ДЗ-06: ELK

#### Установка Elasticsearch

https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html

Authentication and authorization are enabled.

TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : 10DM27XoI52iiDxXZa78

If this node should join an existing cluster, you can reconfigure this with

'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'

after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with

'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with

'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with

'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

----------------------------------------------------------------------------------------------

### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd

sudo systemctl daemon-reload

sudo systemctl enable elasticsearch.service

### You can start elasticsearch service by executing

sudo systemctl start elasticsearch.service

/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

eyJ2ZXIiOiI4LjEyLjIiLCJhZHIiOlsiMTkyLjE2OC4wLjEyMTo5MjAwIl0sImZnciI6ImFmOTQyNDViZDg1NWIwN2Q5NTQ1YzM3N2NiNmNiOWVhMTg5NmNjNTE4Njc5NDBjZmQ2ZmNhMmZlMTM5ZWJiNDMiLCJrZXkiOiJIVmFFYW80QktoYnllcDI5T1dDSDpSbmNVMGQ4dFJLcTJIRnJNdHZTMVV3In0=

/usr/share/kibana/bin/kibana-verification-code

/etc/logstash/logstash.yml

xpack.monitoring.enabled: true

xpack.monitoring.elasticsearch.url: http://X.X.X.X:9200

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable kibana.service

Kibana can be started and stopped as follows:

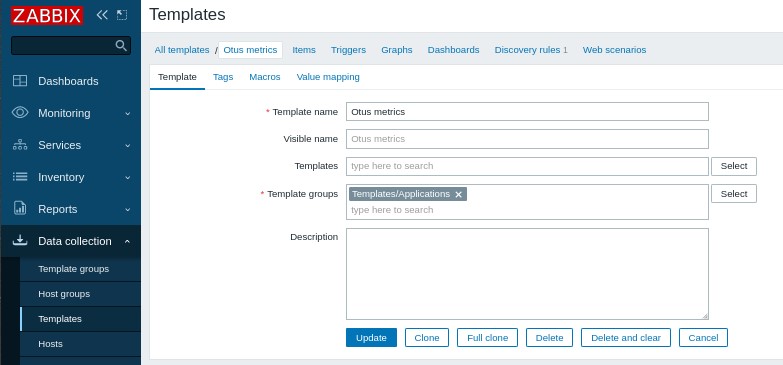
sudo systemctl start kibana.service

sudo systemctl stop kibana.service

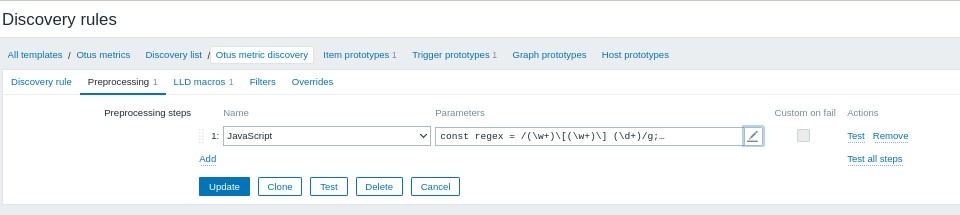
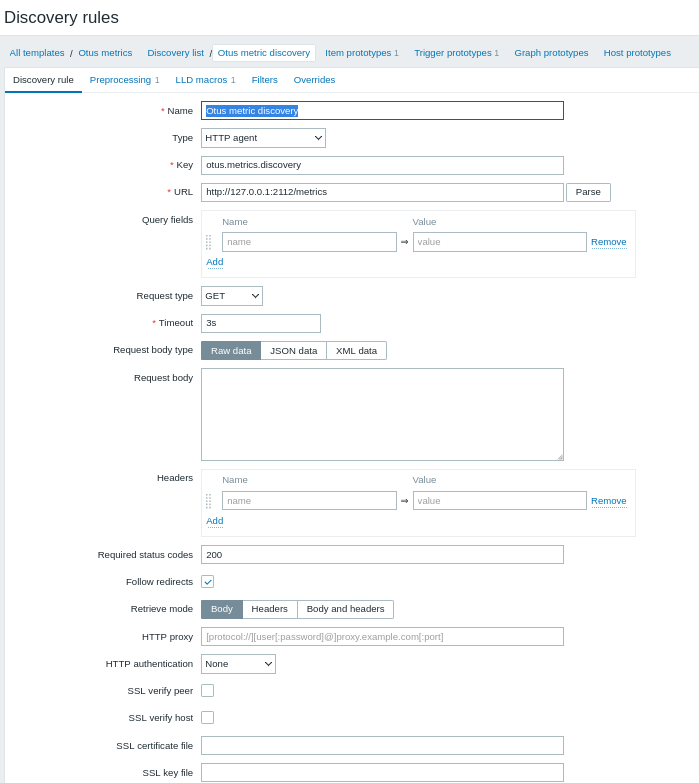
localhost:5601

