06 Добавить Логи С Oncall В Elastic Search(Filebeat)

План семинара (занятия)

- методы отправки логов в ElasticSearch
- чем можно собирать и отправлять логи
- зачем нужны промежуточные очереди
- обработка и обогащение логов
- как и что собираем

Методы отправки логов в ElasticSearch

- сбор на хостах без обработки, централизованная обработка (filebeat => LogStash => ElasticSearch)
- сбор на хостах с частичной или полной обработкой, отправка в ES (filebeat => ElasticSearch)

Чем можно собирать и отправлять логи

- filebeat
- vector
- …

Зачем нужны промежуточные очереди

- сглаживание пиков
- возможность параллельной обработки потока, имея при этом единую точку входа
- защита от кратковременной недоступности получателя (возможность проводить работы с даунтаймом без влияния на клиентов)
- лимитирование нагрузки на систему

Обработка и обогащение логов

- стандартные обработчики для распространённых типов логов, склейка multiline логов
- базовые токенизаторы (regex)
- обработка логов с использованием скриптовых языков (JavaScript, lua,…)

Как и что собираем

- OnCall пишет все свои логи только в syslog => собираем весь syslog
- Настраиваем форвард в rsyslog в UDP порт, filebeat принимает syslog поток, обрабатывает и отправляет его в ES
- Токенизация логов от OnCall - парсинг текстовых строк и извлечение оттуда полезных счётчиков

Установка filebeat

```
wget
https://mirror.yandex.ru/mirrors/elastic/8/pool/main/f/filebeat/filebeat-
8.1.1-amd64.deb -O /tmp/filebeat-8.1.1-amd64.deb
dpkg -i /tmp/filebeat-8.1.1-amd64.deb

ELASTIC_USER=`grep "User" /root/kibana-access.txt | awk '{print $2;}'`
ELASTIC_PASSWORD=`grep "Password" /root/kibana-access.txt | awk '{print
$2;}'`

cat << EOF > /etc/rsyslog.d/30-stream-socket.conf
*.* @127.0.0.1:5514

EOF
systemctl restart rsyslog

mv /etc/filebeat/filebeat.yml /etc/filebeat/filebeat.yml.orig
cat << EOF > /etc/filebeat/filebeat.yml
filebeat.inputs:
  - type: syslog
    format: auto
    protocol.udp:
      host: "localhost:5514"
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.template.settings:
  index.number_of_shards: 1
setup.template:
  name: "syslog"
  pattern: "syslog-*"
```

```
setup.kibana:
output.elasticsearch:
  hosts: ["localhost:9200"]
  protocol: "https"
  ssl.verification_mode: "none"
  index: "syslog-%{+yyyy.MM.dd}"
  username: "__USERNAME__"
  password: "__PASSWORD__"
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~
EOF

sed -i "s/__USERNAME__/"$ELASTIC_USER"/g" /etc/filebeat/filebeat.yml
sed -i "s/__PASSWORD__/"$ELASTIC_PASSWORD"/g" /etc/filebeat/filebeat.yml

systemctl enable filebeat
systemctl start filebeat
```

Задание

1. Установить Filebeat
2. Перенаправить rsyslog в udp socket и настроить прием и отправку в Elastic
3. Токенизация логов от OnCall (разделить на айпи, статус, uri)

Критерии оценки

1. Выполнение 1 задания - оценивается в 5 баллов
2. Выполенние 2 задания - оценивается в 8 баллов
3. Выполнение 3 задания - оценивается в 10 баллов
