Serilog, ElasticSearch e Kibana

O que é o Serilog?

Ele é uma biblioteca para log de informações de qualquer aplicação .NET, que utilizar várias Sinks.

O que são Sinks?

A base do serilog possui somente a implementação básica para cada necessidade específica existe um sink, Ex:

- Sinks.AwsCloudWatch → Ajuda para salvar os logs na aws cloud watch.
- Sinks.File → Ajuda a salvar os logs em um arquivo texto.
- Sinks.ElasticSearch → Ajuda a salvar os logs de forma estruturada o qual iremos utilizar.

O que é ElasticSearch?

É um banco de dados open source, que funciona extremamente bem com indexação e análise de dados.

E o Kibana?

É uma aplicação gratuita e open source, um front-end fornecendo recursos de busca e visualização dos dados indexados no ElasticSearch. Suas principais aplicações são:

- Logging e analítica de log
- Métricas de infraestrutura e monitoramento de container
- Monitoramento de performance de aplicação (APM)
- Análise e visualização de dados geoespaciais
- Analítica de segurança
- Análise de dados empresarial

Elastic + Kibana = docker compose

Vamos utilizar o docker compose para subir os containers com o Elastic e o Kibana, assim facilitando a configuração.

```
version: '3.7'
services:

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:7.7.0
    ports:
      - "9200:9200"
      - "9300:9300"
    environment:
      discovery.type: "single-node"
      ES_JAVA_OPTS: "-Xms2g -Xmx2g"
      xpack.monitoring.enabled: "true"

  kibana:
    image: docker.elastic.co/kibana/kibana:7.7.0
    ports:
      - "5601:5601"
    environment:
      ELASTICSEARCH_URL: http://elasticsearch:9200
    depends_on:
      - elasticsearch
```

Salve um arquivo com o nome de:

docker-compose.yml

Para iniciar os serviços, simplesmente digite isso:

```
docker-compose up -d
```

O parâmetro -d inicia os serviços no modo detached, dessa forma o terminal não ficará bloqueado.

Usamos o comando abaixo para parar a execução dos serviços:

```
docker-compose down
```