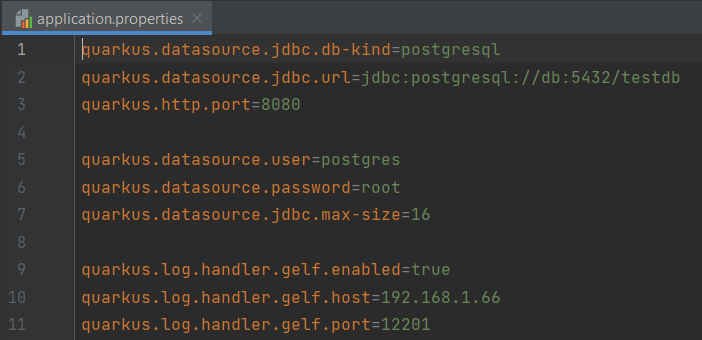
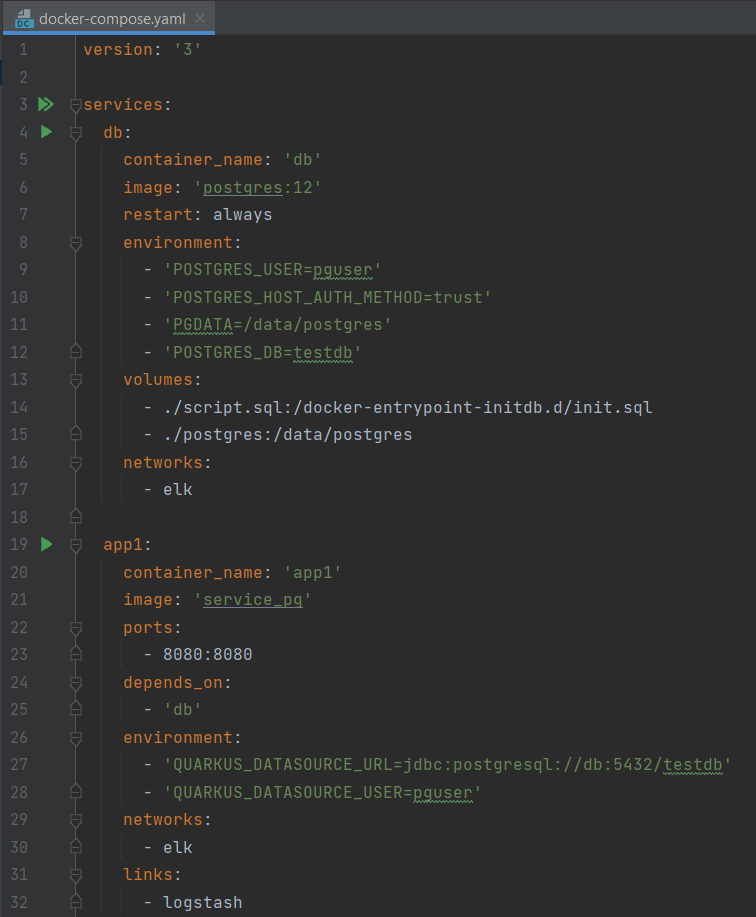
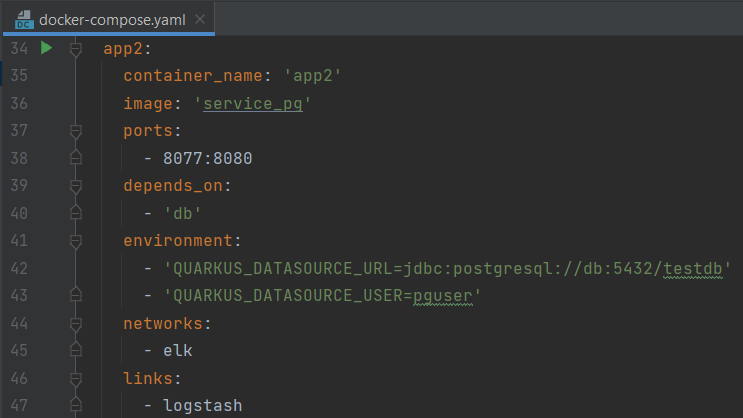
ELK – это аббревиатура, используемая для описания стека из трех проектов:

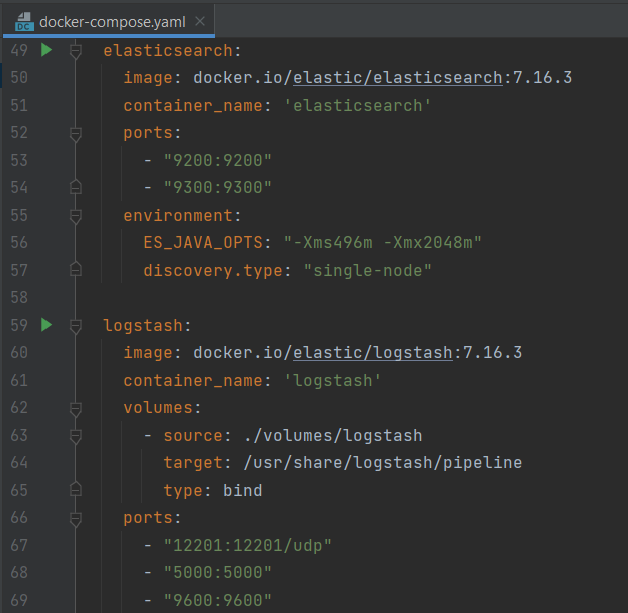
1. Elasticsearch (хранение и поиск данных)
2. Logstash (конвеер для обработки, фильтрации и нормализации логов)
3. Kibana (интерфейс для удобного поиска и администрирования)

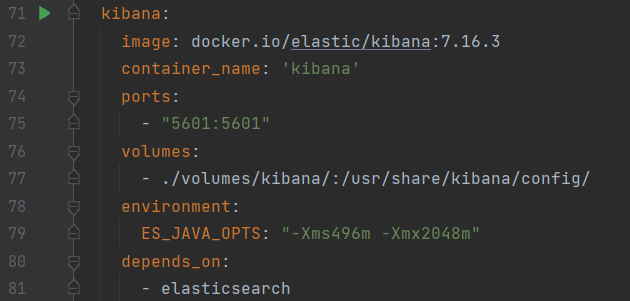
ELK предоставляет возможность собирать журналы всех ваших систем и приложений, анализировать их и создавать визуализации, чтобы мониторить приложения и инфраструктуры, быстрее устранять неполадки, анализировать систему безопасности и другое.

Сначала добавим настройки конфигурации в файл application.properties.

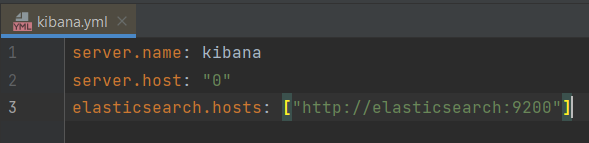
Пропишем в docker-compose.yaml файл настройки для ELK-стека:

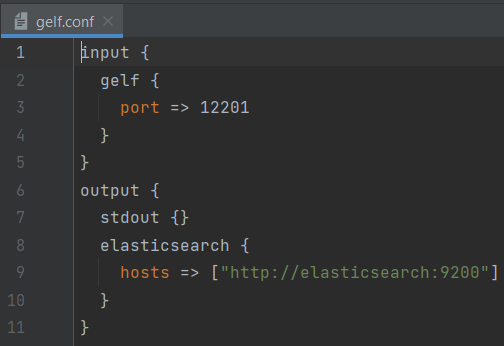




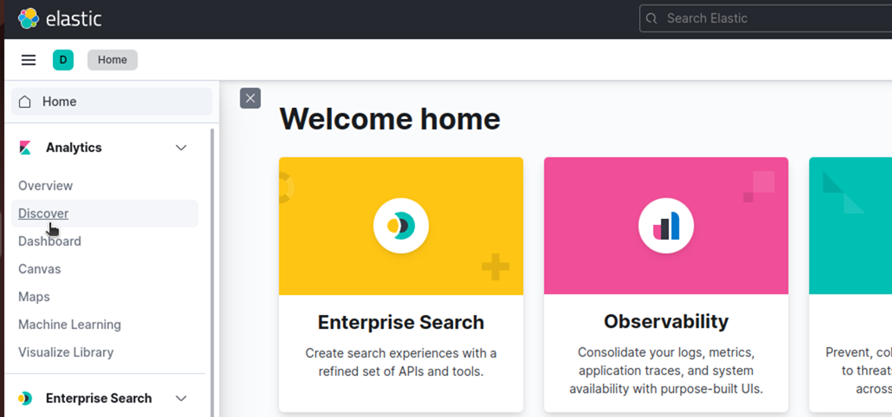


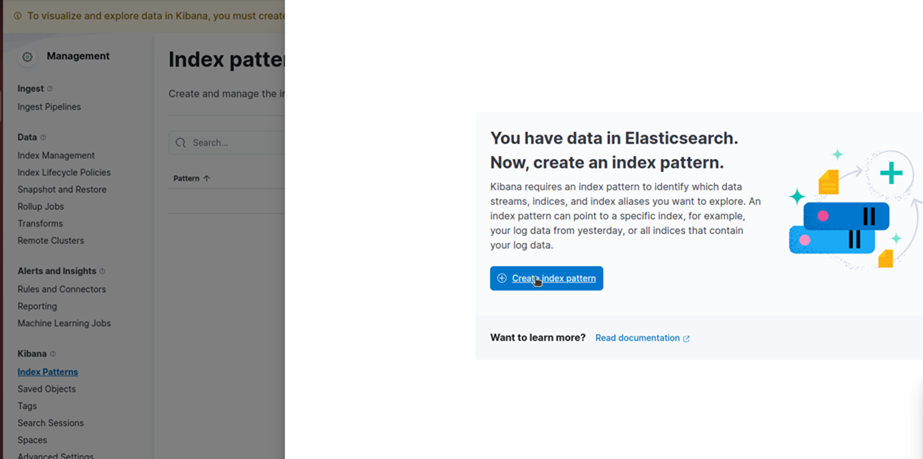
В одной папке с файлом docker-compose.yaml создадим папку volumes, а в ней – 2 папки (logstash и kibana).

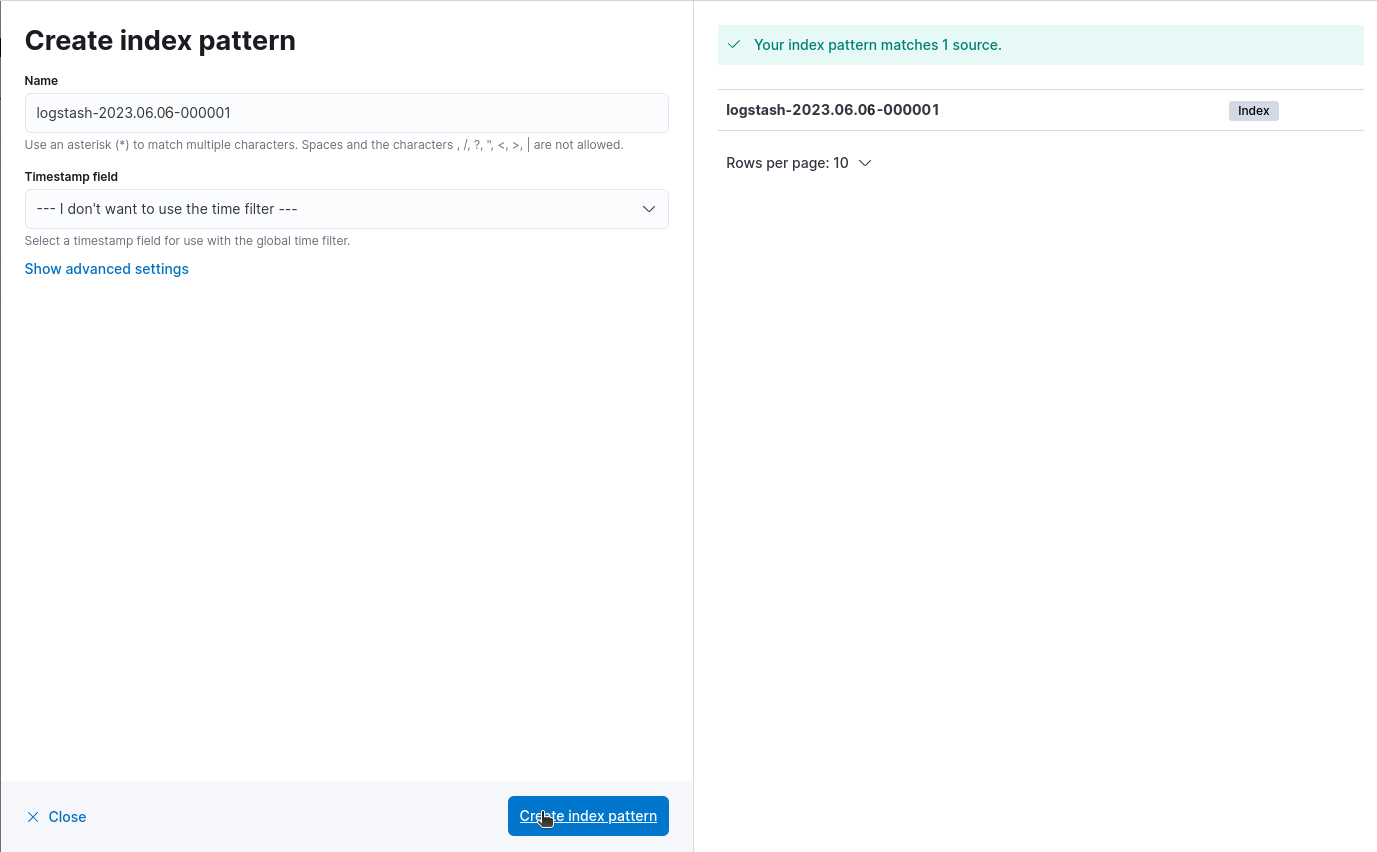
В папке kibana создадим файл kibana.yml:

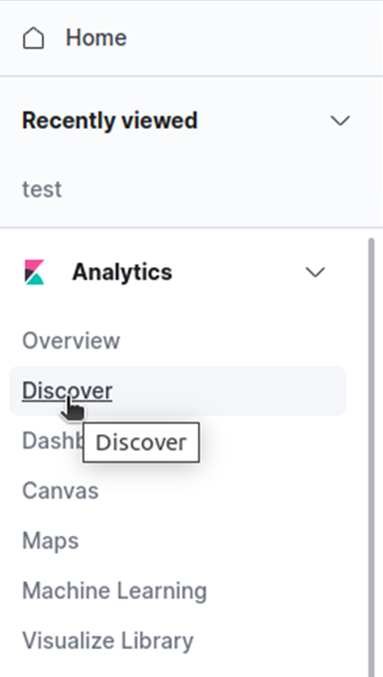
В папке logstash создадим файл gelf.conf:

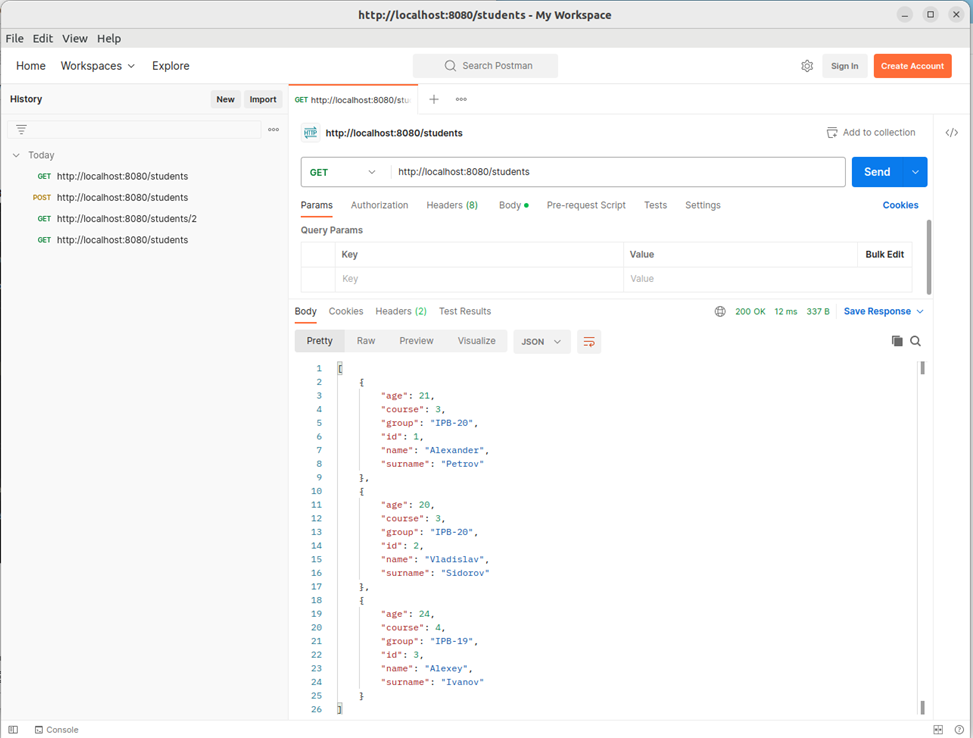
Выполняем команду docker compose up для поднятия контейнеров.

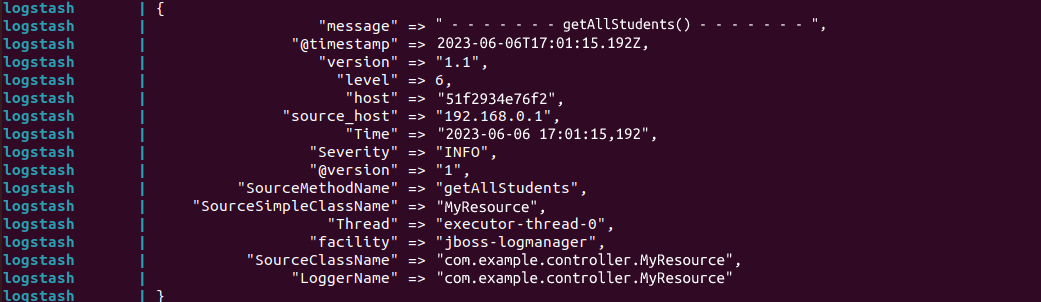
Переходим по ссылке [http://192.168.1.66:5601.](http://192.168.1.66:5601.#)

Нажимаем create index pattern, чтобы создать шаблон индекса для подключения к Elasticsearch.





Несколько раз отправим GET-запрос:

Результат работы в консоли:

Результат работы в Kibana: