#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.

```
[root@mysql-master ~]# cat <<EOF | sudo tee /etc/yum.repos.d/elasticsearch.repo
> [elasticsearch-7.x]
> name=Elasticsearch repository for 7.x packages
> baseurl=https://artifacts.elastic.co/packages/7.x/yum
> gpgcheck=1
> gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
> enabled=1
> autorefresh=1
> type=rpm-md
> EOF
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
[root@mysql-master ~]#
```

#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

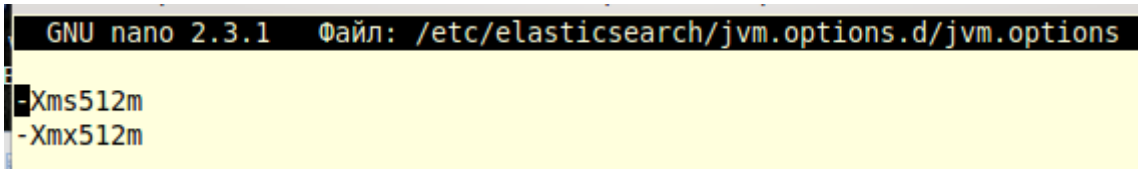
sudo yum -y install elasticsearch

#Подтвердим установку пакета.

rpm -qi elasticsearch

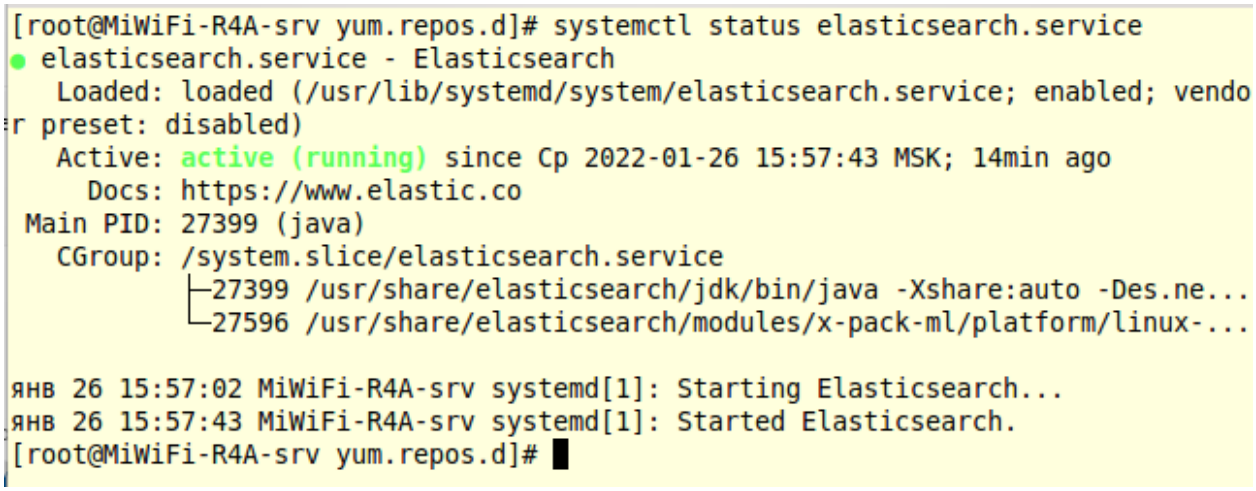
Устанавливаем лимиты памяти для виртуальной машины Java

cat > /etc/elasticsearch/jvm.options.d/jvm.options
-Xms512m
-Xmx512m
Ctrl d - выход



