# Содержание

OE Triggers & Notifications	3
Purpose of use	3
How to create and configure triggers	3
Step 1. Schedule	3
Step 2: Select a data source and metrics	4
Step 3: Conditions	6
Step 4: Error handling	6
Step 5: Actions	7
"Triggers and Notification" page elements description	LO

# **QoE Triggers & Notifications**

# **Purpose of use**

In the "Triggers and Notification" section you can configure sending periodic reports and operational alerts to Telegram or E-mail and display them in the GUI. When a trigger is activated, you will receive a message with information about the specified event and links to the corresponding reports. By default, there are 4 reports in .csv, .tsv, .xlsx, .pdf formats, but the message template can be edited.



Let's make the settings using two scenarios as an example:

- Periodic report to track the RTT delay from a subscriber. The report will show subscribers whose "RTT from subscriber" value is greater than or equal to 150000 ms. It will be sent on Mondays and Thursdays in Telegram.
- Alert about subscribers being a part of a botnet.
   We will set up a table check once a minute every day. Notification will be sent to your email as soon as at least one infected subscriber is detected in the table.

# How to create and configure triggers

- 1. In the GUI, go to QoE analytics  $\rightarrow$  Triggers and Notification.
- 2. Click the + on the Triggers dashboard to add a trigger. This will open the configuration pop-up window.

It takes 5 steps to create a new trigger. Trigger settings are divided into blocks, you need to fill all of them.

# Step 1. Schedule

Fill in the required fields:

- Name choose any unique name for the trigger.
- Severity select the level of importance: information, warning, medium/high importance. For example, "Information" can be set for a regular report, and all others can be set for different notifications as you see fit. **Optional field.**
- Days of the week on which days of the week the trigger will run.
- Check frequency how often the validation script will be run. For example, if the value "1 min" is set the check script will be run once a minute on the specified days of the week.
- Start and end date and time. Optional fields.

Also in this block there is a switch to enable/disable the trigger. After the configuration is

Trigger name *		Severity	-	Disable
RTT Delay		Information	Trigger	Disable
Days of the week *	Ch	eck frequency *	Number of positives	
Mon, Thu	~ 24	hours	~ 0	
Start date	End date	Start time	End time	
	<b>—</b>	Ċ	0	
n this case, the n Monday and c xample of filling	check script wi once on Thursda g out a block for	Il run on the specifi ay. r notification about	ed days once every subscribers with cyb	24 hours er threats
n this case, the n Monday and c xample of filling Common	check script wi once on Thursda g out a block for	ll run on the specifi ay. r notification about	ed days once every subscribers with cyb	24 hours
n this case, the n Monday and c xample of filling Common	check script wi once on Thursda g out a block for	II run on the specifi ay. r notification about	ed days once every subscribers with cyb	24 hours per threats
n this case, the n Monday and c xample of filling Common Trigger name •	check script wi once on Thursda g out a block for	II run on the specificay. r notification about severity worning	ed days once every subscribers with cyb	24 hours - eer threats
n this case, the n Monday and c xample of filling Common Trigger name • Infected subscribers Days of the week •	check script wi once on Thursda g out a block for	Il run on the specificay. r notification about s Severity Warning eck frequency •	ed days once every subscribers with cyb Trigger Number of positives	24 hours - eer threats
n this case, the n Monday and c xample of filling Common Trigger name • Infected subscribers Days of the week • Mon, Tue, Wed, Thu, Fri	check script wi once on Thursda g out a block for i, sat, sun v 1m	II run on the specificaty.	ed days once every subscribers with cyb Trigger Number of positives	24 hours - ber threats
n this case, the n Monday and c xample of filling Common Trigger name • Infected subscribers Days of the week • Mon, Tue, Wed, Thu, Fri Start date	check script wi once on Thursda g out a block for i, sat, sun ~ 1m End date	II run on the specificay. r notification about severity Warning eck frequency • inute	ed days once every subscribers with cyb Trigger Number of positives 0 End time	24 hours - eer threats

# Step 2: Select a data source and metrics

Select a metric and data table. Triggers only work with ready-made tables found in Netflow and Clickstream, to start customization you need to find a table that has the required metric.

To create a query, click on the + under the block name.

- Report select a table with data from the ready-made reports of the system, which are analyzed.
- "Period from" and "-to". For example, if you need to analyze data for the last 24 hours, set "Period from" 24 hours, "Period to" now.



The value "Now" in the query parameters "Period from" and "Period to" means when the trigger is started. It is summarized from the "Days of Week" and "Check Frequency" values from step 1.

