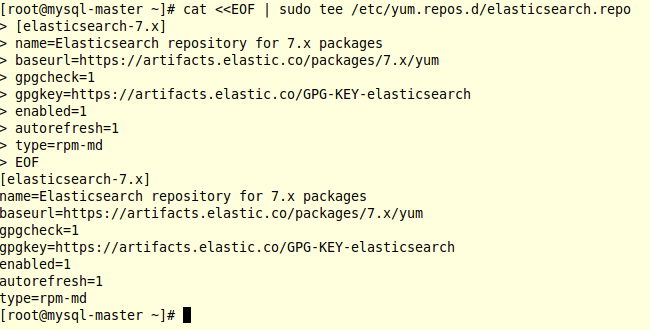


**#Поскольку Elasticsearch зависит от Java, вам необходимо установить Java в вашей системе**

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

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



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

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

**#Очистите и обновите свой индекс пакетов YUM.**

sudo yum clean all

sudo yum makecache

## #Установка и настройка Elasticsearch

## sudo yum -y install elasticsearch

## #Подтвердите установку пакета.

## rpm -qi elasticsearch

## # Устанавливаем лимиты памяти для виртуальной машины Java

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

## -Xms1g

## -Xmx1g

## Ctrl d

## #Запустите и включите службу elasticsearch при загрузке:

## sudo systemctl enable --now elasticsearch.service

## # Проверяем

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

## 

## # Создаём тестовый индекс

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

## # Установка kibana

## sudo yum -y install kibana

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

## server.port: 5601

## server.host: "0.0.0.0"

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

## sudo systemctl enable --now kibana

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

## sudo firewall-cmd --reload

## systemctl stop firewalld

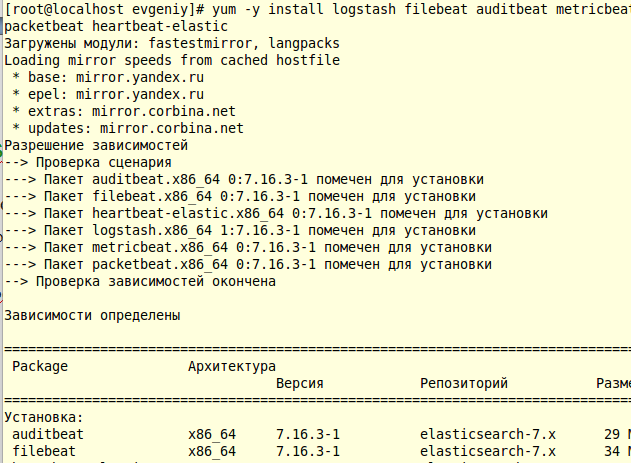
## #Установка и настройка Logstash

Последняя установка предназначена для Logstash. Он будет действовать как централизованный сервер журналов для ваших клиентских систем, на котором работает агент, такой как [filebeat](https://www.elastic.co/products/beats/filebeat" \t "_blank).

Другие инструменты ELK, которые можно установить, включают:

* **Файловый**бит: Легкий отправитель для журналов. Это поможет вам упростить простые вещи, предлагая легкий способ передачи и централизации журналов и файлов
* **Metricbeat**: Сбор показателей из ваших систем и служб. От процессора до памяти, от Redis до NGINX и многого другого, Metricbeat-это легкий способ отправки статистики системы и службы.
* **Packetbeat**: Легкий отправитель для сетевых данных
* **Сердцебиение**: Легкий отправитель для мониторинга времени безотказной работы. Это помогает вам отслеживать доступность служб с помощью активного зондирования
* **Auditbeat**: Легкий отправитель, который помогает вам проводить аудит действий пользователей и процессов в ваших системах

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



## 

## 

## # 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

## input {

## beats {

## port => 5400

## }

## }

## filter {

## grok {

## match => [ "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra\_fields}"]

## overwrite => [ "message" ]

## }

## mutate {

## convert => ["response", "integer"]

## convert => ["bytes", "integer"]

## convert => ["responsetime", "float"]

## }

## geoip {

## source => "clientip"

## add\_tag => [ "nginx-geoip" ]

## }

## date {

## match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]

## remove\_field => [ "timestamp" ]

## }

## useragent {

## source => "agent"

## }

## }

## output {

## elasticsearch {

## hosts => ["localhost:9200"]

## index => "weblogs-%{+YYYY.MM.dd}"

## document\_type => "nginx\_logs"

## }

## stdout { codec => rubydebug }

## }

## 

## 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"]

## 

## 

## Cd /etc/nginx/conf.d

## Nano default.conf

## 

## Nginx –t

## Service nginx reboot

## 

filebeat modules list

[20:39](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643045944022000)

sudo filebeat modules enable nginx

[20:40](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046019023200)

В этом файле /etc/filebeat/filebeat.yml оставим только output.logstash и на какой hosts

https://ca.slack-edge.com/T73A2HU1L-U02LJUL7360-90a40b8266bd-48

[**Романов Евгений Алексеевич**](https://app.slack.com/team/U02LJUL7360)  [20:44](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046258023600)

image.png

https://ca.slack-edge.com/T73A2HU1L-URPSP2MEY-c33a02795a85-48

[**Alexandr Kholodov**](https://app.slack.com/team/URPSP2MEY)  [20:44](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046291024200)

можно еще просто переименовать mv /etc/filebeat/modules.d/nginx.yml.disabled /etc/filebeat/modules.d/nginx.yml

[20:46](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046404024900)

Самый простой способ, оставить только эти настройки в файле конфигурации

filebeat.inputs:

- type: log

paths:

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

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

output.logstash:

hosts: ["127.0.0.1:5400"]

(отредактировано)

[20:46](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046414025200)

Остальные настройки убрать

https://ca.slack-edge.com/T73A2HU1L-U02LJUL7360-90a40b8266bd-48

[**Романов Евгений Алексеевич**](https://app.slack.com/team/U02LJUL7360)  [20:47](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046479025800)

Даже все закомментированные?

[20:48](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046492026000)

только это и все

https://ca.slack-edge.com/T73A2HU1L-URPSP2MEY-c33a02795a85-48

[**Alexandr Kholodov**](https://app.slack.com/team/URPSP2MEY)  [20:49](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046548027000)

Да, только бекап оставь или копию сделай filebeat.yml.backup

https://ca.slack-edge.com/T73A2HU1L-U02LJUL7360-90a40b8266bd-48

[**Романов Евгений Алексеевич**](https://app.slack.com/team/U02LJUL7360)  [20:51](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046668027100)

image.png

[20:51](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046719028100)

т.е. после перемещения мне надо еще редактировать как вы говорите? или это другой вариант?

**Новое**

https://ca.slack-edge.com/T73A2HU1L-URPSP2MEY-c33a02795a85-48

[**Alexandr Kholodov**](https://app.slack.com/team/URPSP2MEY)  [20:52](https://otus-linux.slack.com/archives/D02LQ13DMRB/p1643046755028700)

это другой вариант, без включения модуля