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.
- c) Запуск стека:
  - 1. Запустите Docker Compose с файлом elk.yml.
  - 2. 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:
        - Настраивая Logstash для получения данных и отправки их в Elasticsearch

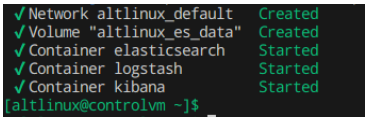
```
input {
  beats {
    port => 5044
  }
}

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

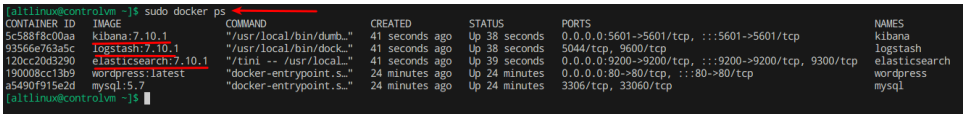
- Выполняем запуск стека контейнеров для **WordPress** и **MySQL**:
    - Запуск команды выполняется из домашнего каталога пользователя **altlinux**;

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

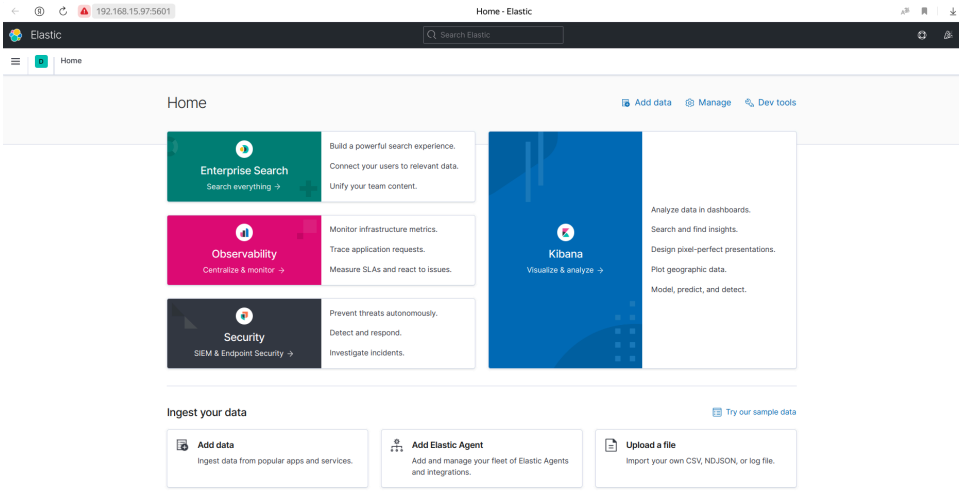
    - Результат:



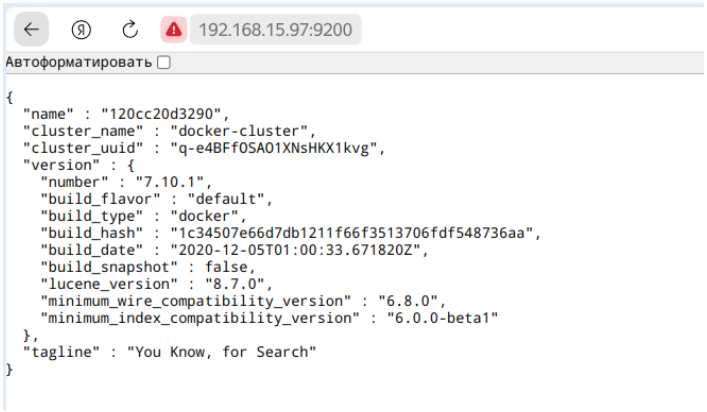
- Проверяем запущенные контейнеры:



- 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**;



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