**Настройка шаблона (LLD)**

Создание шаблона



Правило обнаружения



Препроцесинг при помощи JS:

const regex = /(\w+)\[(\w+)\] (\d+)/g;

var match;

var lines = [];

while ((match = regex.exec(value)) !== null) {

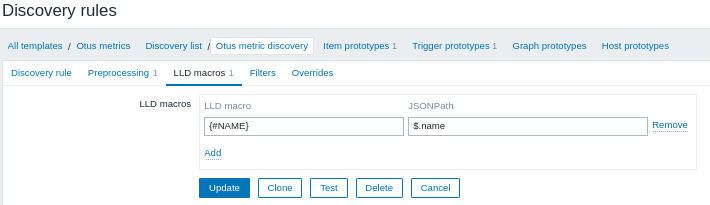
const name = match[2];

const val = match[3];

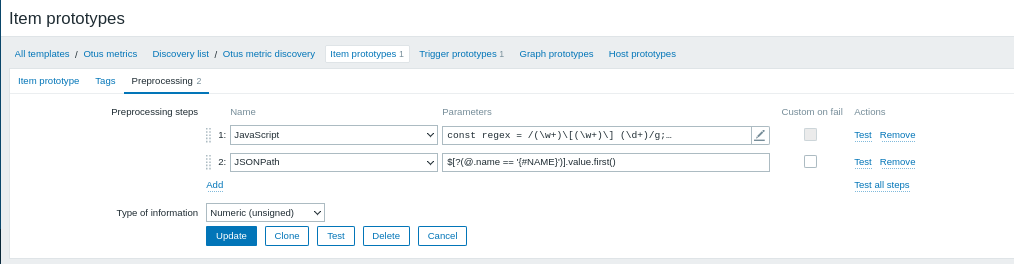
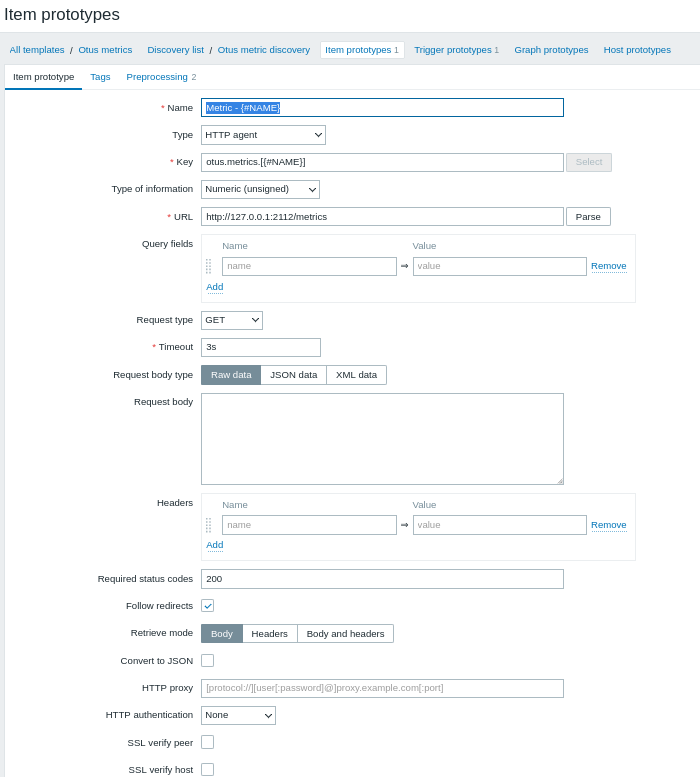
lines.push({ name, value: Number(val) });

}

return JSON.stringify(lines);

