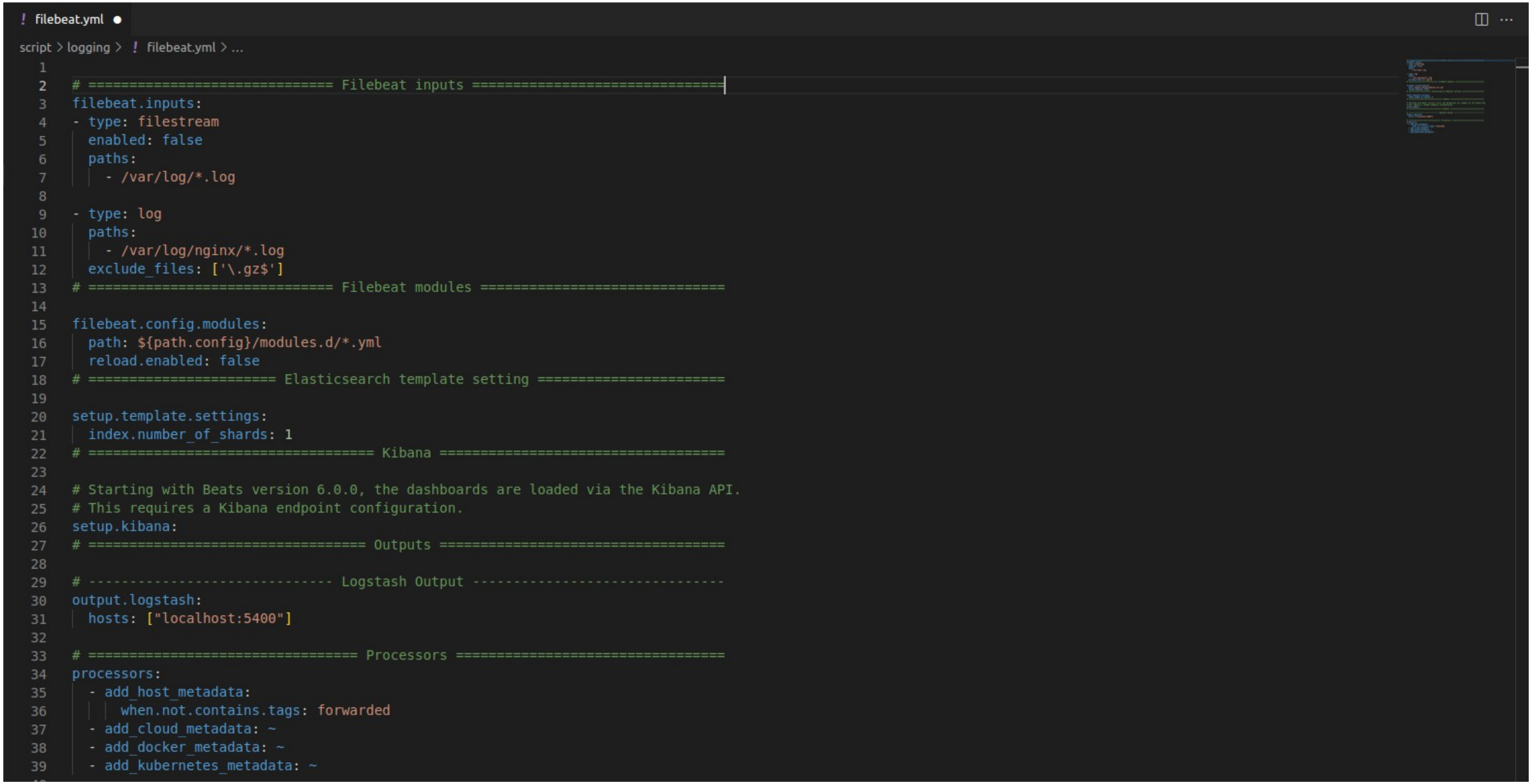
Стек ELK.

