# **Задание 1**

Установите и запустите Elasticsearch, после чего поменяйте параметр cluster\_name на случайный.

*Приведите скриншот команды 'curl -X GET 'localhost:9200/\_cluster/health?pretty', сделанной на сервере с установленным Elasticsearch. Где будет виден нестандартный cluster\_name*.

# **Решение 1**

Запущено в докере через такой компоуз:

version: '3'

services:

elasticsearch:

image: docker.elastic.co/elasticsearch/elasticsearch:7.10.0

container\_name: elasticsearch

environment:

- discovery.type=single-node

ports:

- "9200:9200"

- "9300:9300"

networks:

- esnet

volumes:

- ./elasticsearch/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml:ro

networks:

esnet:

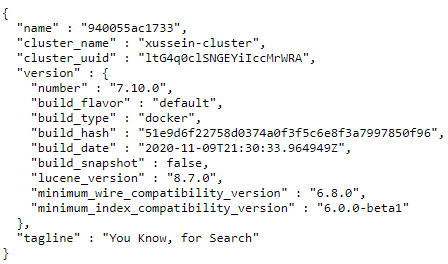
driver: bridge

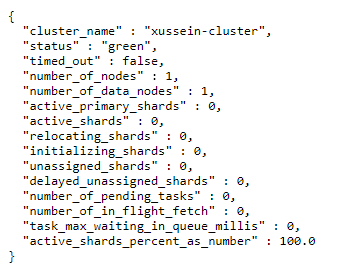
Сам файл конфига:

cluster.name: "xussein-cluster"

network.host: 0.0.0.0

Результат при переходе извне на хост:





# **Задание 2**

Установите и запустите Kibana.

*Приведите скриншот интерфейса Kibana на странице http://<ip вашего сервера>:5601/app/dev\_tools#/console, где будет выполнен запрос GET /\_cluster/health?pretty*.

# **Решение 2**

Добавил в компоуз файл такую конфигурацию кибаны:

kibana:

image: docker.elastic.co/kibana/kibana:7.10.0

container\_name: kibana

ports:

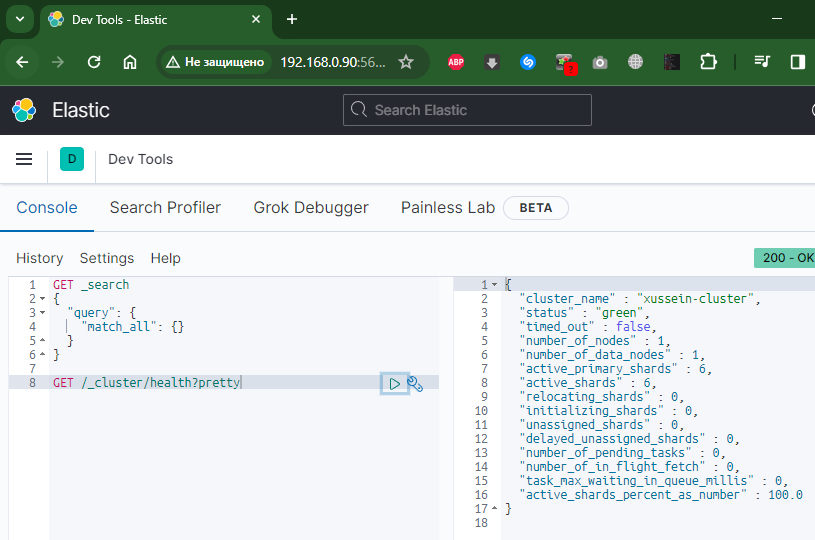
- "5601:5601"

networks:

- esnet

Конфиг пока не трогал, настроек по-умолчанию достаточно.

Требуемый результат в кибане от эластика:



# **Задание 3**

Установите и запустите Logstash и Nginx. С помощью Logstash отправьте access-лог Nginx в Elasticsearch.

*Приведите скриншот интерфейса Kibana, на котором видны логи Nginx.*

# **Решение 3**

Добавил в компот такое:

logstash:

image: logstash:7.16.2

container\_name: logstash

ports:

- "5044:5044"

- "9600:9600"

volumes:

- ./logstash/pipelines/service\_stamped\_json\_logs.conf:/usr/share/logstash/config/pipelines/service\_stamped\_json\_logs.conf:ro

- ./logstash/logstash.yml:/usr/share/logstash/config/logstash.yml:ro

- ./logstash/pipelines.yml:/usr/share/logstash/config/pipelines.yml:ro

- /var/log/nginx/netology.example.local.log:/var/log/nginx/netology.example.local.log

networks:

- esnet

Прокидываю файлик лога в контейнер.

pipelines.yml:

- pipeline.id: service\_stamped\_json\_logs

pipeline.workers: 1

pipeline.batch.size: 1

path.config: "/usr/share/logstash/config/pipelines/service\_stamped\_json\_logs.conf"