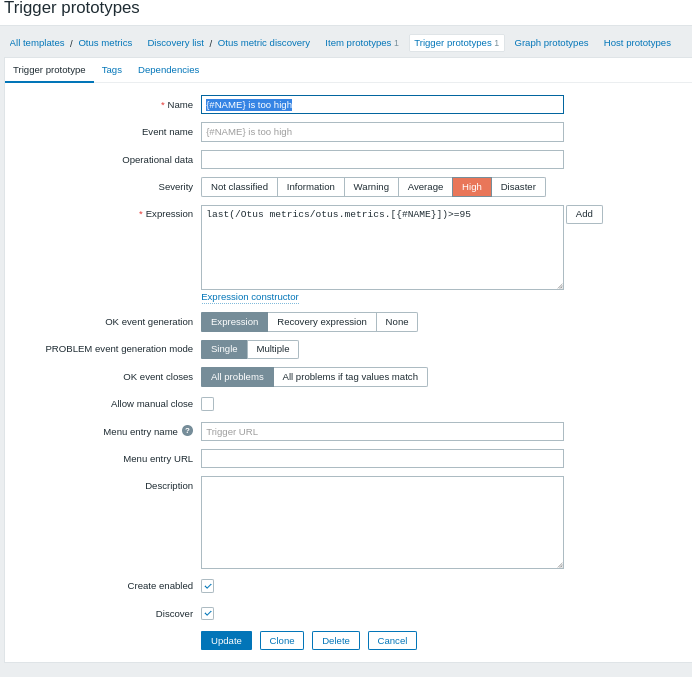


Прототип итема



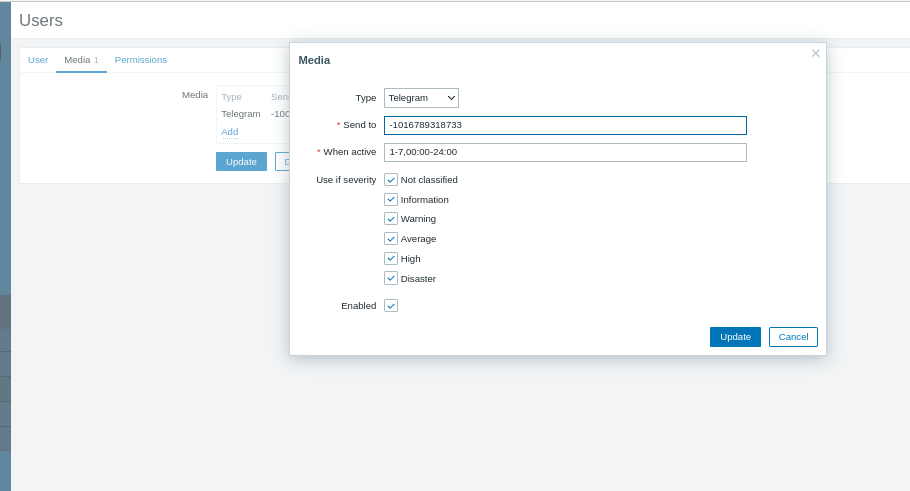
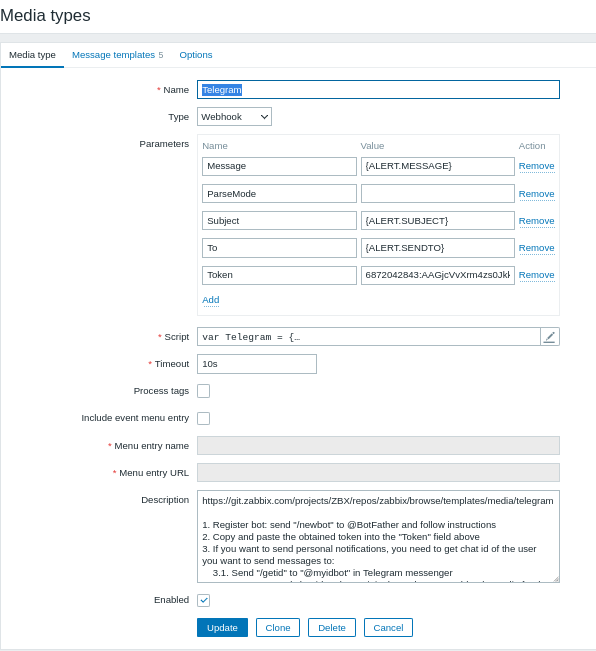