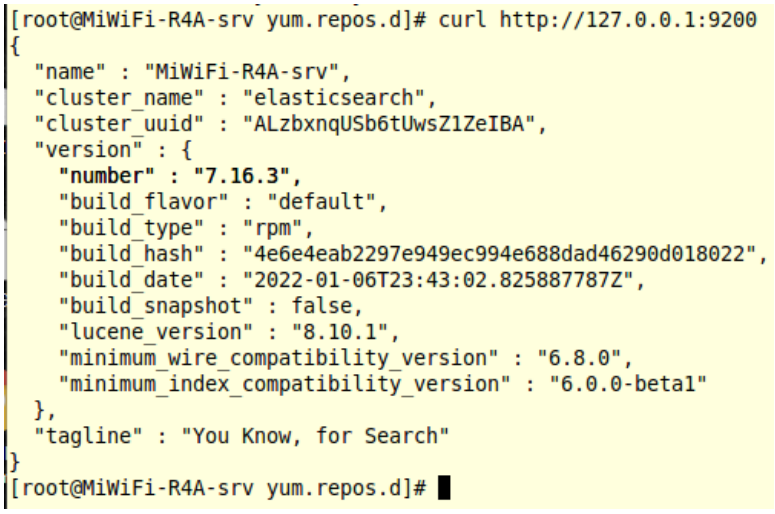
#Запустим и поставим в автозагрузку службу elasticsearch:

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

```
  GNU nano 2.3.1          Файл: /etc/kibana/kibana.yml                Изменён

# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601
```

server.host: "0.0.0.0"

```
# Specifies the address to which the Kibana server will bind. IP addresses and
# The default is 'localhost', which usually means remote machines will not be a
# To allow connections from remote users, set this parameter to a non-loopback
server.host: "0.0.0.0"
```

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

```
# The URLs of the Elasticsearch instances to use for all your queries.
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

```
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl enable --now kibana
Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service
to /etc/systemd/system/kibana.service.
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: d
isabled)
   Active: active (running) since Ср 2022-01-26 16:10:20 MSK; 10s ago
     Docs: https://www.elastic.co
 Main PID: 28201 (node)
   CGroup: /system.slice/kibana.service
           └─28201 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/b...

янв 26 16:10:20 MiWiFi-R4A-srv systemd[1]: Started Kibana.
[root@MiWiFi-R4A-srv yum.repos.d]#
```

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

systemctl stop firewalld

```
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor p
reset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)
[root@MiWiFi-R4A-srv yum.repos.d]#
```

#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

```
# ------------ Data path ------------------
#
# Which directory should be used by logstash and its plugins
# for any persistent needs. Defaults to LOGSTASH_HOME/data
#
path.data: /var/lib/logstash
#
```

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

```
# ------------ Pipeline Configuration Settings --------------
#
# Where to fetch the pipeline configuration for the main pipeline
#
path.config: /etc/logstash/conf.d
#
# Pipeline configuration string for the main pipeline
#
# config.string:
#
```

path.logs: /var/log/logstash

```
# ------------ Debugging Settings --------------
#
# Options for log.level:
#   * fatal
#   * error
#   * warn
#   * info (default)
#   * debug
#   * trace
#
# log.level: info
path.logs: /var/log/logstash
#
# ------------ Other Settings --------------
```

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

```
[root@MiWiFi-R4A-srv yum.repos.d]# cat /etc/logstash/conf.d/logstash-nginx-es.co
nf
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 }
}

[root@MiWiFi-R4A-srv yum.repos.d]#
```

#Перезагрузим службу logstash.service

sudo systemctl restart logstash.service

```
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl status logstash.service
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset
: disabled)
   Active: active (running) since Ср 2022-01-26 16:40:14 MSK; 10s ago
 Main PID: 29130 (java)
   CGroup: /system.slice/logstash.service
           └─29130 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon...