Файлик самого конфига пайплайна:

input {

file {

path => "/var/log/nginx/netology.example.local.log"

start\_position => "beginning"

}

}

filter {

grok {

match => {

"message" => '%{IPORHOST:remote\_ip} - %{DATA:user\_name} \[%{HTTPDATE:access\_time}\] "%{WORD:http\_method} %{DATA:url} HTTP/%{NUMBER:http\_version}" %{NUMBER:response\_code} %{NUMBER:body\_sent\_bytes} "%{DATA:referrer}" "%{DATA:agent}"'

}

}

mutate {

remove\_field => [ "host" ]

}

}

output {

elasticsearch {

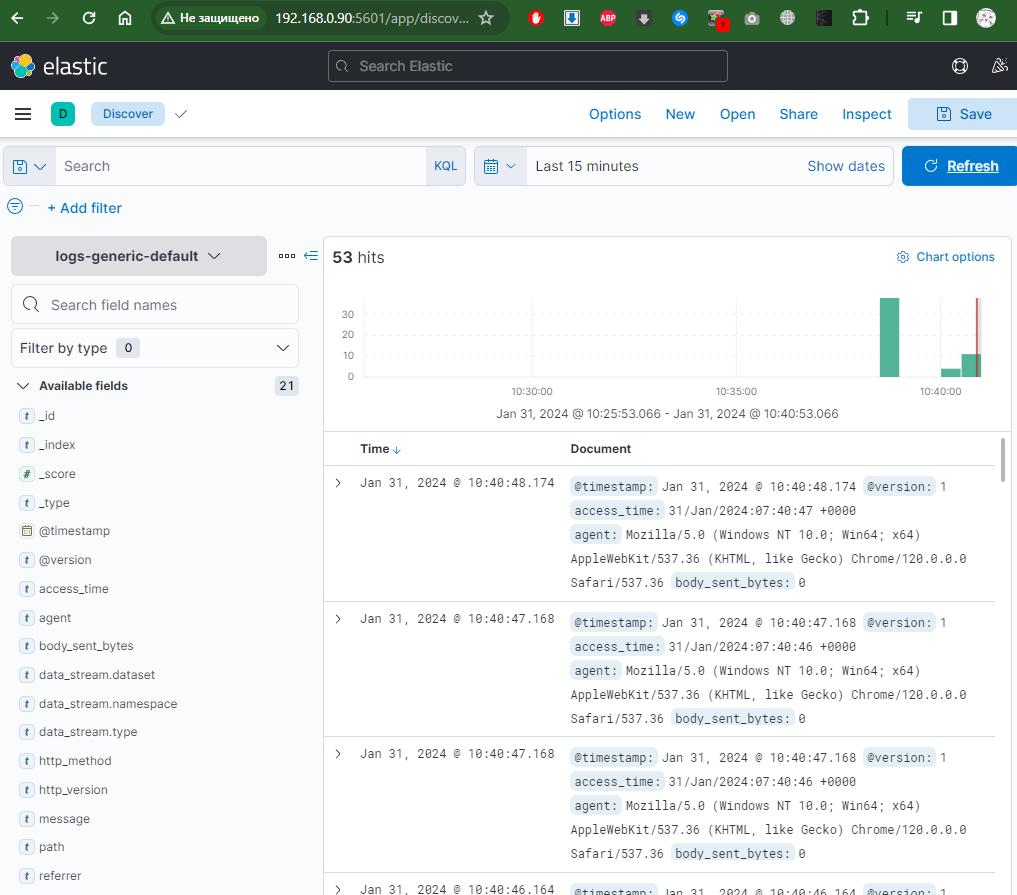
hosts => "elasticsearch:9200"

data\_stream => "true"

}

}

Итог работы:



# **Задание 4**

Установите и запустите Filebeat. Переключите поставку логов Nginx с Logstash на Filebeat.

*Приведите скриншот интерфейса Kibana, на котором видны логи Nginx, которые были отправлены через Filebeat.*

# **Решение 4**

В первую очередь добавляем бит в компоуз файл:

filebeat:

image: elastic/filebeat:7.16.2

container\_name: filebeat

depends\_on:

- elasticsearch

volumes:

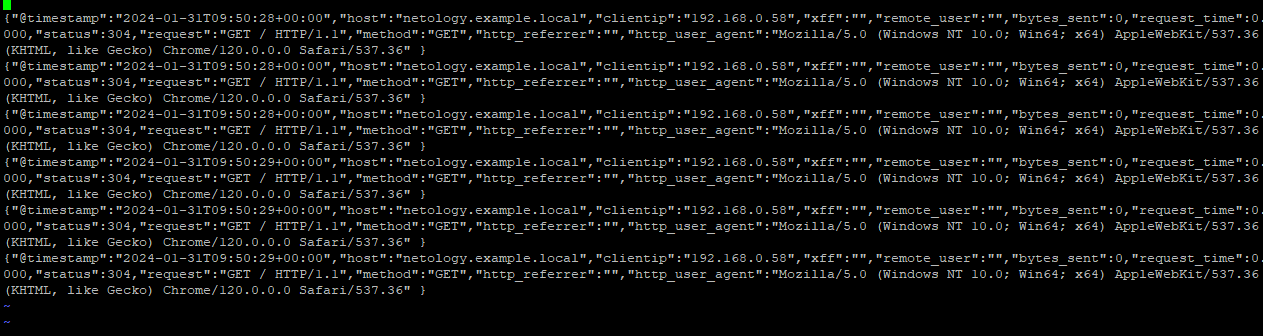
- ./filebeat/filebeat.yml:/usr/share/filebeat/filebeat.yml:ro

- /var/log/nginx/netology.example.local.log:/var/log/nginx/netology.example.local.log

networks:

- esnet

В итоге лог nginx выглядит таким образом:



То есть он уже в JSON формате.

Дальше, конфиг бита:

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/nginx/netology.example.local.log

output.logstash:

hosts: ["logstash:5044"]

И логсташа:

input {

beats {

port => 5044

}

}

filter {

json {

source => "message"

}

mutate {

remove\_field => [ "host" ]

}

}

output {

elasticsearch {

hosts => "elasticsearch:9200"

index => "logs-%{+YYYY.MM.dd}"

}

}

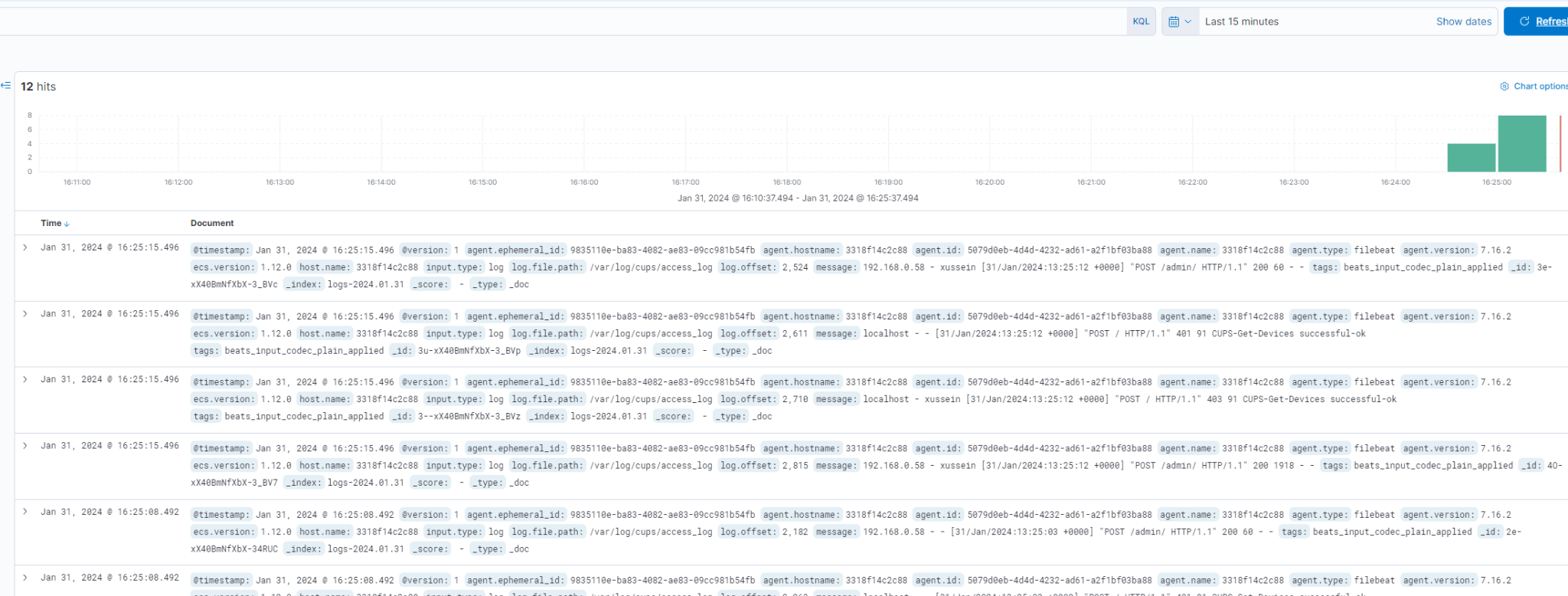
# **Задание 5**

Настройте поставку лога в Elasticsearch через Logstash и Filebeat любого другого сервиса , но не Nginx. Для этого лог должен писаться на файловую систему, Logstash должен корректно его распарсить и разложить на поля.

*Приведите скриншот интерфейса Kibana, на котором будет виден этот лог и напишите лог какого приложения отправляется.*

# **Решение 5**

Взял cups:



Тут я уже это дело не парсил, времени не хватает красоту навести.

В файлбите добавил лог и все.