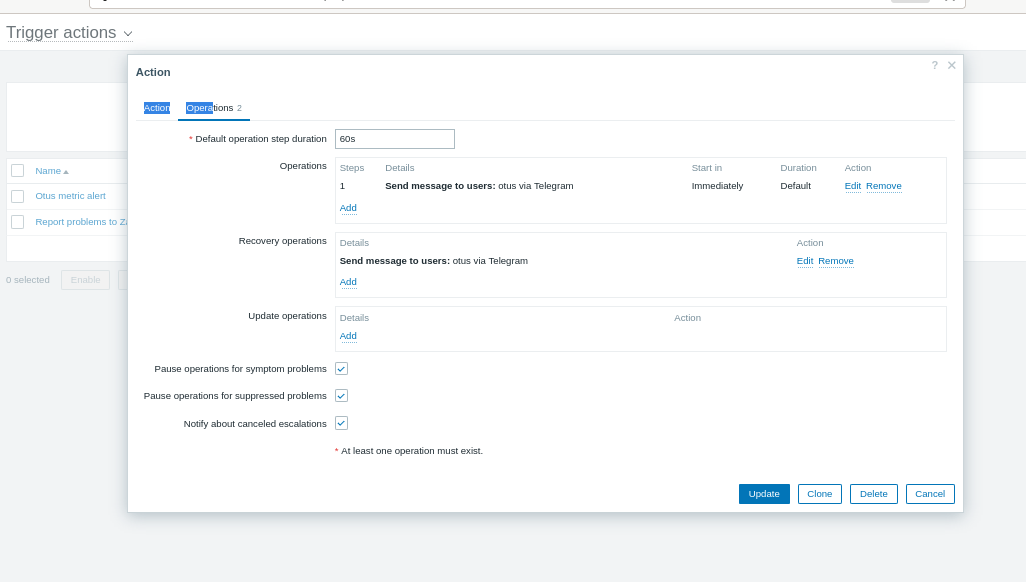
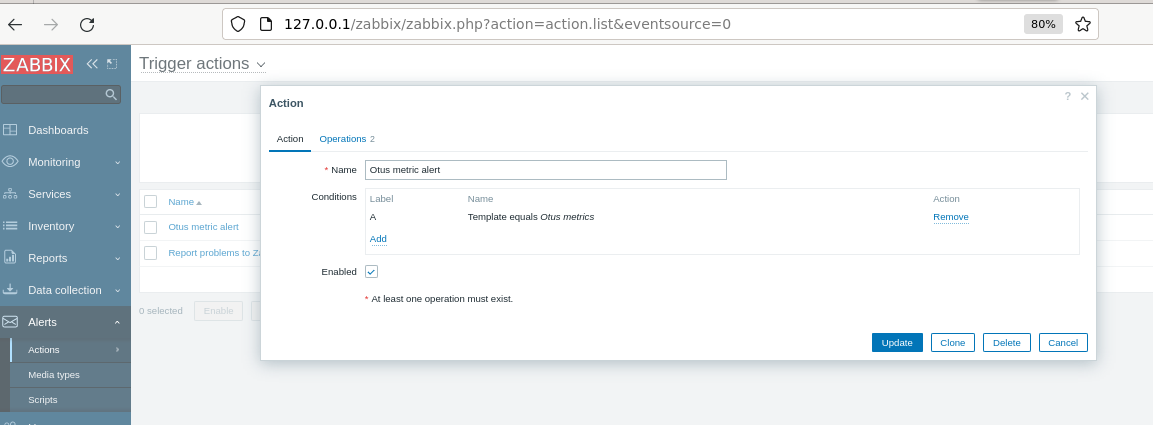
Тайкой же JS скрипт как выше + берем значение нужной метрики.