янв 26 16:40:14 MiWiFi-R4A-srv systemd[1]: Started logstash.
янв 26 16:40:14 MiWiFi-R4A-srv logstash[29130]: Using bundled JDK: /usr/sh...
янв 26 16:40:15 MiWiFi-R4A-srv logstash[29130]: OpenJDK 64-Bit Server VM w...
Hint: Some lines were ellipsized, use -l to show in full.
[root@MiWiFi-R4A-srv yum.repos.d]#
```

#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"]
```

```
  GNU nano 2.3.1               Файл: /etc/filebeat/filebeat.yml

#################### Filebeat Configuration Example #########################

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*

  # Exclude lines. A list of regular expressions to match. It drops the lines that are
  # matching any regular expression from the list.
  #include_lines: ['^ERR', '^WARN']

  # Exclude files. A list of regular expressions to match. Filebeat drops the files that
  # are matching any regular expression from the list. By default, no files are dropped.
  #prospector.scanner.exclude_files: ['.gz$']

  # Optional additional fields. These fields can be freely picked
  # to add additional information to the crawled log files for filtering
  #fields:
  #  level: debug
  #  review: 1

- type: log
  paths:
    - /var/log/nginx/*.log
  exclude_files: ['\.gz$']

# ============================== Filebeat modules ==============================

filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: false

  # Period on which files under path should be checked for changes
  #reload.period: 10s

# ======================= Elasticsearch template setting =======================

setup.template.settings:
  index.number_of_shards: 1
  #index.codec: best_compression
  #_source.enabled: false


# ================================== General ===================================

# The name of the shipper that publishes the network data. It can be used to group
# all the transactions sent by a single shipper in the web interface.
#name:

# The tags of the shipper are included in their own field with each
# transaction published.
#tags: ["service-X", "web-tier"]
```

```
# Optional fields that you can specify to add additional information to the
# output.
#fields:
#  env: staging

# ================================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here or by using the `setup` command.
#setup.dashboards.enabled: false

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:
# ================================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

# ============================== Elastic Cloud ==============================

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ================================== Outputs ===================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5400"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

```
# ================================== Processors ===================================
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~

# ================================== Logging ===================================

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: debug

# At debug level, you can selectively enable logging only for some components.
# To enable all selectors use ["*"]. Examples of other selectors are "beat",
# "publisher", "service".
#logging.selectors: ["*"]

# ============================= X-Pack Monitoring ==============================
# Filebeat can export internal metrics to a central Elasticsearch monitoring
# cluster.  This requires xpack monitoring to be enabled in Elasticsearch.  The
# reporting is disabled by default.

# Set to true to enable the monitoring reporter.
#monitoring.enabled: false

# Sets the UUID of the Elasticsearch cluster under which monitoring data for this
# Filebeat instance will appear in the Stack Monitoring UI. If output.elasticsearch
# is enabled, the UUID is derived from the Elasticsearch cluster referenced by output.elasticsearch.
#monitoring.cluster_uuid:

# Uncomment to send the metrics to Elasticsearch. Most settings from the
# Elasticsearch output are accepted here as well.
# Note that the settings should point to your Elasticsearch *monitoring* cluster.
# Any setting that is not set is automatically inherited from the Elasticsearch
# output configuration, so if you have the Elasticsearch output configured such
# that it is pointing to your Elasticsearch monitoring cluster, you can simply
# uncomment the following line.
#monitoring.elasticsearch:

# ============================== Instrumentation ===============================

# Instrumentation support for the filebeat.
#instrumentation:
    # Set to true to enable instrumentation of filebeat.
    #enabled: false

    # Environment in which filebeat is running on (eg: staging, production, etc.)
    #environment: ""

    # APM Server hosts to report instrumentation results to.
    #hosts:
    #  - http://localhost:8200

    # API Key for the APM Server(s).
    # If api_key is set then secret_token will be ignored.
    #api_key:

    # Secret token for the APM Server(s).
    #secret_token:


# ================================= Migration ==================================

# This allows to enable 6.7 migration aliases
#migration.6_to_7.enabled: true
```

#Перезагрузим службу

Systemctl enable filebeat

