План семинара (занятия)

- вводный рассказ про базы данных
- причина выбора Elasticsearch
- какие существуют альтернативы
- установка Elasticsearch и Kibana
- подключение системных логов к Elasticsearch при помощи filebeat
- просмотр логов в Kibana

Вводный рассказ про базы данных

- какие существуют базы данных: реляционные, нереляционные (Key-Value, документоориентированные, столбцовые, графовые)
- реляционные базы: MySQL, PostgreSQL, Oracle,...
- нереляционные: Key-Value (Redis,...), документоориентированные (Elasticsearch,...),...
- столбцовые/колоночные: (cassandra)
- графовые

Причины выбора ElasticSearch

- логи - неструктуированные данные, для работы с ними нужна документо-ориентированная база данных
- хорошее масштабирование, балансировка нагрузки, шардирование из коробки
- ELK/EFK-стек содержит всё необходимое для сбора логов (Elasticsearch + Logstash/Filebeat + Kibana)
- kibana - готовы инструмент визуализации, построения графиков,...

Какие существуют альтернативы

- loki, построен на идеологии prometheus (использование меток), малое потребление ресурсов, нет индексации контента
- хранение логов в базах данных
- хранение логов в файлах (сбор логов с разных серверов в одном месте)

Установка Elasticsearch и Kibana

```
echo "#05: Elasticsearch"

echo "Downloading ElasticSearch from Yandex mirror"
wget https://mirror.yandex.ru/mirrors/elastic/8/pool/main/e/elasticsearch/elasticsearch-
wget https://mirror.yandex.ru/mirrors/elastic/8/pool/main/k/kibana/kibana-8.1.1-amd64.de

# Install ElasticSearch from Yandex
echo "Installing ElasticSearch + Kibana"
dpkg -i /tmp/elasticsearch-8.1.1-amd64.deb
dpkg -i /tmp/kibana-8.1.1-amd64.deb

# Configure kibana to listen on 0.0.0.0
sed -i "s/^#server.host:.*/server.host: \"0.0.0.0\"/g" /etc/kibana/kibana.yml

# Restart Elasticsearch & Kibana
systemctl enable elasticsearch
systemctl enable kibana

systemctl restart elasticsearch
systemctl restart kibana

echo "Configuring Kibana"
echo "## Generating enrollment token..."
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana

MYIP=`ifconfig enp0s3 | grep "inet " | awk '{print $2;}' | head -1`

echo "## Please open http://${MYIP}:5601/ and enter this token in web page"

echo "Please use this verification code:"
/usr/share/kibana/bin/kibana-verification-code

ELK_PWD=`/usr/share/elasticsearch/bin/elasticsearch-reset-password -s -b -u elastic`
echo "Kibana URL: http://${MYIP}:5601/" >> /root/kibana-access.txt
echo "User: elastic" >> /root/kibana-access.txt
echo "Password: ${ELK_PWD}" >> /root/kibana-access.txt

echo "Please login with user 'elastic' and password '${ELK_PWD}'"
```

Задание

1. Установить Elasticsearch
2. Установить Kibana

Критерии оценки

1. Выполнение 1 задания - оценивается в 5 баллов
2. Выполенние 2 задания - оценивается в 8 баллов

Ссылки/литература

- Официальная документация по ElasticSearch
- Официальный сайт по Loki
- Habr: Loki — сбор логов, используя подход Prometheus