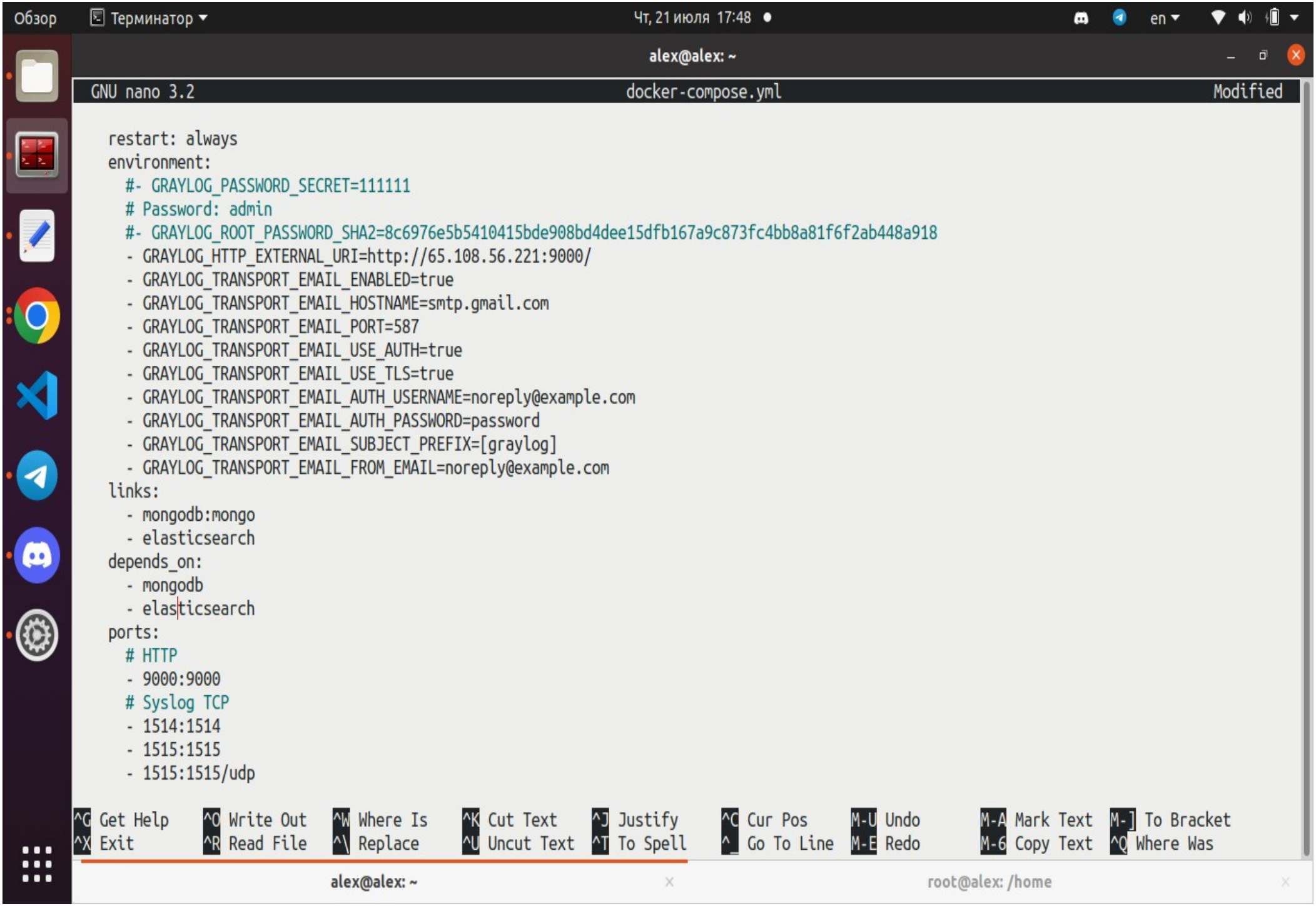
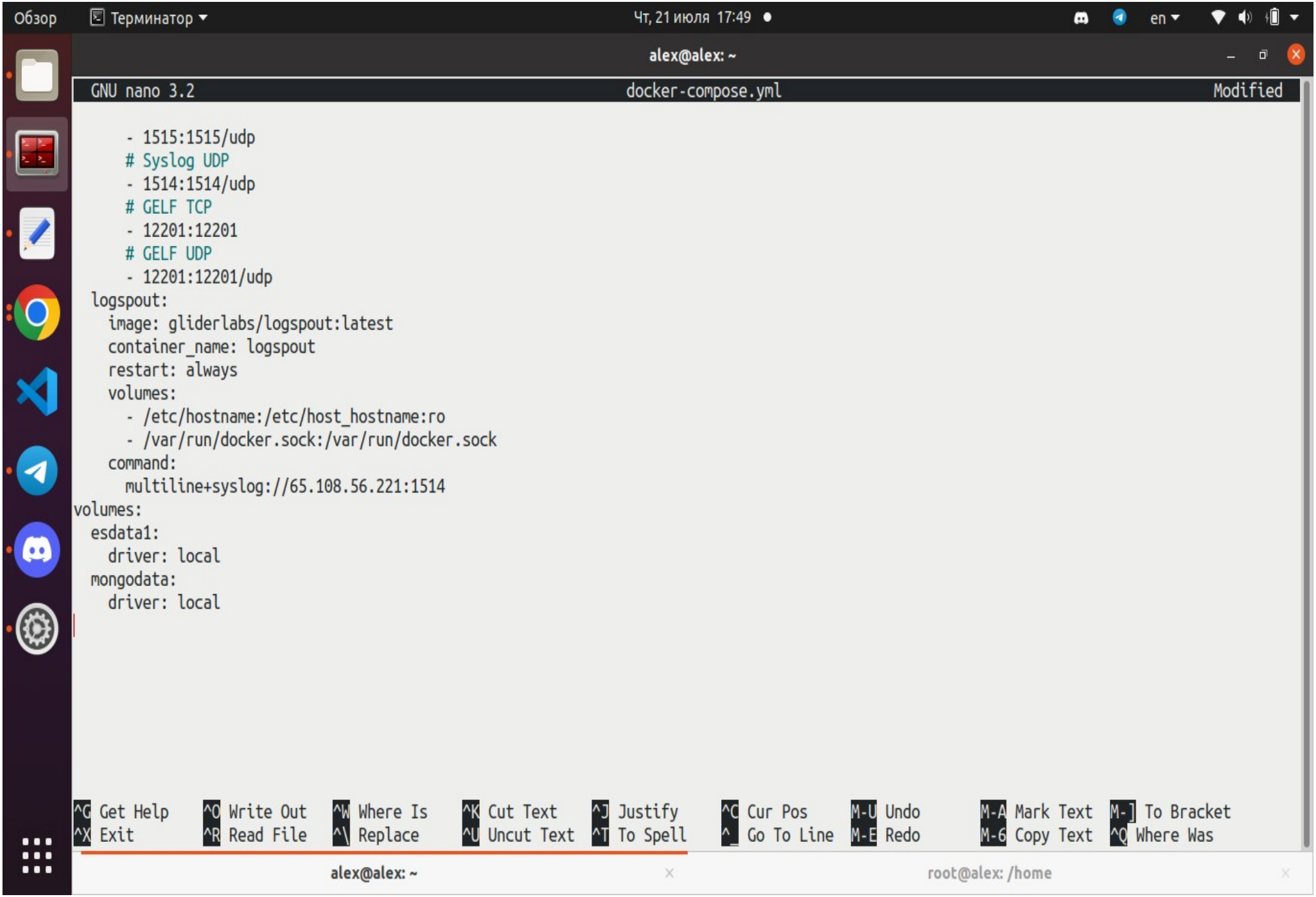
Graylog

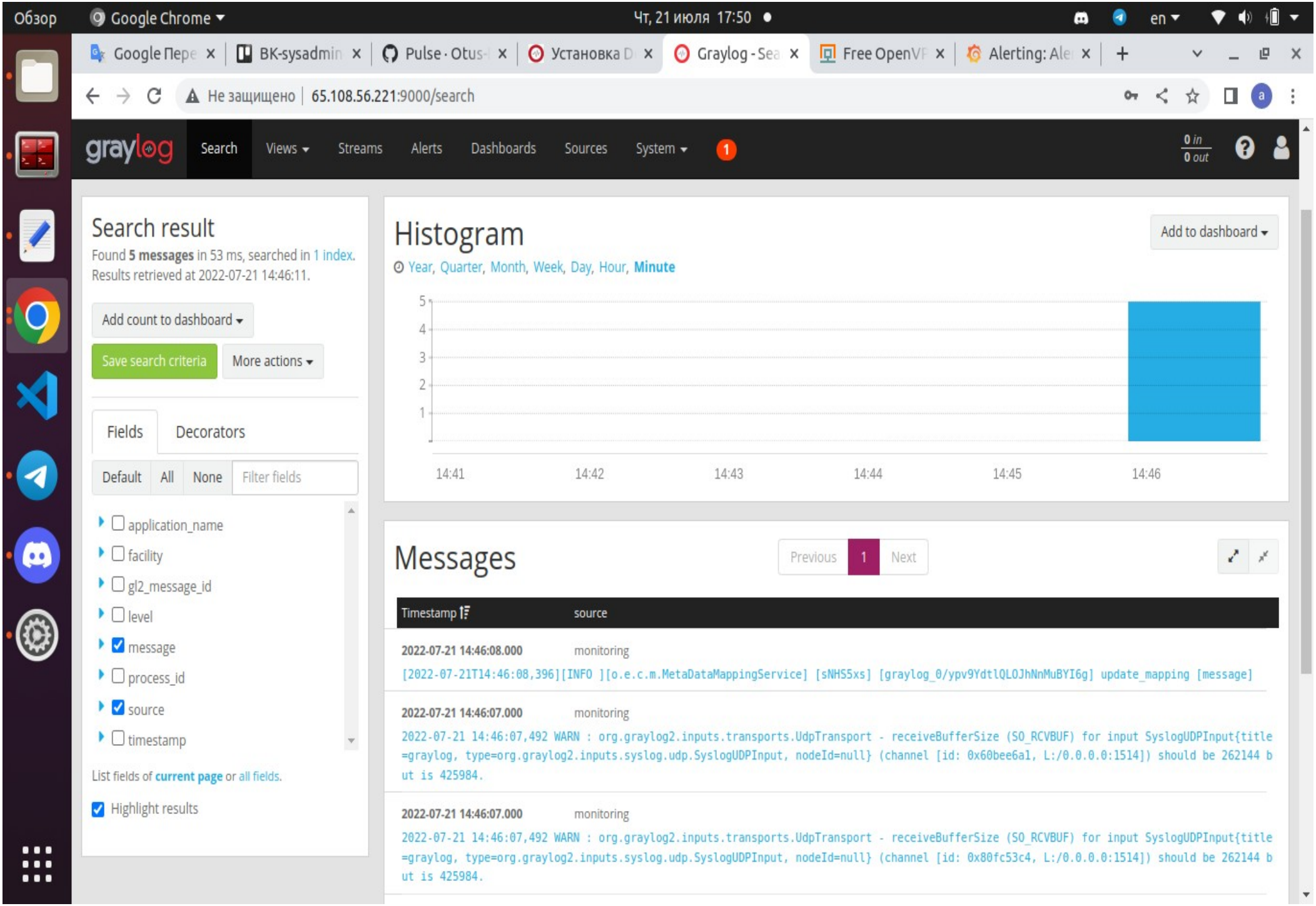
Задание.

- Собрать в Docker Compose систему бора логов на основе Graylog-Elasticsearch-Logspout


Обзор
Терминатор
Чт, 21 июля 17:48
en
alex@alex: ~
GNU nano 3.2
docker-compose.yml
Modified
version: '3'
services:
mongodb:
image: mongo:4.1
container_name: mongodb
restart: always
volumes:
- mongodata:/data/db:rw
elasticsearch:
image: docker.elastic.co/elasticsearch/elasticsearch-oss:6.8.2
container_name: elasticsearch
restart: always
environment:
- http.host=0.0.0.0
- transport.host=localhost
- network.host=0.0.0.0
- "ES_JAVA_OPTS=-Xms512m -Xmx512m"
ulimits:
memlock:
soft: -1
hard: -1
volumes:
- esdata1:/usr/share/elasticsearch/data:rw
graylog:
image: graylog/graylog:3.1
container_name: graylog
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was
alex@alex: ~
root@alex: /home


Обзор
Терминатор
Чт, 21 июля 17:48
en
alex@alex: ~
GNU nano 3.2
docker-compose.yml
Modified
restart: always
environment:
#- GRAYLOG_PASSWORD_SECRET=111111
Password: admin
#- GRAYLOG_ROOT_PASSWORD_SHA2=8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
- GRAYLOG_HTTP_EXTERNAL_URI=http://65.108.56.221:9000/
- GRAYLOG_TRANSPORT_EMAIL_ENABLED=true
- GRAYLOG_TRANSPORT_EMAIL_HOSTNAME=smtp.gmail.com
- GRAYLOG_TRANSPORT_EMAIL_PORT=587
- GRAYLOG_TRANSPORT_EMAIL_USE_AUTH=true
- GRAYLOG_TRANSPORT_EMAIL_USE_TLS=true
- GRAYLOG_TRANSPORT_EMAIL_AUTH_USERNAME=noreply@example.com
- GRAYLOG_TRANSPORT_EMAIL_AUTH_PASSWORD=password
- GRAYLOG_TRANSPORT_EMAIL_SUBJECT_PREFIX=[graylog]
- GRAYLOG_TRANSPORT_EMAIL_FROM_EMAIL=noreply@example.com
links:
- mongodb:mongo
- elasticsearch
depends_on:
- mongodb
- elasticsearch
ports:
HTTP
- 9000:9000
Syslog TCP
- 1514:1514
- 1515:1515
- 1515:1515/udp
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was
alex@alex: ~
root@alex: /home


Обзор
Терминатор
Чт, 21 июля 17:49
en
alex@alex: ~
GNU nano 3.2
docker-compose.yml
Modified
- 1515:1515/udp
Syslog UDP
- 1514:1514/udp
GELF TCP
- 12201:12201
GELF UDP
- 12201:12201/udp
logspout:
image: gliderlabs/logspout:latest
container_name: logspout
restart: always
volumes:
- /etc/hostname:/etc/host_hostname:ro
- /var/run/docker.sock:/var/run/docker.sock
command:
multiline+syslog://65.108.56.221:1514
volumes:
esdata1:
driver: local
mongodata:
driver: local
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was
alex@alex: ~
root@alex: /home


Обзор
Google Chrome
Чт, 21 июля 17:50
en
Graylog - Sea
Free OpenVF
Alerting: Ale
Не защищено
65.108.56.221:9000/search
graylog
Search
Views
Streams
Alerts
Dashboards
Sources
System
0 in
0 out
Search result
Found 5 messages in 53 ms, searched in 1 index.
Results retrieved at 2022-07-21 14:46:11.
Add count to dashboard
Save search criteria
More actions
Fields
Decorators
Default
All
None
Filter fields
application_name
facility
gl2_message_id
level
message
process_id
source
timestamp
List fields of current page or all fields.
Highlight results
Histogram
Add to dashboard
Year, Quarter, Month, Week, Day, Hour, Minute
5
4
3
2
1
14:41
14:42
14:43
14:44
14:45
14:46
Messages
Previous
1
Next
Timestamp
source
2022-07-21 14:46:08.000
monitoring
[2022-07-21T14:46:08,396][INFO][o.e.c.m.MetaDataMappingService] [sNHS5xs] [graylog_0/ypv9YdtlQLOJhNnMuBYI6g] update_mapping [message]
2022-07-21 14:46:07.000
monitoring
2022-07-21 14:46:07,492 WARN : org.graylog2.inputs.transports.UdpTransport - receiveBufferSize (SO_RCVBUF) for input SyslogUDPInput{title=graylog, type=org.graylog2.inputs.syslog.udp.SyslogUDPInput, nodeId=null} (channel [id: 0x60bee6a1, L:/0.0.0.0:1514]) should be 262144 but is 425984.
2022-07-21 14:46:07.000
monitoring
2022-07-21 14:46:07,492 WARN : org.graylog2.inputs.transports.UdpTransport - receiveBufferSize (SO_RCVBUF) for input SyslogUDPInput{title=graylog, type=org.graylog2.inputs.syslog.udp.SyslogUDPInput, nodeId=null} (channel [id: 0x80fc53c4, L:/0.0.0.0:1514]) should be 262144 but is 425984.