For each request, you can create a filter where you can set the value of IP host, subscriber login, etc. For example, you can customize the generation of a report or notification for one specific host, if you

#### set the filter like this:

Queries											-		
Ŧ	Query name	Report				Period	from		Period to				
🛛 On	A	Top subscribe	ers with high F	RTT	7	ø	II	Filters	5				<
						Saved	+						
Condition	5					filters			Filter	Operator	Value		
+								Off	Host	like	google.com	0	Û
	Bind	Query name	Function	Combinator	Serie			Off	Subscriber	like		0	Û
On	AND	A	any	if is not NaN	RTT from			Off	Login	like		0	Û
								Off	Host IP	like		0	Û
o data &	error handling							Off	Protocol	like		0	Û
if no dat Ok	a •			lfe ∽ Ale	execution e			Off	App protocols gr	in			Û
								Off	Application proto	like		0	Û
								Off	Source AS numbe	like		0	Û
ctions								Off	Destination AS nu	like		0	Ô
E-m	ail ×	Telegram	×					Off	Host category	in			Û
Chat Id						•		Off	Infected traffic c	in			Û
Chat Id 36891300 Message	05					•		Off	Infected traffic c	in	Cancel	Apply	Û

Example of filling out a block for a report to track RTT delay from a subscriber. Here you need to select the report "Top subscribers with high RTT", it has the required metrics for this trigger. Since you want the report to come on Mondays and Thursdays, "Period from" should be set equal to the interval between these days – "Now – 4 days", the data for the last 4 days will be analyzed.

Qu	eries						•
+							
		Query name	Report		Period from	Period to	
	On	А	Top subscribers with high RTT	7	now - 4 days	now	Û

Example of filling out the block for notification about subscribers with cyber threats. Here you need to select the report "Top infected subscribers with botnet traffic", it has the required metrics for this trigger. In this case, the data for the last 24 hours will be analyzed.

Queries						•
+						
	Query name	Report		Period from	Period to	
🗹 On	A	Top infected subscribers with botnet botnet	7	now - 24 hours	now	Û

# **Step 3: Conditions**

Set conditions – what should happen to the metric to run the trigger.

To create a condition, click the + below the block name.

For each condition, you need to configure the following parameters:

- AND/OR relationship compare with the names of requests for fulfillment of either several conditions at once or at least one of the specified conditions.
- Name select one of the created requests.
- Function select the type of aggregate function to be applied to the values in the condition:
  - $\,\circ\,$  "count" counts the number of items or records in the dataset,
  - $\circ\,$  "any" returns any value available in the dataset,
  - $\circ\,$  "anyLast" returns the last value available in the dataset,
  - $\circ\,$  "avg" calculates the average value of the numeric data in the dataset,
  - $\circ\,$  "min" returns the minimum value from the available data in the dataset,
  - $\circ\,$  "max" returns the maximum value from the available data set,
  - $\circ$  "sum" calculates the sum of the numeric data in the set,
  - "uniq" returns unique values in the dataset, removing duplicates.
- Combinator select a non-numeric/non-zero/numeric/zero value or leave blank.
- Series select the desired metric from the report.
- Operator select: =, !=, >, >=, <, ←, between (will return records where the expression is between value1 and value2 inclusive),, not between (returns all records where the expression is NOT between value1 and value2 inclusive).
- Value assign the required value for the condition.

c	ondition	S								-
+	F									
		Bind	Query name	Function	Combinator	Serie		Operator	Value	
	On	AND	A	any	if is not NaN	RTT from sub	scriber, ms	>=	150000	Û
or Ex	equa ample	l to 150 e of fillir	000 ms in t ng out the b	he table block for	from step alerts abou	2. ıt subscri	bers with	n cyber t	hreats:	
or Ex	equa ample condition	l to 150 e of fillir s	000 ms in t ng out the b	he table block for	from step alerts abou	2. ıt subscri	bers with	n cyber t	hreats:	•
or Ex	equa ample condition	l to 150 e of fillir	000 ms in t ng out the k	he table	from step alerts abou	2. ıt subscri	bers with	n cyber t	hreats:	•
or Ex	equa ample condition	l to 150 e of fillir s Bind	out the k	he table block for	from step alerts abou	2. ut subscri serie	bers with	value	hreats:	•
or Ex	equa ample	l to 150 e of fillir	000 ms in t ng out the b	he table block for	from step alerts abou	2. ıt subscri	bers with	n cyber t	hreats	:

### Step 4: Error handling

Set the trigger behavior when errors occur.

Select one of the values in the "If there is no data" and "If there is a runtime error or timeout" fields:

- "Notification" there is the condition specified in the trigger.
- "No data" no data is found when processing the reports set in the trigger.
- "Save last condition" no action needed.
- "Ok" the conditions set in the trigger did not work, everything is fine, and no actions needed.

