# Содержание

OE Triggers & Notifications	3
Purpose of use	3
How to create and configure triggers	3
Step 1. Schedule	
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 * RTT Delay		Severity Information	Trigger	Disabled
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>	Ö	O	C
n Monday and o xample of filling	nce on Thursd	ay.	ed days once every subscribers with cyb	
n Monday and o	nce on Thursd	ay.		
n Monday and o xample of filling	nce on Thursd	ay.	subscribers with cyb	er threats:
n Monday and o xample of filling <sup>Common</sup>	nce on Thursd	ay. r notification about		
n Monday and o xample of filling Common Trigger name •	nce on Thursd	ay. r notification about Severity	subscribers with cyb	er threats:
n Monday and o xample of filling Common Trigger name • Infected subscribers	out a block fo	ay. r notification about Severity Warning	subscribers with cyb	er threats:
n Monday and o xample of filling Common Trigger name • Infected subscribers Days of the week •	out a block fo	ay. r notification about Severity Warning eck frequency •	subscribers with cyb	er 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 query, 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										-				
+														
	Query name	Report				Period f	from	F	eriod to					
🗹 On	A	Top subscribe	ers with high F	RTT	7	8	IШ	Filters					<	e
						Saveo	+							TISU0
Condition	5					Saved filters			Filter	Operator	Value			
+						Ĩ		Off	Host	like	google.com	0	Û	
	Bind	Query name	Function	Combinator	Serie			Off	Subscriber	like		0	Û	1
🗹 On	AND	A	any	if is not NaN	RTT from			Off	Login	like		0	Û	
No data P	error handling							Off	Host IP	like		0	Û	
	-							Off	Protocol	like		0	Û	
If no dat Ok	0 *			lf e ∽ Ale	execution e erting			Off	App protocols gr	in			Û	
					-			Off	Application proto	like		0	Û	
Actions								Off	Source AS numbe	like		0	Û	
	ail × lia		×					Off	Destination AS nu	like		0	Û	
E-mo	- ni	Telegram						Off	Host category	in			Û	
Chat Id 36891300	35					•		Off	Infected traffic c	in			Û	4

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.

Que	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.

	Que	ries							•
	+								
			Query name	Report		Period from	Period to		
6	2	On	A	Top infected subscribers with botnet botnet	7	now - 24 hours	now	1	Ū

# **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 queries for fulfillment of either several conditions at once or at least one of the specified conditions.
- Name select one of the created queries.
- 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.

	Condition	ns								•
	+									
		Bind	Query name	Function	Combinator	Serie		Operator	Value	
	🗹 On	AND	A	any	if is not NaN	RTT from sul	bscriber, ms	>=	150000	Û
2	or equa	l to 150	e trigger wi 1000 ms in t ng out the t	he table	from step	2.			J	er tha
2	or equa	ll to 150 e of filli	0000 ms in t	he table	from step	2.			J	er tha
P	or equa Exampl	ll to 150 e of filli	0000 ms in t	he table	from step	2.			J	er tha
	or equa	ll to 150 e of filli	0000 ms in t	he table	from step	2.			J	er tha

## 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**

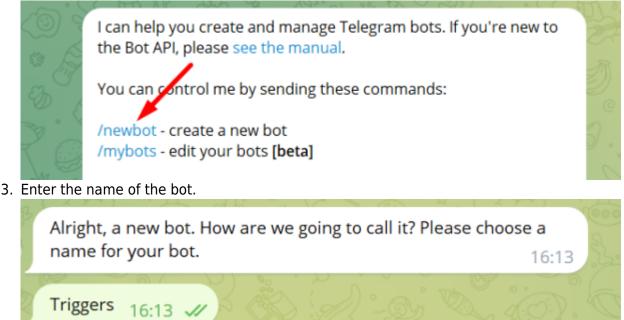
Setting up an action will allow you to receive a message to E-mail or Telegram in case of triggering. To create an action, press + under the block name.

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").



- 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).

$\checkmark$	VAS Experts	≡	Administrator > GUI configuration	
Sec	arch	х	D Save 12 D	
*	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	•
~			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		Ulr 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!

