

Стек ELK.

Задание:

Развернуть и настроить стек ELK на сервере с ОС Centos.

В процессах видно что запущены:

- Elasticsearch
- Logstash
- Kibana
- Filebeat

```
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/lvmstat -f
506 ?      Ss      0:00 /usr/lib/systemd/systemd-udev
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 ?      Ssl     1:32 /usr/share/logstash/jdk/bin/java -Xmsig -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

```
Обзор Терминатор Вт, 26 апреля 15:03 root@localhost:~ root@localhost:~ 203x55
[root@localhost ~]# ss -ntlp
State      Recv-Q Send-Q           Local Address:Port           Peer Address:Port
LISTEN     0      128             *:80                          *:*
```

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 ~]#
```

Стек ELK настроен.
Для примера создан dashboard по ошибкам 300 200 400