	No data & error handling		
	If no data *	If execution error or timeout *	
1	Ok	<ul> <li>Alerting</li> </ul>	

### **Step 5: Actions**

Setting up an action will allow you to receive a message to E-mail or Telegram in case of triggering. To create an action, press + under the block name.

To delete an action, press  $\times$  next to the action name.

#### Telegram

#### Step 1: Register your bot via <a href="https://t.me/BotFather">https://t.me/BotFather</a>.

- 1. Start BotFather with the /start command.
- 2. Type / newbot to create a new bot.



4. Enter a unique username (Latin only, ending in "bot").

![](_page_7_Picture_0.jpeg)

- 5. Copy the HTTP API access token from the bot registration message, it looks like this: 5995002635:AAGdSR0udY9K9uxENaPu2HF4azmpsKQq98X
- 6. Paste the copied token into the GUI settings (Administrator → GUI Configuration → Telegram Settings → Telegram bot API token).

	VAS Experts	=	Administrator > GUI configuration	
Sec	rch	х	11 Sorve 12, D	
4	QoE analytics	~	Settings Common	Telegram settings
$\bigcirc$	VAS cloud services	~	Jobs intervals and periods	Telegram bot API token (TELEGRAM_BOT_API_TOKEN) 6195306860:AAH5tQwZiqtXRwrpwCSEkITT2P4ND452Kmc
-0-	Lawful interception	~	QoE Stor: DB (Clickhouse) connection	4
~			QoE Stor: Raw log aggregation settings	
20	Administrator	^	QoE Stor: DB lifetime settings	
	Equipment		QoE Stor: Discs settings	
	Users		SMTP settings	
	Roles		System	
	Users actions log		DB (MySql) connection	
	GUI configuration		Uir settings	
	GUI logs		Push notifications settings	
	GUI update		Lawful interception	
			SSO authorization settings	
	QoE Stor configuration		Maps settings	
	QoE Stor logs		VasCloud settings	
	Captcha configuration		Cluster settings	
	Captcha template		Bockup settings	
	Captcha logs		Backup auto restoration settings	
>_	Hardware SSH terminal	~	Telegram settings	
			Trigger settings	

### Step 2: Get a chat ID for your personal Telegram account via https://t.me/RawDataBot

To get chat ID, user must have username in Telegram profile!

- 1. Start Telegram Bot Raw with the /start command.
- 2. Copy the ID, it looks like this:

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

},

### Step 3: Connect Telegram to the configured trigger

Add the ID from step 2 to the Telegram action in the "Chat ID" field.

![](_page_8_Figure_3.jpeg)

### E-Mail

Creates a notification and sends it to the specified e-mail address.

- 1. If the "Message" field is not filled in click on the "Set default template" button (1) to fill the action fields with default values. If necessary, all values can be edited.
- 2. If you click on the "Template parameters" button (2), it will open a menu with identifiers that can be used to compose the message.

Actions	•
E-mail × Telegram ×	+
Send to	On
name@mail.com	
Subject	
Trigger's been triggered: {trigger.name}	2
Message	1
B I U 書 書 書 目 日 Font Size > Font Family. > Font Format > 運 運 夢 馬 吗 会 参 ② X <sub>1</sub> x <sup>2</sup> S /落	≅ ⊒
Id: {trigger.id}	
Trigger: {trigger.name}	
Status: {trigger.state}	
Severity: {trigger.severity}	
<b>B</b> under	
Quenes:	•
{trigger.queries}	2

For E-mail actions to work, you need to configure SMTP. Go to Administrator  $\rightarrow$  GUI Configuration, select "SMTP Settings".

#### **GUI Notifications**

Notification can be used to test the functionality of triggers.

1. Click on the "Set default template" button (1) to fill the action fields with default values. All

values can be edited if necessary.

2. Clicking on the "Template Options" button (2) opens a menu with identifiers that can be used to compose the message.

Notification ×		+
lotification title		On
{trigger.name}		
Notification subtitle	Notification type	
{trigger.id}	Warning	2、~
Message		1
B I U 🗟 🗟 🗃 🗮 🗄 Font Size 🗸 Fon	t Family. 👻 Font Format 👻 🕃 🕃 📝 ቘ 🗠 🏟 🍛 🍙 X <sub>2</sub> 🗴 🛠 🏂	= 📖
Id: {trigger.id}		
Trigger: {trigger.name}		
Status: {trigger.state}		
Severity: {trigger.severity}		
Queries:		

After creating a trigger, click "Save". On the "Triggers" dashboard, enable the necessary triggers. If the GUI page has not been refreshed – refresh the page in the browser or click the "Refresh" button.