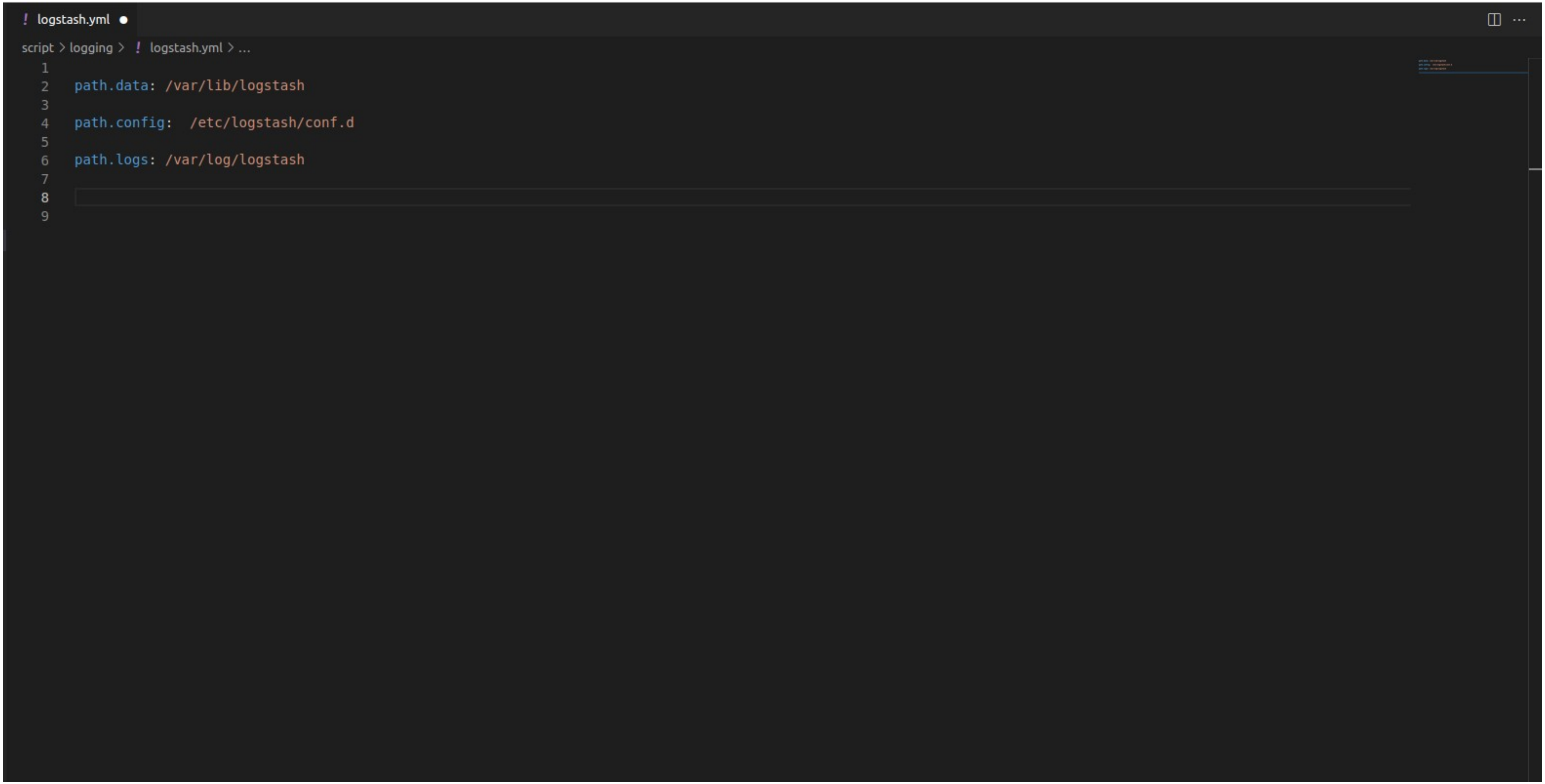
Задание:
Развернуть и настроить стек ELK на сервере с ОС Centos.

Конфигурационный файл filebeat



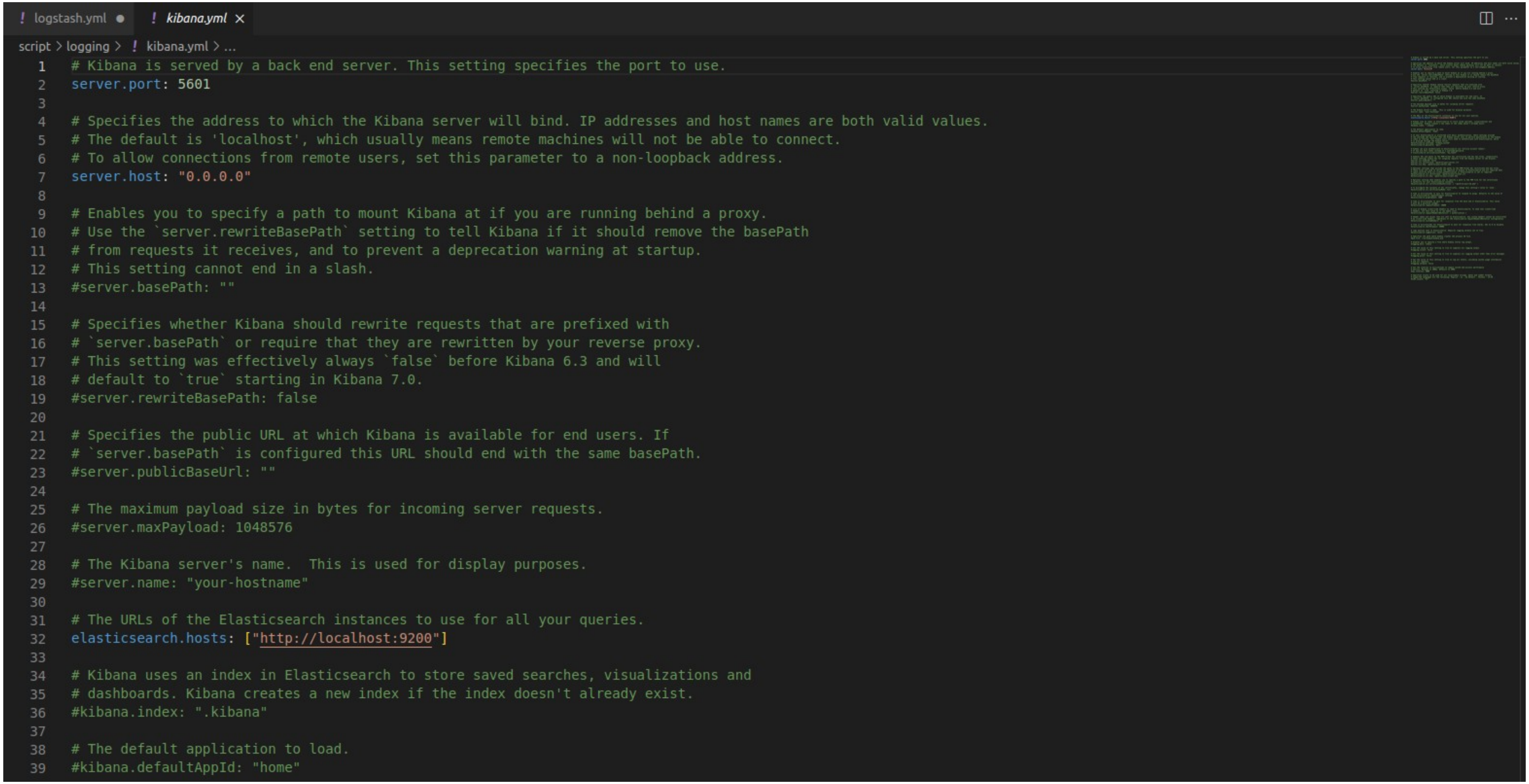
```yaml

# ============================== Filebeat inputs ===============================
filebeat.inputs:
- type: filestream
  enabled: false
  paths:
    - /var/log/*.log

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

filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
# ======================= Elasticsearch template setting =======================

setup.template.settings:
  index.number_of_shards: 1
# =================================== Kibana ===================================

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

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

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

Конфигурационный файл logstash



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

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

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

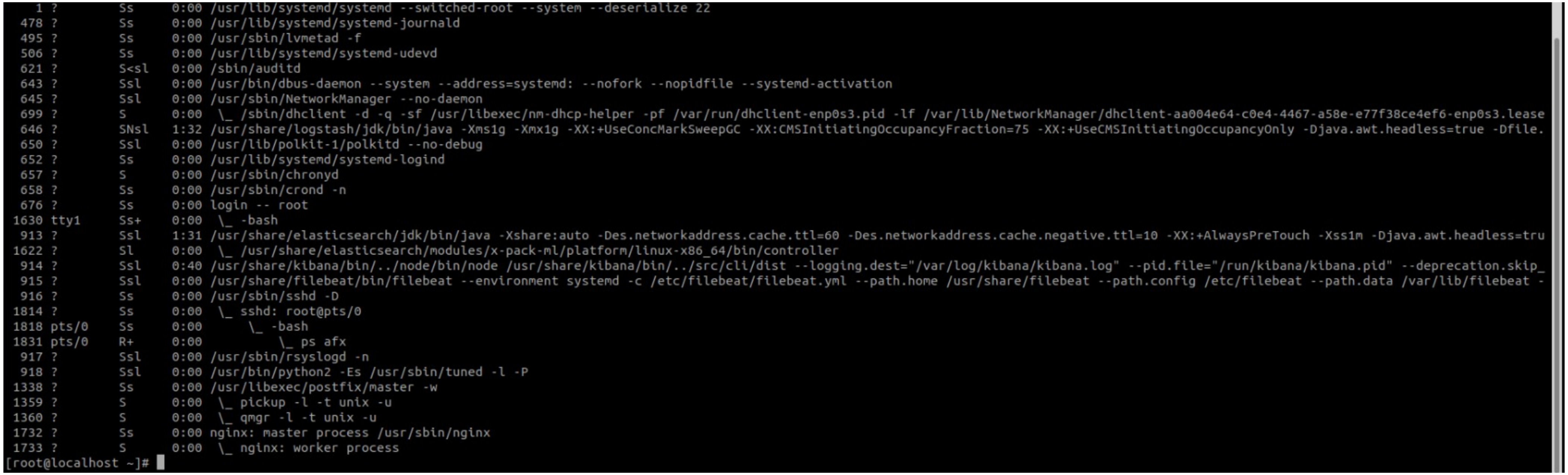
Конфигурационный файл kibana



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

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

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"
```

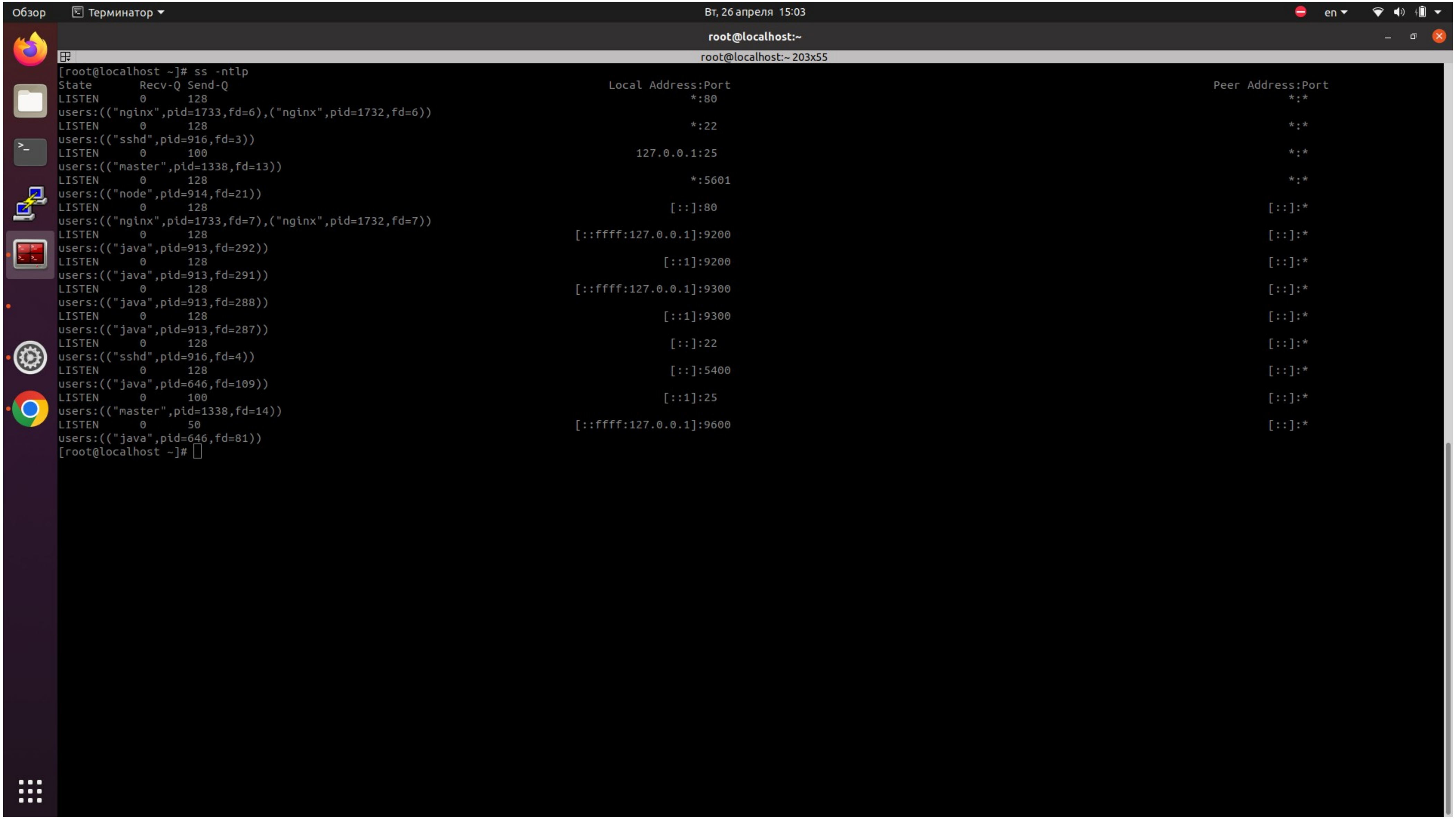
В процессах видно что запущенны:

- Elasticsearch
- Logstash
- Kibana
- Falebeat



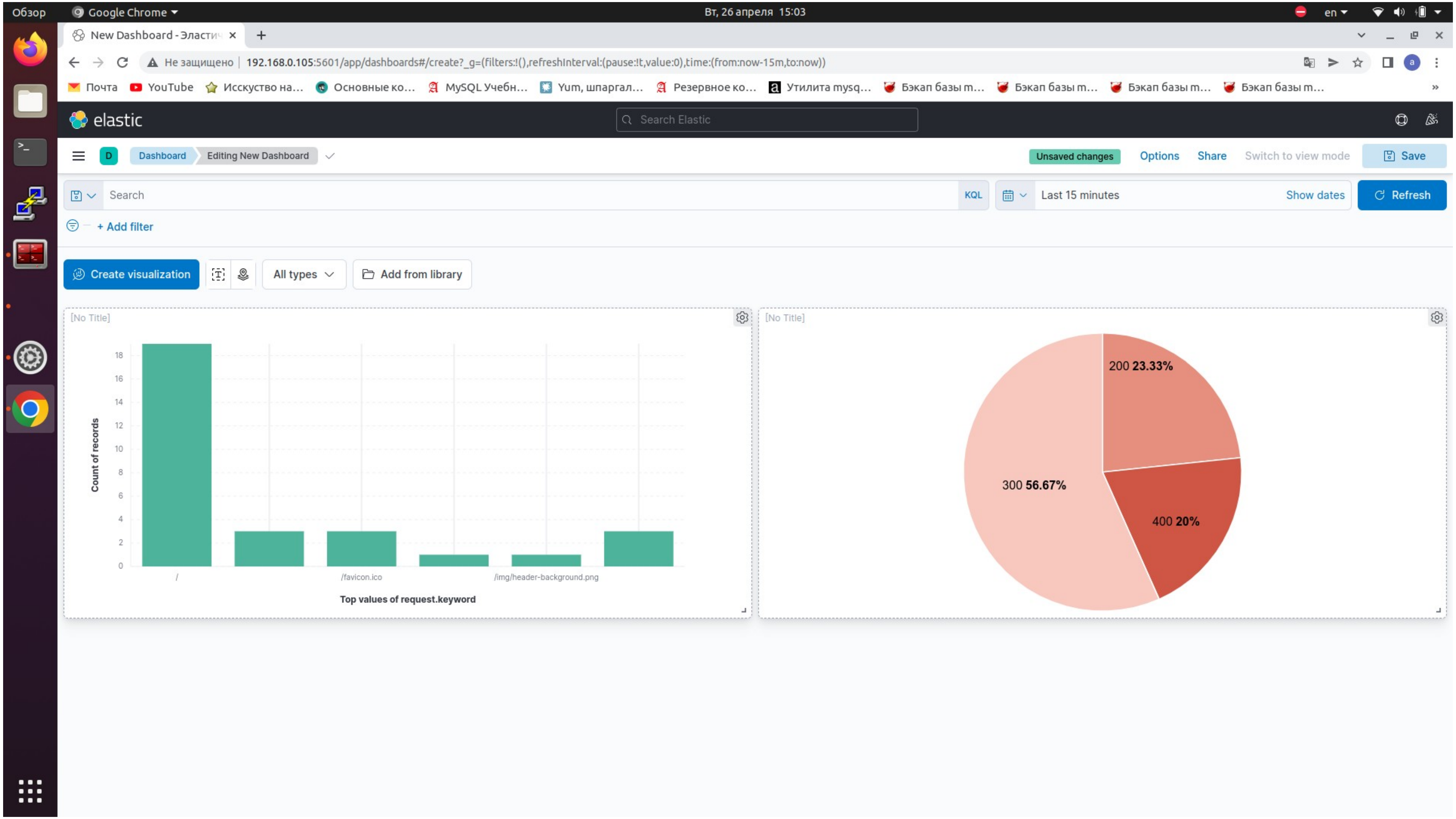
```
    1 ?        Ss     0:00 /usr/lib/systemd/systemd --switched-root --system --deserialize 22
  478 ?        Ss     0:00 /usr/lib/systemd/systemd-journald
  495 ?        Ss     0:00 /usr/sbin/lvmetad -f
  506 ?        Ss     0:00 /usr/lib/systemd/systemd-udevd
  621 ?        S<sl   0:00 /sbin/auditd
  643 ?        Ssl    0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
  645 ?        Ssl    0:00 /usr/sbin/NetworkManager --no-daemon
  699 ?        S      0:00  \_ /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf /var/run/dhclient-enp0s3.pid -lf /var/lib/NetworkManager/dhclient-aa004e64-c0e4-4467-a58e-e77f38ce4ef6-enp0s3.lease
  646 ?        SNsl   1:32 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.
  650 ?        Ssl    0:00 /usr/lib/polkit-1/polkitd --no-debug
  652 ?        Ss     0:00 /usr/lib/systemd/systemd-logind
  657 ?        S      0:00 /usr/sbin/chronyd
  658 ?        Ss     0:00 /usr/sbin/crond -n
  676 ?        Ss     0:00 login -- root
 1630 tty1     Ss+    0:00  \_ -bash
  913 ?        Ssl    1:31 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=tru
 1622 ?        Sl     0:00  \_ /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
  914 ?        Ssl    0:40 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest="/var/log/kibana/kibana.log" --pid.file="/run/kibana/kibana.pid" --deprecation.skip_
  915 ?        Ssl    0:00 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat --path.data /var/lib/filebeat -
  916 ?        Ss     0:00 /usr/sbin/sshd -D
 1814 ?        Ss     0:00  \_ sshd: root@pts/0
 1818 pts/0    Ss     0:00      \_ -bash
 1831 pts/0    R+     0:00          \_ ps afx
  917 ?        Ssl    0:00 /usr/sbin/rsyslogd -n
  918 ?        Ssl    0:00 /usr/bin/python2 -Es /usr/sbin/tuned -l -P
 1338 ?        Ss     0:00 /usr/libexec/postfix/master -w
 1359 ?        S      0:00  \_ pickup -l -t unix -u
 1360 ?        S      0:00  \_ qmgr -l -t unix -u
 1732 ?        Ss     0:00 nginx: master process /usr/sbin/nginx
 1733 ?        S      0:00  \_ nginx: worker process
[root@localhost ~]# 
```

Вывод команды ss -ntlp



```
[root@localhost ~]# ss -ntlp
State       Recv-Q Send-Q                                                        Local Address:Port                                                                        Peer Address:Port
LISTEN      0      128                                                                       *:80                                                                                     *:*
users:(("nginx",pid=1733,fd=6),("nginx",pid=1732,fd=6))
LISTEN      0      128                                                                       *:22                                                                                     *:*
users:(("sshd",pid=916,fd=3))
LISTEN      0      100                                                               127.0.0.1:25                                                                                     *:*
users:(("master",pid=1338,fd=13))
LISTEN      0      128                                                                       *:5601                                                                                   *:*
users:(("node",pid=914,fd=21))
LISTEN      0      128                                                                    [::]:80                                                                                  [::]:*
users:(("nginx",pid=1733,fd=7),("nginx",pid=1732,fd=7))
LISTEN      0      128                                                      [::ffff:127.0.0.1]:9200                                                                                [::]:*
users:(("java",pid=913,fd=292))
LISTEN      0      128                                                                   [::1]:9200                                                                                [::]:*
users:(("java",pid=913,fd=291))
LISTEN      0      128                                                      [::ffff:127.0.0.1]:9300                                                                                [::]:*
users:(("java",pid=913,fd=288))
LISTEN      0      128                                                                   [::1]:9300                                                                                [::]:*
users:(("java",pid=913,fd=287))
LISTEN      0      128                                                                    [::]:22                                                                                  [::]:*
users:(("sshd",pid=916,fd=4))
LISTEN      0      128                                                                    [::]:5400                                                                                [::]:*
users:(("java",pid=646,fd=109))
LISTEN      0      100                                                                   [::1]:25                                                                                  [::]:*
users:(("master",pid=1338,fd=14))
LISTEN      0      50                                                       [::ffff:127.0.0.1]:9600                                                                                [::]:*
users:(("java",pid=646,fd=81))
[root@localhost ~]# 
```

Для примера запущен nginx и создан dashboard по ошибкам 300 200 400



192.168.0.105:5601/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))