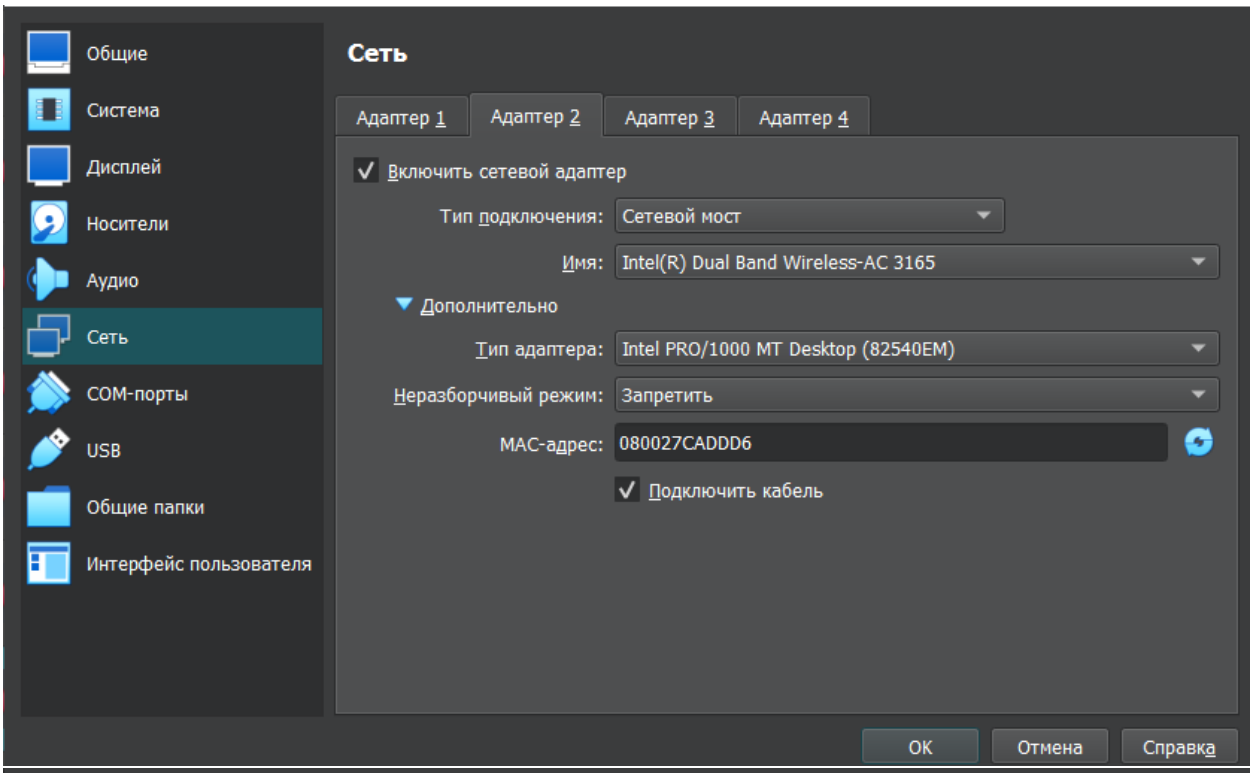
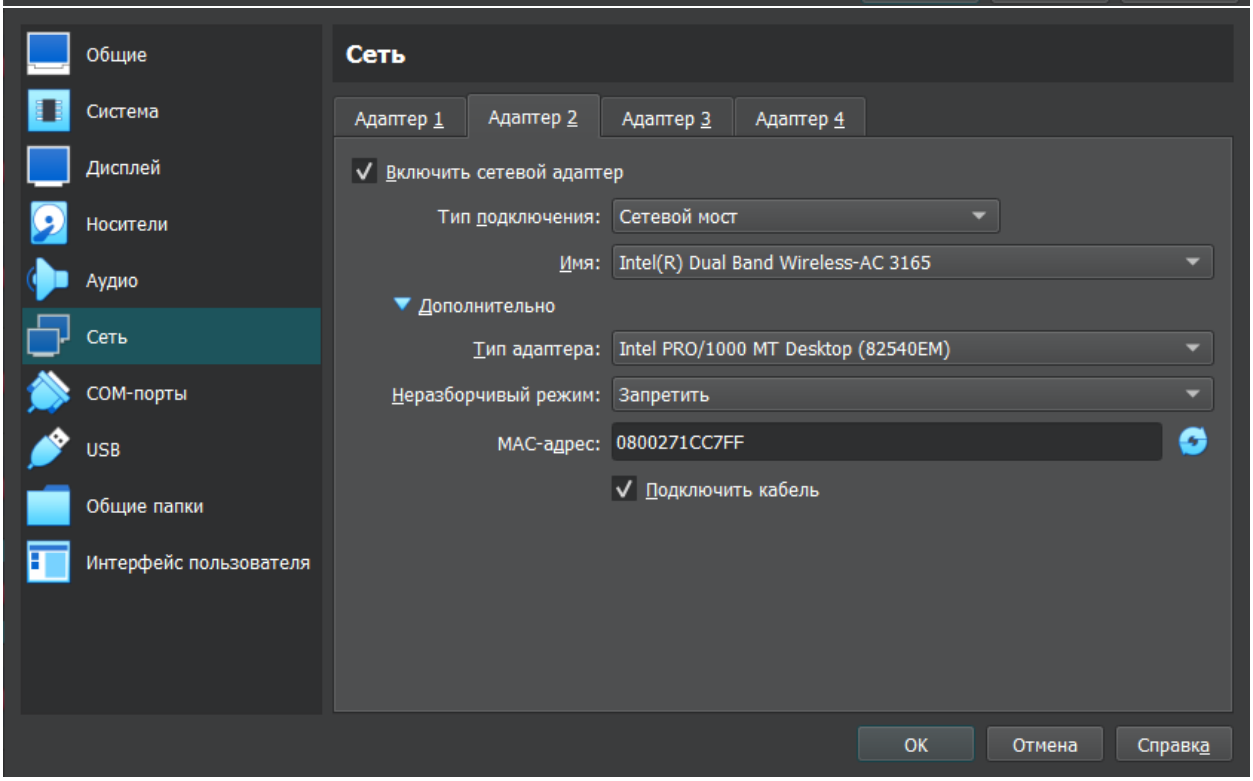
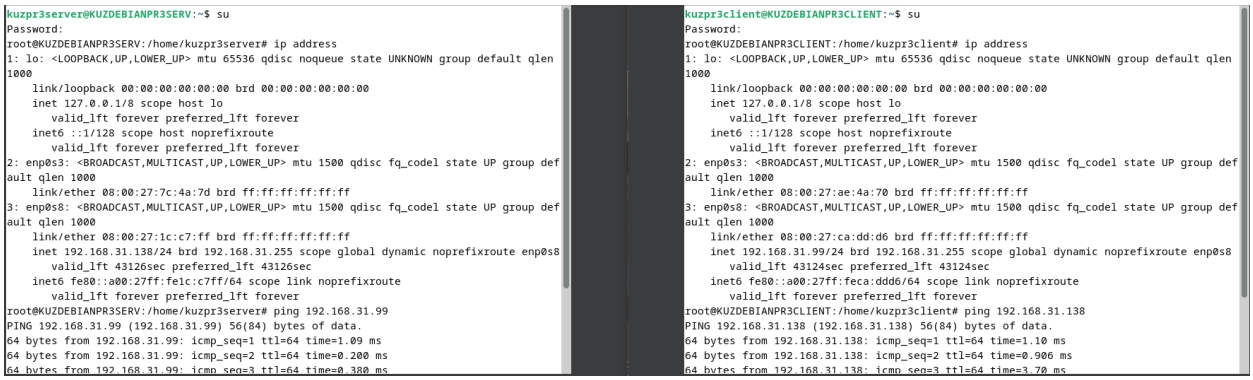
Практика № 1

