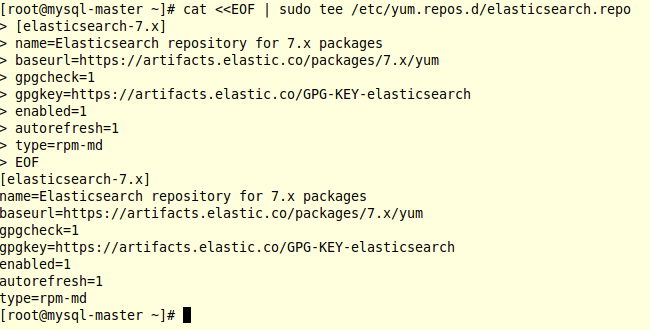
**#Поскольку Elasticsearch зависит от Java, нам необходимо установить Java**

sudo yum -y install java-openjdk-devel java-openjdk

**#После установки Java добавляем репозиторий ELK stack, который предоставляет пакеты ELK stack.**



**#После добавления репо импортируем ключ GPG:**

sudo rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

**#Очистим и обновим свой индекс пакетов YUM.**

sudo yum clean all

sudo yum makecache

## #Установим и настроим Elasticsearch

## sudo yum -y install elasticsearch

## #Подтвердим установку пакета.

## rpm -qi elasticsearch

## # Устанавливаем лимиты памяти для виртуальной машины Java

## cat > /etc/elasticsearch/jvm.options.d/jvm.options

## -Xms512m

## -Xmx512m

## Ctrl d - выход

## #Запустим и поставим в автозагрузку службу elasticsearch:

## sudo systemctl enable --now elasticsearch.service

## 

## # Проверяем и видим elasticsearch работает

## curl <http://127.0.0.1:9200>

## 

## # Создадим тестовый индекс

## curl -X PUT <http://127.0.0.1:9200/mytest_index>

## # Установим kibana

## sudo yum -y install kibana

## # Отредактируем конфигурационный файл kibana

## sudo nano /etc/kibana/kibana.yml

## server.port: 5601

## 

## server.host: "0.0.0.0"

## 

## elasticsearch.hosts: ["http://localhost:9200"]

## 

## # Запустим и поставим в автозагрузку службу kibana и добавим разрешение на соединение через порт 5601 в браундмауэре.

## sudo systemctl enable --now kibana

## 

## sudo firewall-cmd --add-port=5601/tcp --permanent

## sudo firewall-cmd --reload

## systemctl stop firewalld

## 

## #Установим и настроим Logstash

sudo yum -y install logstash filebeat auditbeat metricbeat packetbeat heartbeat-elastic

## #Пропишем конфигурационные файлы logstash config

## sudo nano /etc/logstash/logstash.yml

## path.data: /var/lib/logstash

## 

## path.config: /etc/logstash/conf.d

## 

## path.logs: /var/log/logstash

## 

## cat > /etc/logstash/conf.d/logstash-nginx-es.conf

## 

## #Перезагрузим службу logstash.service

## sudo systemctl restart logstash.service

## 

## #Пропишем конфигурационные файлы

## sudo nano /etc/filebeat/filebeat.yml

## # Закомментарить output.elasticsearch

## filebeat.inputs:

## - type: log

## paths:

## - /var/log/nginx/\*.log

## exclude\_files: ['\.gz$']

## output.logstash:

## hosts: ["localhost:5400"]

## 

## #Перезагрузим службу

## Systemctl enable filebeat

## 

## Systemctl restart filebeat

## Systemctl status filebeat

## 

## #Проверим процессы служб

## Ps afx

## 

## Остановил httpd

## 

## было

## 

## Сделал

## 

## 

## #Проверим доступность портов веб интерфейса

## 

## 

## 

## 

## 

## Здесь мы видим что логии разобраны по полям, есть возможность поиска по ним возможность агрегации

## При возвращении на discover

## 

## 

## Диаграмма кодов ответов 200, 500,300,400 ошибок.

## 