```
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl enable filebeat
Created symlink from /etc/systemd/system/multi-user.target.wants/filebeat.servic
e to /usr/lib/systemd/system/filebeat.service.
[root@MiWiFi-R4A-srv yum.repos.d]#
```

Systemctl restart filebeat

Systemctl status filebeat

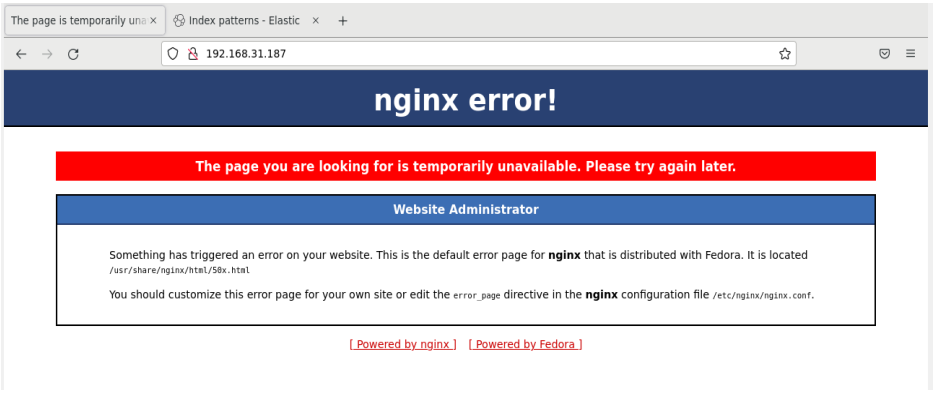
```
[root@MiWiFi-R4A-srv yum.repos.d]# systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elastic
search.
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; vendor pre
set: disabled)
   Active: active (running) since Ср 2022-01-26 17:00:21 MSK; 9s ago
     Docs: https://www.elastic.co/beats/filebeat
 Main PID: 29363 (filebeat)
   CGroup: /system.slice/filebeat.service
           └─29363 /usr/share/filebeat/bin/filebeat --environment systemd -c ...

янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.878+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.879+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.886+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.886+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.887+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.887+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.888+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.889+03...
янв 26 17:00:24 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:24.890+03...
янв 26 17:00:27 MiWiFi-R4A-srv filebeat[29363]: 2022-01-26T17:00:27.861+03...
Hint: Some lines were ellipsized, use -l to show in full.
[root@MiWiFi-R4A-srv yum.repos.d]#
```

#Проверим процессы служб

Ps afx

```
11690 ?        Sl     1:14 kdeinit4: konsole [kdeinit]
11734 pts/1    Ss     0:00  \_ /bin/bash
12617 pts/1    S      0:00      \_ su root
12942 pts/1    S      0:01          \_ bash
31353 pts/1    R+     0:00              \_ ps afx
27013 ?        Ss     0:03 /usr/sbin/httpd -DFOREGROUND
27014 ?        S      0:00  \_ /usr/sbin/httpd -DFOREGROUND
27015 ?        S      0:00  \_ /usr/sbin/httpd -DFOREGROUND
27016 ?        S      0:00  \_ /usr/sbin/httpd -DFOREGROUND
27017 ?        S      0:00  \_ /usr/sbin/httpd -DFOREGROUND
27018 ?        S      0:00  \_ /usr/sbin/httpd -DFOREGROUND
27399 ?        Ssl   19:57 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache
27596 ?        Sl     0:00  \_ /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/con
28201 ?        Ssl   15:48 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist
29039 ?        Ss     0:00 nginx: master process /usr/sbin/nginx
29040 ?        S      0:00  \_ nginx: worker process
29041 ?        S      0:00  \_ nginx: worker process
29130 ?        SNsl   9:41 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:C
31099 ?        Ssl    0:04 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/file
[root@MiWiFi-R4A-srv yum.repos.d]#
```

#Проверим работу службы nginx и обновим несколько раз для сбора логов



#Настройки nginx, проверка синтаксиса и перезапуск приложения

```
 GNU nano 2.3.1                  Файл: default.conf                      Изменён