4	frigger	5					<	Ŭ	Alerts				<	۰	Alerts actions				<
+	Ð					Û	2		Only selected trigg	gers		Û	e		Only selected notification	s		Û	C
		Trigger	Days of	Check	Trigger type	State			Trigger name	Туре	Date	Note			Туре	Date	State		
		Q, Filter	~	~	~	~			Q, Filter	~	Ö	Q, Filter			~	0		~	
	0 2	RTT Delay	Mon,Thu	24 hours	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:29:02	anyIf(rtt_from_su	Û		notification	30.06.2023 17:36:23	Complete		Û
	0	Infected su	Mon,Tue,We	1 minute	Custom	Ready	٥		RTT delay	Ok	11.07.2023 18:25:24	anylf(rtt_from_su	0		telegram	29.06.2023 18:24:04	Complete		Û
	O Ø	Топ абонен	Mon,Tue,We	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:21:24	anyif(rtt_from_su	Û						
	o Ø	Тест	Thu	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:17:45	anyif(rtt_from_su	Û						
	0	Дельта пак	Fri	1 minute	Custom	Ready	٥		RTT delay	Ok	11.07.2023 18:12:03	anylf(rtt_from_su	0						
	0	test2	Mon	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:08:04	anyif(rtt_from_su	Û						
	0	test	Mon	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:03:45	anyIf(rtt_from_su	Û						
									RTT delay	Ok	11.07.2023 17:55:23	anyIf(rtt_avg,isNa	٥						
									Топ абонентов	Alerting	30.06.2023 17:31:43	maxIf(traffic,isNa	Û						
									Топ абонентов	Alerting	29.06.2023 18:19:03	maxIf(traffic,isNa	Û						
									Топ абонентов	Alerting	29.06.2023 18:00:4	maxIf(traffic,isNa	0						
									Топ абонентов	Alerting	29.06.2023 17:41:07	maxIf(traffic,isNa	Û						
									Топ абонентов	Alerting	29.06.2023 17:22:03	maxIf(traffic,isNa	0						
									test	Keep last state	29.05.2023 14:31:02	Error: Unknown err	0						
									test	Keep last state	29.05.2023 14:28:43	Error: Unknown err	Û						

# "Triggers and Notification" page elements description

Go to QoE Analytics  $\rightarrow$  Triggers and Notification. This will open the section as shown in the image below.

стоян	MP 00		Ch 2741 JHER >	+	Состояние по	одписк	И						E	сли	в триггере в	ыбрано действ	зие 🦯	
													"H	юти	фикация", он	а хранится зд	есь	
Три	rrepe	Добави	ть тригі	гер			<	10	Нотификации				<	۲	Действия			<
E						Û	Ø		Только выбранные т	риггеры		C	Ø		Только выбранные н	отифика		0 8
		Название	Дни	Частота	Тип триггера	Статуо		2	Название триггера	Тип	Дата	Заметка			Тип	Дата	Статуо	
		Q, Фильтр	<b>~</b>	~	~	v			Q. Фильтр	v	Ö	Q, Фильтр			v	0		~
Φ		Топ абонент	Пн,Вт,Ср,Чт	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотификация	30.06.2023 17:31:43	maxIf(traffic,is)	ioN 🗍		notification	30.06.2023 17:36:23	Завершено	ſ
Ø		Тест	Чт	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотификация	29.06.2023 18:19:03	maxIf(traffic,is)	aN 🖞		telegram	29.06.2023 18:24:04	Завершено	r
Φ		Дельта паке	Пт	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотификация	29.06.2023 18:00:43	maxIf(traffic,isN	IaN 🗊		Спис	ок действий п	о нотифик	ациям
Ø		test2	Пн	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотификация	29.06.2023 17:41:07	maxIf(traffic,is)	aN 🖞					
Φ		test	Пн	1 минута	Пользовательский	Готов	Û		Топ абонентов	🛆 Нотификация	29.06.2023 17:22:03	maxIf(traffic,is)	oN 🗊					
					Список	григгер	ров			Список і	нотификаций	по тригге	рам					
		1 > >>			На странице	100	~		< 1 2 3	4 5 >	>> На ст	ранице 100	~		< 1 > >	> Ho	а странице 1	00

This section contains three sections:

- List of the triggers.
- List of the notifications.
- List of actions performed by triggers as a result of notifications.

Types of triggers:

- System. These are set by the vendor and can only be enabled/disabled.
- Custom. User-defined and can be freely configured.

For a detailed description of configuring a trigger, see How to create and configure triggers.