

# Развертывание базового стека ELK

## Задание:

### 4) Развертывание базового стека ELK

- a) Создание файла `elk.yml`:
  - 1. В домашней директории пользователя создайте файл `elk.yml`, описывающий стек контейнеров для Elasticsearch, Logstash и Kibana.
- b) Конфигурация стека Docker Compose:
  - 1. Определите три сервиса:
    - **elasticsearch:**
      - Используйте образ **elasticsearch:7.10.1**.
      - Прокиньте порт 9200 для доступа к Elasticsearch API.
    - **logstash:**
      - Используйте образ **logstash:7.10.1**.
      - Настройте Logstash для получения данных и отправки их в Elasticsearch.
    - **kibana:**
      - Используйте образ **kibana:7.10.1**.
      - Прокиньте порт 5601 для доступа к веб-интерфейсу Kibana.
  - 2. Запустите Docker Compose с файлом `elk.yml`.
  - 3. Убедитесь, что все сервисы работают и Kibana доступна по порту 5601.

## Вариант реализации:

- В домашней директории пользователя `altlinux` из под пользователя `altlinux` создаём файл `elk.yml`:

```
vim ~/elk.yml
```

- Помещаем в него следующее содержимое:
  - Реализуем функционал согласно требованиям задания:

```

version: '3.7'

services:
  elasticsearch:
    image: elasticsearch:7.10.1
    container_name: elasticsearch
    environment:
      - discovery.type=single-node
      - bootstrap.memory_lock=true
      - "ES_JAVA_OPTS=-Xms1g -Xmx1g"
    ulimits:
      memlock:
        soft: -1
        hard: -1
    ports:
      - "9200:9200"
    volumes:
      - es_data:/usr/share/elasticsearch/data

  logstash:
    image: logstash:7.10.1
    container_name: logstash
    depends_on:
      - elasticsearch
    volumes:
      - ./logstash.conf:/usr/share/logstash/pipeline/logstash.conf
    environment:
      LS_JAVA_OPTS: "-Xms1g -Xmx1g"

  kibana:
    image: kibana:7.10.1
    container_name: kibana
    depends_on:
      - elasticsearch
    ports:
      - "5601:5601"
    environment:
      ELASTICSEARCH_HOSTS: "http://elasticsearch:9200"

volumes:
  es_data:

```

- В домашней директории пользователя **altlinux** из под пользователя **altlinux** создаём файл **logstash.conf**:

```
vim ~/logstash.conf
```

- Помещаем в него следующее содержимое:
  - Настроивая Logstash для получения данных и отправки их в Elasticsearch

```

input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "logstash-%{+YYYY.MM.dd}"
  }
}

```

- Выполняем запуск стека контейнеров для **WordPress** и **MySQL**:
  - Запуск команды выполняется из домашнего каталога пользователя **altlinux**;

```
sudo docker compose -f elk.yml up -d
```

- Результат:

```

✓ Network altlinux_default Created
✓ Volume "altlinux_es_data" Created
✓ Container elasticsearch Started
✓ Container logstash Started
✓ Container kibana Started
[altlinux@controlvm ~]$

```

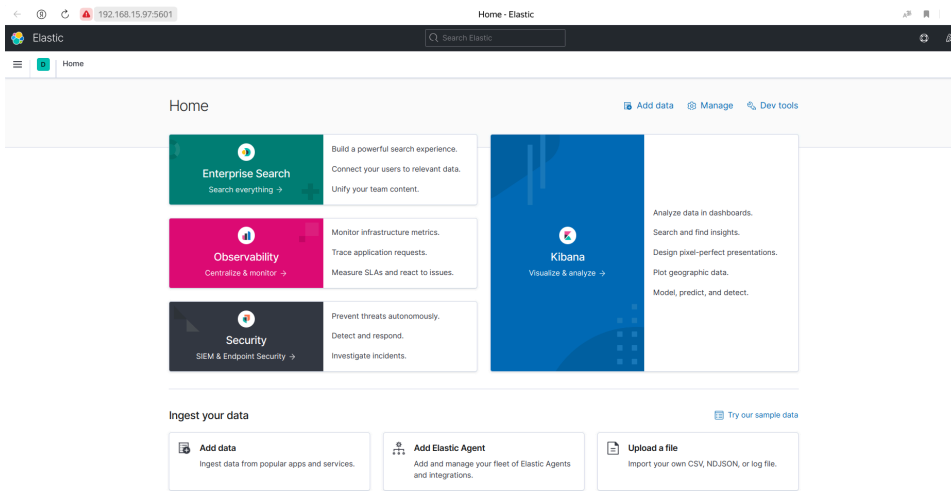
- Проверяем запущенные контейнеры:

```

[altlinux@controlvm ~]$ sudo docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                                                                 NAMES
5c538f8c0089   kibana:7.10.1                       "/usr/local/bin/dumb..." 41 seconds ago Up 38 seconds 0.0.0.0:5601->5601/tcp, :::5601->5601/tcp  kibana
93566e763a5c   logstash:7.10.1                     "/usr/local/bin/dock..." 41 seconds ago Up 38 seconds 5044/tcp, 9600/tcp          logstash
120cc2d3290   elasticsearch:7.10.1                "/tini -- /usr/local..." 41 seconds ago Up 39 seconds 0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp  elasticsearch
190008cc13b9   wordpress:latest                    "docker-entrypoint.s..." 24 minutes ago Up 24 minutes 0.0.0.0:80->80/tcp, :::80->80/tcp  wordpress
a5490f915e2d   mysql:5.7                           "docker-entrypoint.s..." 24 minutes ago Up 24 minutes 3306/tcp, 33060/tcp        mysql

```

- Проверяем доступ к веб-интерфейсу **Kibana**:
  - Обращаясь на Плавающий-IP адрес **ControlVM** на порт **5601**;



- Проверяем доступ к веб-интерфейсу **Elasticsearch API**:
  - Обращаясь на Плавающий-IP адрес **ControlVM** на порт **9200**;

```
192.168.15.97:9200
{
  "name" : "120cc20d3290",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "q-e4BFf05A01XNsHKX1kvg",
  "version" : {
    "number" : "7.10.1",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "1c34507e66d7db1211f66f3513706fdf548736aa",
    "build_date" : "2020-12-05T01:00:33.671820Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Последнее изменение: четверг, 16 января 2025, 09:18

[Обратная связь](#)

[Подпишитесь](#)

[Вы используете гостевой доступ \(Вход\)](#)

[Сводка хранения данных](#)

Тема оформления сайта разработана

[connect.me](#)