# Balance server

upstream backend {
        server 127.0.0.1:8080 weight=2;
        server 127.0.0.1:8081;
        server 127.0.0.1:8082;
}

server {
        listen       80;
        listen       [::]:80;
        server_name  _;
        root         /usr/share/nginx/html;

        include /etc/nginx/default.d/*.conf;

                location / {
                        try_files $uri $uri/ =404;
                        #proxy_pass http://backend;
                        #proxy_set_header Host $host;
                        #proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                        #proxy_set_header X-Real-IP $remote_addr;
                }

                location ~ \.php$ {
                        include fastcgi_params;
                        root /var/www/html;

                        fastcgi_pass unix:/run/php/php7.4-fpm.sock;
                        #fastcgi_pass 127.0.0.1:9000;
                }
```

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[root@MiWiFi-R4A-srv conf.d]#
[root@MiWiFi-R4A-srv conf.d]#
[root@MiWiFi-R4A-srv conf.d]#
[root@MiWiFi-R4A-srv conf.d]#
[root@MiWiFi-R4A-srv conf.d]# service nginx reload
Redirecting to /bin/systemctl reload nginx.service
[root@MiWiFi-R4A-srv conf.d]#
```

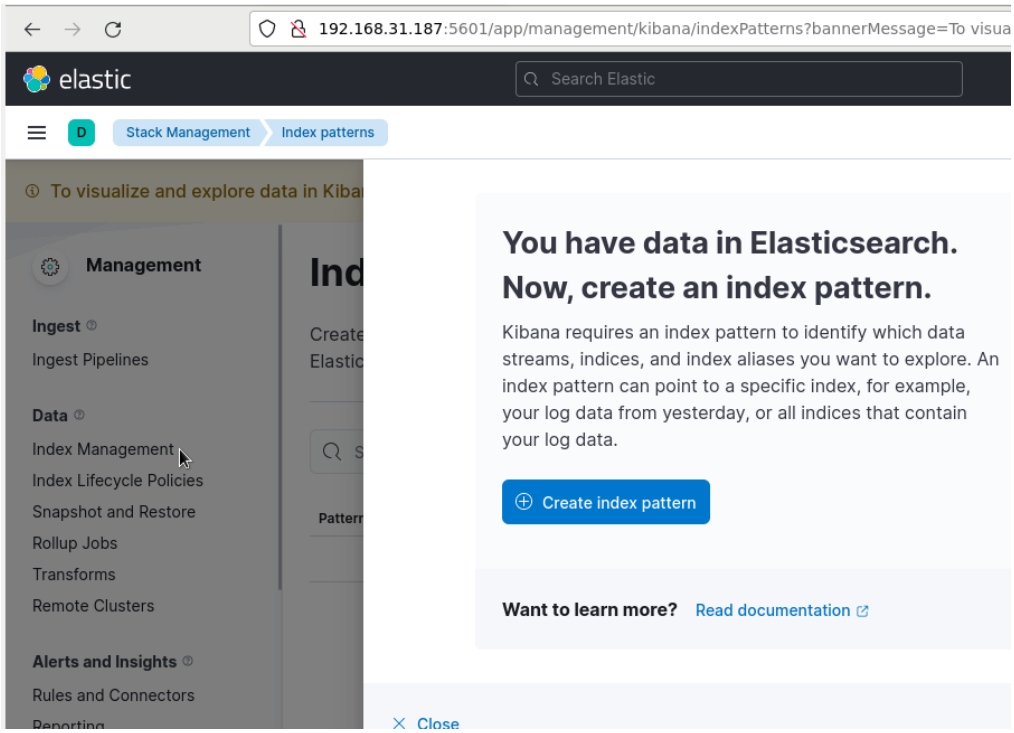
#Проверим доступность портов веб интерфейса