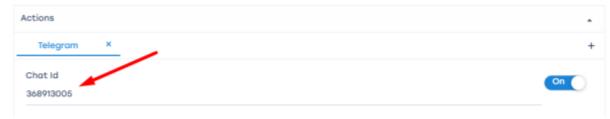
- 1. Start Telegram Bot Raw with the /start command.
- 2. Copy the ID, it looks like this:

```
"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.



### 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 name@mail.com	On
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 陽 % 会 ② ③ X <sub>i</sub> X <sup>2</sup> S 復 3	2 🖂
Id: {trigger.id}	
Trigger: {trigger.name}	
Status: {trigger.state}	
Severity: {trigger.severity}	
Queries:	
{trigger.queries}	0

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 ×		+
Notification title		On
{trigger.name}		
Notification subtitle	Notification type	
{trigger.id}	Warning	2、~
Message		1
B I U 🗟 🗟 🗃 🗮 🗄 Font Size 🗸 Fon	t Family. 👻 Font Format 👻 🕃 🕃 📝 통 🗠 🏟 🎒 🎴 X, 🗴 🛠 🎉	= 📖
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.

¢τ	rigg	gers						<	Ø	Alerts				4	Alerts actions			<
+	Ð						Û	C		Only selected trigg	jers		÷	3	Only selected notification	s		Û Â
			Trigger	Days of	Check	Trigger type	State			Trigger name	Туре	Date	Note	C	Туре	Date	State	
			Q Filter	~	~	~	v			Q, Filter	~	Ö	Q Filter		~			~
1	Φ		RTT Delay	Mon,Thu	24 hours	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:29:02	anyIf(rtt_from_sul		notification	30.06.2023 17:36:23	Complete	1
•	Φ		Infected su	Mon,Tue,We	1 minute	Custom	Ready	٥		RTT delay	Ok	11.07.2023 18:25:24	anylf(rtt_from_sul		telegram	29.06.2023 18:24:04	Complete	1
1	Φ	2	Топ абонен	Mon,Tue,We	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:21:24	anylf(rtt_from_sul	2				
1	Φ	ø	Тест	Thu	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:17:45	anylf(rtt_from_sul	0				
1	٥	Z	Дельта пак	Fri	1 minute	Custom	Ready	٥		RTT delay	Ok	11.07.2023 18:12:03	anylf(rtt_from_sul	0				
	Φ	2	test2	Mon	1 minute	Custom	Ready	Û	٥	RTT delay	Ok	11.07.2023 18:08:04	anyif(rtt_from_sul	0				
	Φ	Ø	test	Mon	1 minute	Custom	Ready	Û		RTT delay	Ok	11.07.2023 18:03:45	anylf(rtt_from_sul	0				
										RTT delay	Ok	11.07.2023 17:55:23	anylf(rtt_avg,isNa	0				
										Топ абонентов	Alerting	30.06.2023 17:31:43	maxIf(traffic,isNat	0				
										топ абонентов	Alerting	29.06.2023 18:19:03	maxIf(traffic,isNat	Û,				
										Топ абонентов	Alerting	29.06.2023 18:00:4	maxIf(traffic,isNat	0				
										Топ абонентов	Alerting	29.06.2023 17:41:07	maxIf(traffic,isNaf	0				
										топ абонентов	Alerting	29.06.2023 17:22:03	maxIf(traffic,isNaf	Ċ				
										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	3				

# "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.

		on" action is sele gger, it is stored	If the "Notificatio in the trig	lf									status	Ibscription	Su Su	27 DAYS 🗸 🕇	itus: REMAIN 27	ption st	ubscr
			Alerts actions	۰	<					lerts	ত্র	<				ager	Add trig	ggers	Tr ل
Ŭ,		IS	Only selected notification		0 8				gers	nly selected trig		0 0	Û					2	+ *
	State	Date	Туре			Note	Date		Туре	Trigger name			State	Trigger type	Check	Days of	Trigger		כ
v		0	~		er	C Q.Fi	c	~		Q, Filter		,	~	~	~	~	Q, Filter		
	Complete	30.06.2023 17:36:23	notification		rtt_from_sul 🖞	29:02 anylf	11.07.2023 18:29		OK	RTT delay		Û	Ready	Custom	24 hours	Mon,Thu	RTT Delay		0
	Complete	29.06.2023 18:24:04	telegram		tt_from_sul 📋	25:24 anylf	11.07.2023 18:25		Ok	RTT delay		Û	Ready	Custom	1 minute	Mon,Tue,We	Infected su		0
on l	Alerts acti				rtt_from_sul 🗊	21:24 anylf	11.07.2023 18:21		Ok	RTT delay		Û	Ready	Custom	1 minute	Mon,Tue,We	Топ абонен		0
					tt_from_sul 🗍	:17:45 anylf	11.07.2023 18:17		Ok	RTT delay	0	Û	Ready	Custom	1 minute	Thu	Тест		0
					tt_from_sul 🗍	12:03 anylf	11.07.2023 18:12		Ok	RTT delay		Û	Ready	Custom	1 minute	Fri	Дельта пак		0
					rtt_from_sul 🖞	:08:04 anylf	11.07.2023 18:08		Ok	RTT delay		Û	Ready	Custom	1 minute	Mon	test2		0
					tt_from_sul 🗍	:03:45 anyIf	11.07.2023 18:03		Ok	RTT delay		Û	Ready	Custom	1 minute	Mon	test		0
					tt_avg,isNa 🖞	55:23 anylf	11.07.2023 17:55		Ok	RTT delay	٥	rs list	Trigger						
					traffic,isNat 📋	7:31:43 maxi	30.06.2023 17:3	9	Alerting	Топ абонентов									
					traffic,isNat 📋	8:19:03 maxi	29.06.2023 18:1	9	Alerting	Топ абонентов	0								
					traffic,isNat 📋	8:00:45 maxi	29.06.2023 18:0	9	Alerting	Топ абонентов									
					traffic,isNat 🗍	7:41:07 maxi	29.06.2023 17:4	9	Alerting	Топ абонентов									
					traffic,isNaf 🖞	7:22:03 maxi	29.06.2023 17:2	9	Alerting	Топ абонентов									
					r alerts list	Trigge													

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.