Нотификация

**Действия**

**E-mail** Нотификация

Заголовок нотификации  
{trigger.name} Вкл.

Подзаголовок нотификации  
{trigger.id} Тип нотификации  
Предупреждение

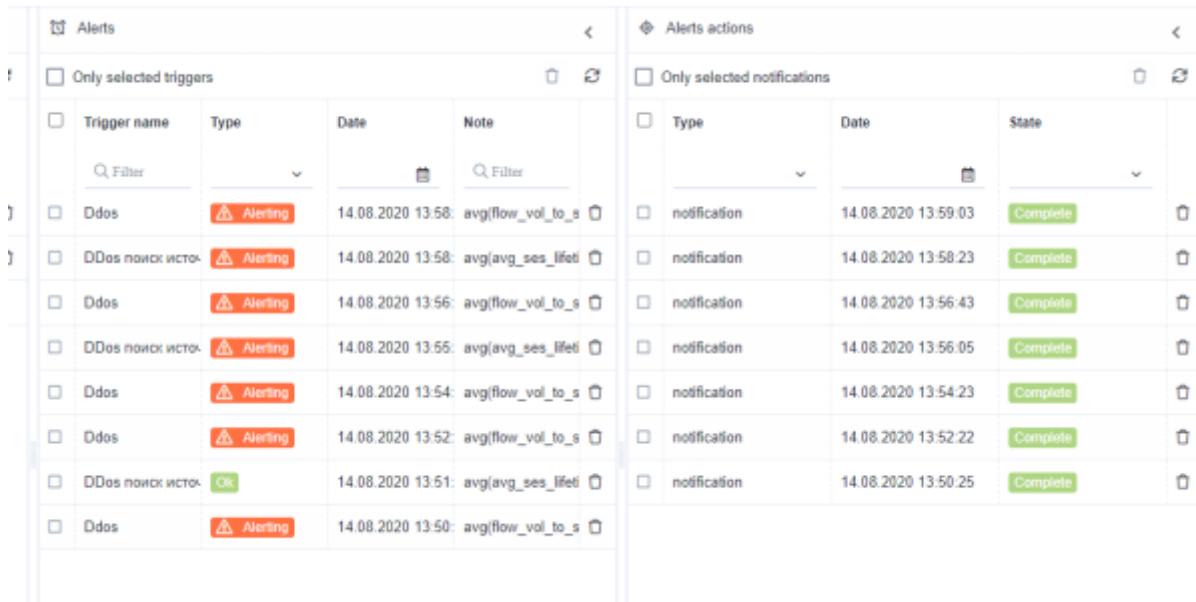
Сообщение

Font Size... Font Family... Font Format...

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

Запросы:  
{trigger.queries}

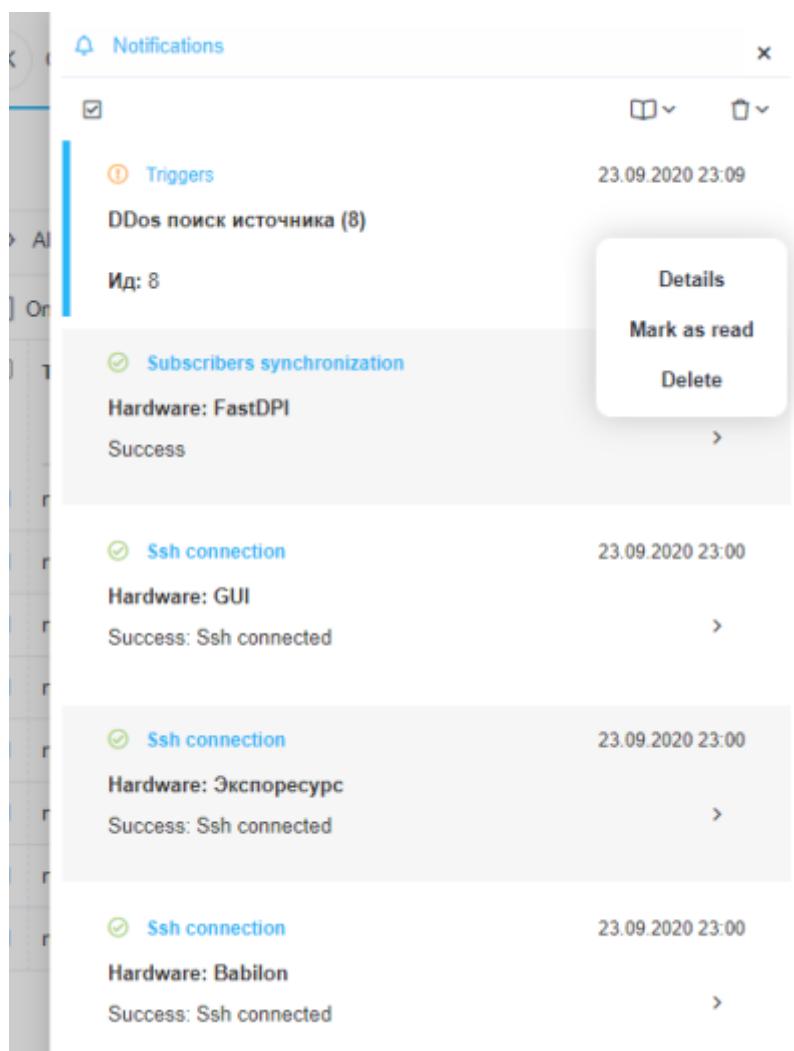
- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ



