**Федеральное государственное автономное образовательное учреждение**

**высшего образования**   
**"Национальный исследовательский университет**   
**"Высшая школа экономики"**

Московский институт электроники и математики

им. А. Н. Тихонова НИУ ВШЭ

Департамент компьютерной инженерии

Лабораторная работа №7

по теме:

«Установка и настройка ELK стека для анализа журналов и логов»

По дисциплине

«Проектный семинар "Инструментальные средства программирования"»

|  |  |
| --- | --- |
| **Группа:** | **БИВ-224** |
| **Студент:** | **Болезнов Степан** |

**Москва 2025**

**Оглавление**

[Ход работы 3](#_Toc198207288)

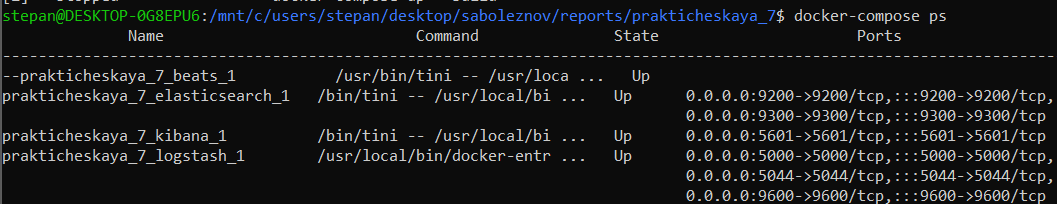
[Выводы 5](#_Toc198207289)

# Ход работы

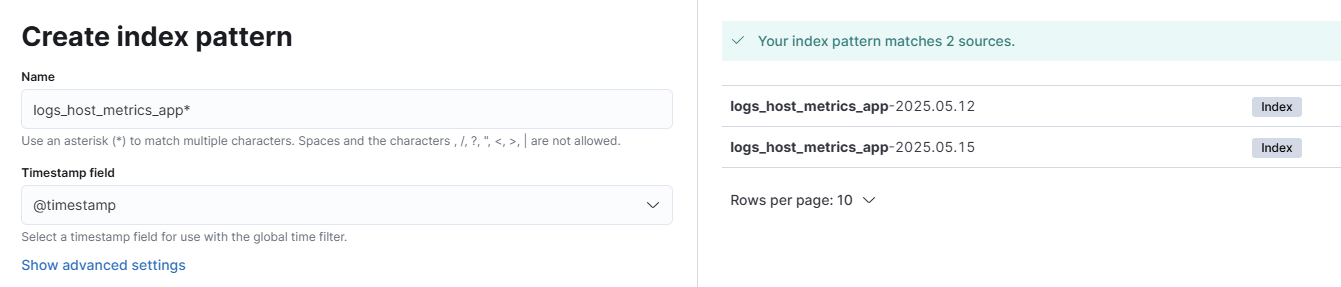
Был создан файл docker-compose.yml для запуска 4 сервисов, а также скрипт на питоне для генерации log файла:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host\_metrics\_app | filebeat | logstash | elasticsearch | kibana |
| Генерация логов | Считывает логи приложения и передает их в logstash | Преобразовывает логи | Хранение и анализ логов | Web-панель для визуализации данных |
|  |  | http://localhost:9600 | http://localhost:9200 | http://localhost:5601 |

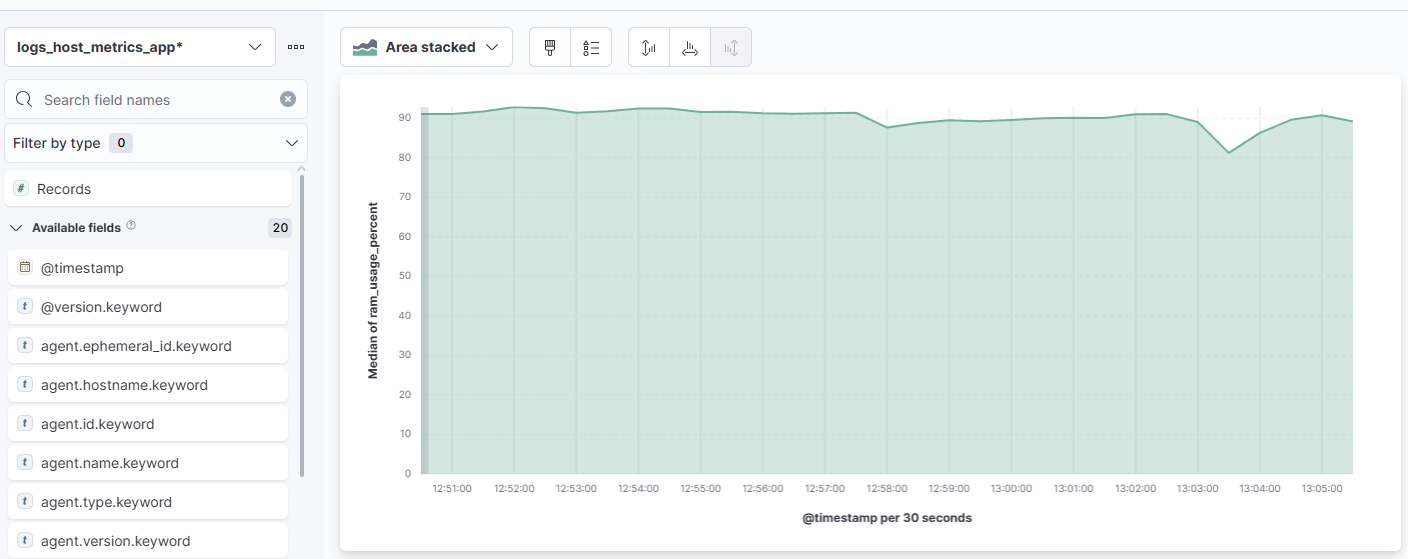
После запуска docker-compose up, можно проверить успешно ли все запустилось командой docker-compose ps:



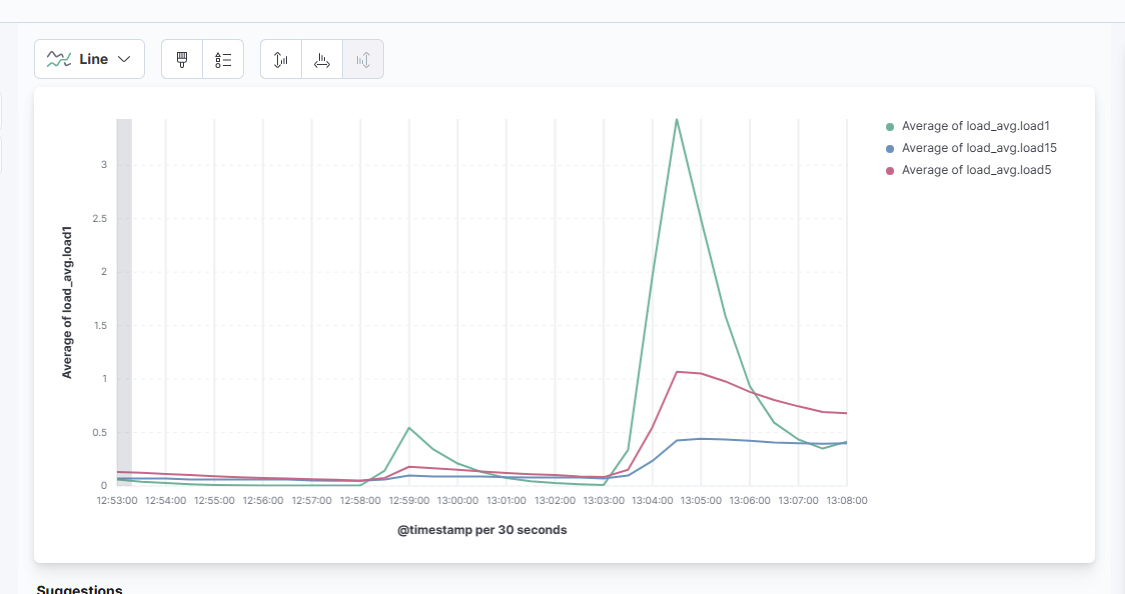
Все 4 сервиса работают исправно, можно зайти в kibana и посмотреть пришли ли логи, но сначала надо добавить index pattern:



Теперь можно посмотреть пример визуализации данных из логов, например, график использования оперативной памяти:



Или график количества процессов в очереди процессора за разное время:

****

# Выводы

В ходе выполнения данной практической работы была развернута полноценная система сбора, обработки и визуализации логов - стек ELK (Elasticsearch, Logstash, Kibana) с использованием Filebeat для отправки данных. Были реализованы следующие задачи:

1. Создание инфраструктуры с помощью Docker Compose  
   С использованием **docker-compose.yml** были запущены контейнеры всех компонентов ELK-стека, обеспечена сетевая связь между ними и настроены необходимые параметры окружения.
2. Настройка Filebeat для сбора метрик хоста  
   Написан Python-скрипт, собирающий информацию о загрузке процессора (**load average**) и использовании оперативной памяти. Эти данные записываются в файл, который Filebeat передаёт далее в Logstash для обработки.
3. Решение проблемы с правами доступа к конфигурации Filebeat  
   В процессе запуска было выявлено и исправлено нарушение требований безопасности Filebeat к правам доступа на конфигурационный файл. Ошибка устранена с помощью отключения просмотра прав через команду в docker-compose.
4. Интеграция компонентов стека  
   Данные, собранные Filebeat, успешно передаются в Logstash, индексируются в Elasticsearch и становятся доступны для визуализации в Kibana.
5. Готовность к анализу метрик  
   Полученные данные позволяют отслеживать нагрузку на систему во времени, что может быть использовано для мониторинга производительности сервера или хоста.

Выполнение работы позволило получить практические навыки настройки и взаимодействия компонентов ELK-стека, а также понимание принципов централизованного сбора и анализа логов.