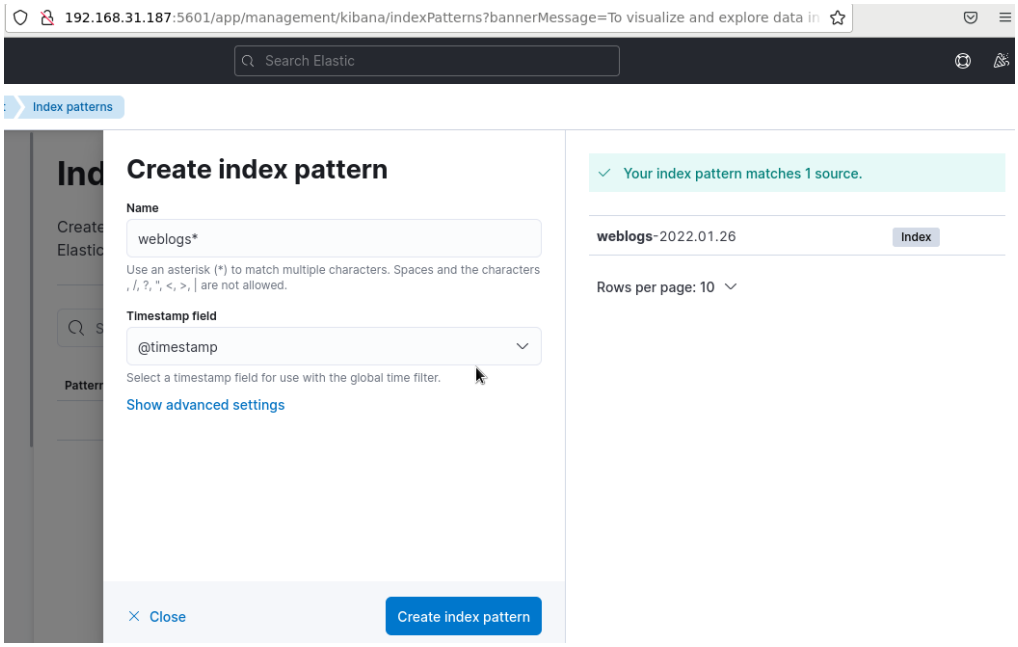
```
[root@MiWiFi-R4A-srv conf.d]# ss -tnlp
State       Recv-Q Send-Q      Local Address:Port                    Peer Address:Port
LISTEN      0      128                 *:22                                 *:*
users:(("sshd",pid=1047,fd=3))
LISTEN      0      128             127.0.0.1:631                            *:*
users:(("cupsd",pid=1051,fd=11))
LISTEN      0      100             127.0.0.1:25                             *:*
users:(("master",pid=1577,fd=13))
LISTEN      0      128                 *:5601                               *:*
users:(("node",pid=28201,fd=23))
LISTEN      0      128                 *:111                                *:*
users:(("rpcbind",pid=694,fd=8))
LISTEN      0      128                 *:80                                 *:*
users:(("nginx",pid=31717,fd=6),("nginx",pid=31716,fd=6),("nginx",pid=31609,fd=6))
LISTEN      0      128    [::ffff:127.0.0.1]:9300                           [::]:*
users:(("java",pid=27399,fd=290))
LISTEN      0      128            [::1]:9300                                [::]:*
users:(("java",pid=27399,fd=289))
LISTEN      0      128             [::]:22                                  [::]:*
users:(("sshd",pid=1047,fd=4))
LISTEN      0      128            [::1]:631                                 [::]:*
users:(("cupsd",pid=1051,fd=10))
LISTEN      0      128             [::]:5400                                [::]:*
users:(("java",pid=29130,fd=118))
LISTEN      0      100            [::1]:25                                  [::]:*
users:(("master",pid=1577,fd=14))
LISTEN      0      50     [::ffff:127.0.0.1]:9600                           [::]:*
users:(("java",pid=29130,fd=69))
LISTEN      0      128             [::]:111                                 [::]:*
users:(("rpcbind",pid=694,fd=11))
LISTEN      0      128             [::]:80                                  [::]:*
users:(("nginx",pid=31717,fd=7),("nginx",pid=31716,fd=7),("nginx",pid=31609,fd=7))
LISTEN      0      128    [::ffff:127.0.0.1]:9200                           [::]:*
users:(("java",pid=27399,fd=294))
LISTEN      0      128            [::1]:9200                                [::]:*
users:(("java",pid=27399,fd=292))
[root@MiWiFi-R4A-srv conf.d]#
```

#Работаем в Kibana, читаем, сохраняем логии, делаем диаграммы

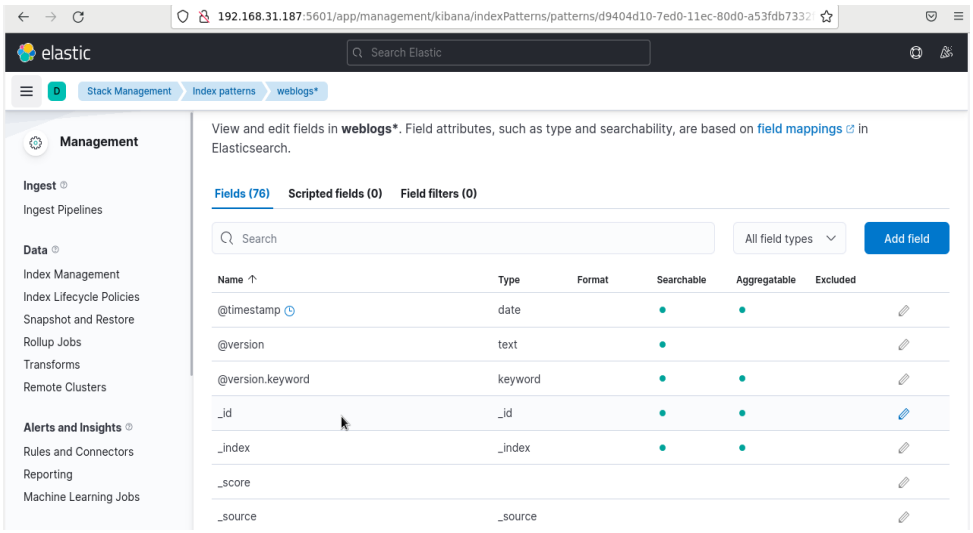
Создадим шаблон индекса

Заходим в левом меню во вкладку Discover

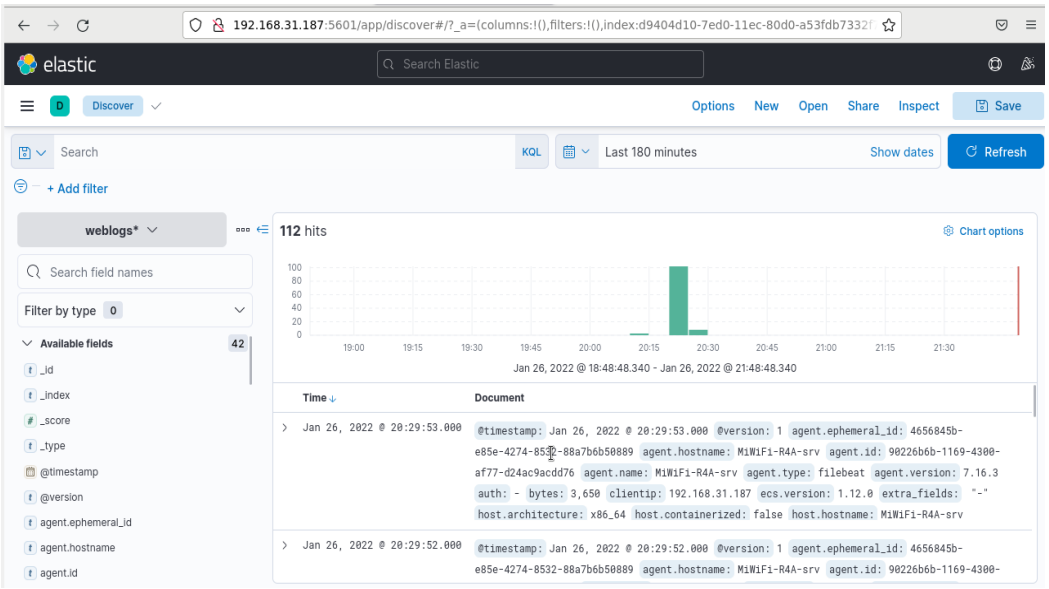




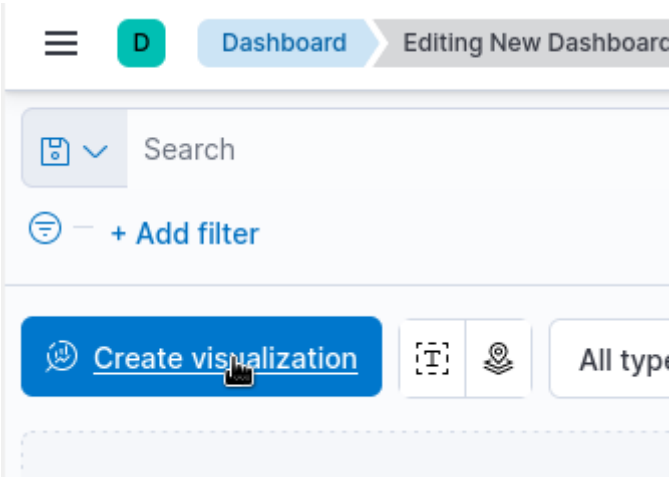
Здесь мы видим, что логи разобраны по полям, есть