The image shows two side-by-side tables. The left table is titled 'Alerts' and has columns for 'Trigger name', 'Type', 'Date', and 'Note'. It lists several entries, mostly 'Ddos' triggers with 'Alerting' status. The right table is titled 'Alerts actions' and has columns for 'Type', 'Date', and 'State'. It lists 'notification' entries with various completion states like 'Complete' and 'In progress'.

Alerts				Alerts actions		
Only selected triggers				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 источника	Alerting	14.08.2020 13:58:	avg(avg_ses_lifeti	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 источника	Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti	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 источника	Ok	14.08.2020 13:51:	avg(avg_ses_lifeti	notification	14.08.2020 13:50:25	Complete
Ddos	Alerting	14.08.2020 13:50:	avg(flow_vol_to_s)			

Получить ссылку на отчет можно через меню нотификаций



The image shows a 'Notifications' window with a list of events. A context menu is open over the second event, which is a 'Subscribers synchronization' entry. The menu options are 'Details', 'Mark as read', and 'Delete'.

Trigger	Date
DDos поиск источника (8)	23.09.2020 23:09
Subscribers synchronization	23.09.2020 23:00
Ssh connection	23.09.2020 23:00
Ssh connection	23.09.2020 23:00
Ssh connection	23.09.2020 23:00

Выбрать нотификацию Выбрать — "Детали"

**Notifications**

**Triggers**

Status	Read
Notification date	23.09.2020 23:09
Notify type	① Warning

Notification content

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostslpsWidget

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)

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

#### HTTP действие

Действия

E-mail	×	Нотификация	×	Http	+
Метод	Урл	<input checked="" type="checkbox"/> Вкл.			
POST	https://your_redmine_host/issues.xml?key=your_redmine_api_key				
Заголовки		<		Тело	>
+					
Имя	Значение	<pre>&lt;?xml version="1.0"?&gt; &lt;issue&gt;   &lt;project_id&gt;1&lt;/project_id&gt;   &lt;subject&gt;Trigger fired: {trigger.name}&lt;/subject&gt;   &lt;priорity_id&gt;1&lt;/priority_id&gt;   &lt;description&gt;Id: {trigger.id}\nTrigger: {trigger.name}\nStatus: {trigger.state}\nSeverity: {trigger.severity}\nQueries: {trigger.queries}\nReasons for the occurrence of notification: {trigger.notification.notes}\nLinks to reports:\n{trigger.report.link}\n\nLinks to files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report.xlsx}\n\n{trigger.report.xlsx}&lt;/description&gt; &lt;/issue&gt;</pre>			
Content-Type	application/xml	<input type="checkbox"/>			

json Шаблон по умолчанию

xml Шаблон по умолчанию

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.