Триггер

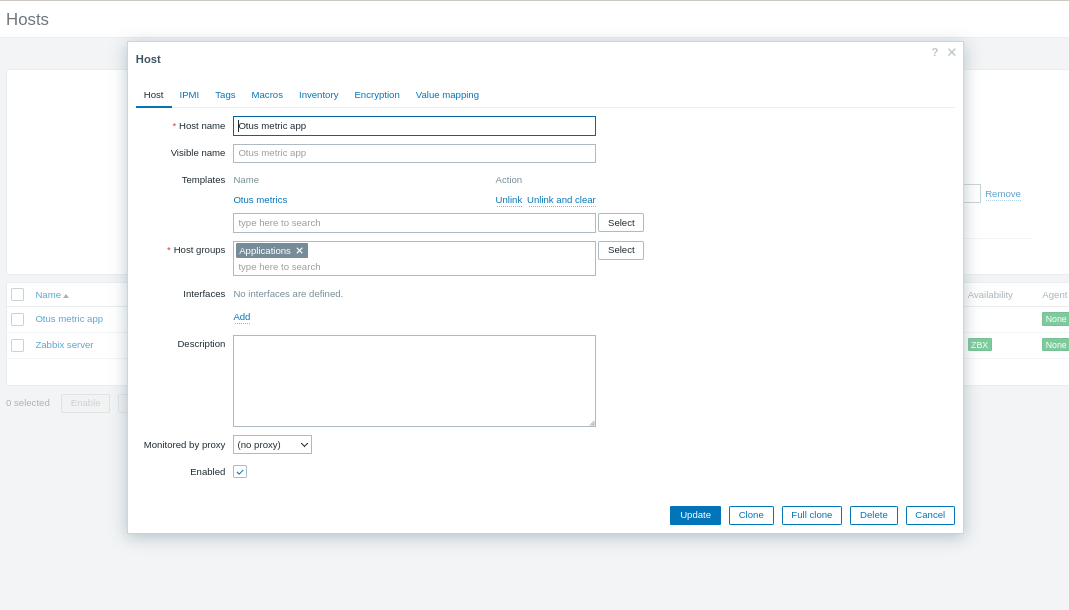


Алерт

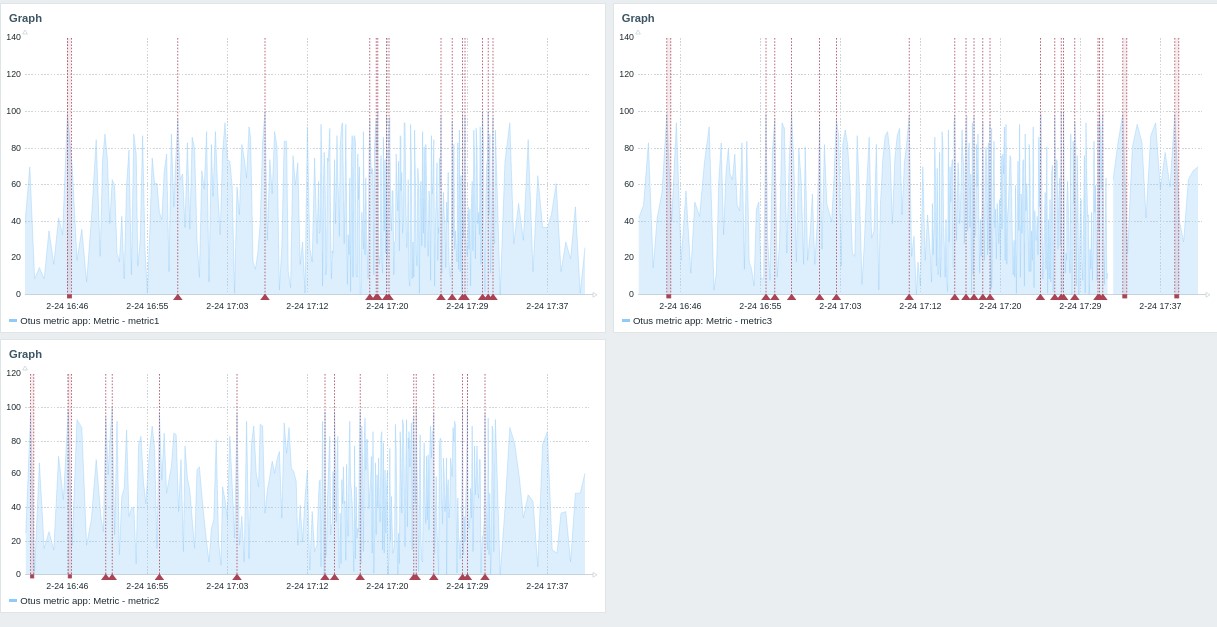
У пользователя должны быть права на чтение host’a.



Хост



**Дашбоард**



**Телеграм**