возможность поиска по ним, возможность агрегации.



Снова заходим в левом меню во вкладку Discover и видим отображаемые логи nginx.



Переходим во вкладку Dashboard, создать визуализацию



Создадим диаграмму частоты запросов

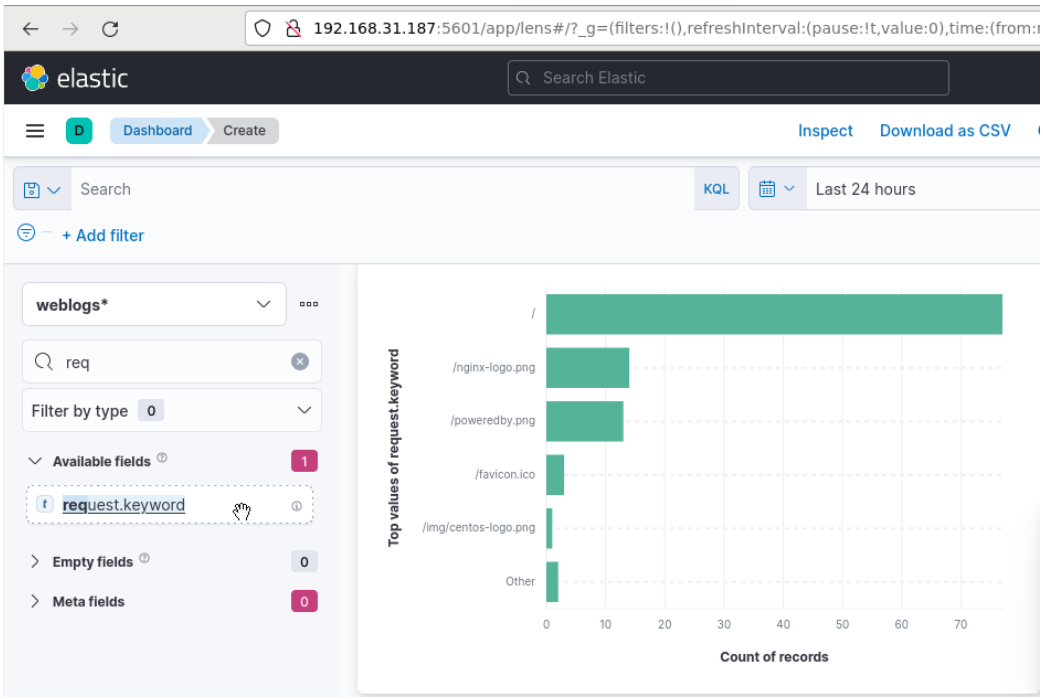


Диаграмма кодов ответов 200, 500,300,400 ошибок