Выполнил Лялин Илья ББМО-02-24

1. Создадим 2 виртуальные машины на базе ОС Debian 12 и обеспечим между ними сетевой обмен с помощью сетевого моста

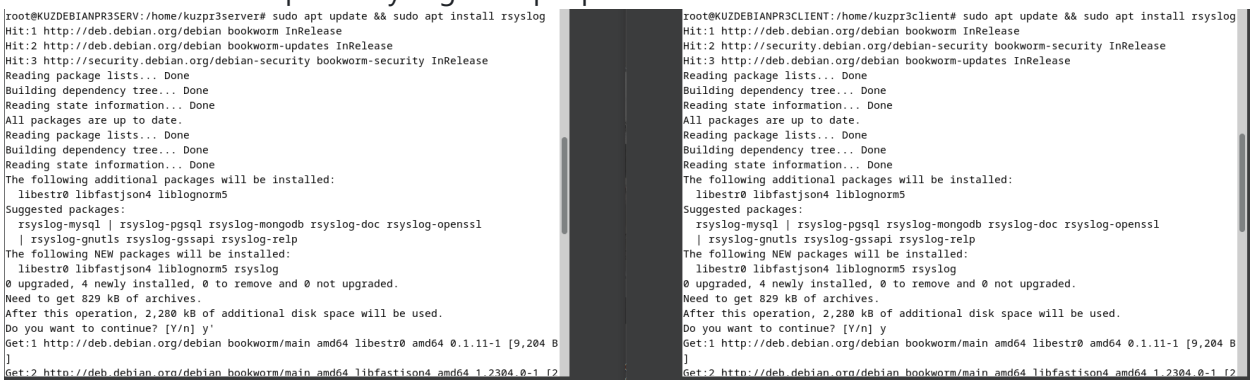






2. Включим на 1-й (серверной) ВМ передачу логов по протоколу rsyslog на 2-ю ВМ (клиент)

2.1 Установим и настроим rsyslog на сервере и клиенте



2.2 Проверим работоспособность rsyslog на сервере и клиенте

2.3 Включим UDP и TCP соединения

2.4 Установим правила на сервере

```
 GNU nano 7.2                        /etc/rsyslog.conf *
*.*;auth,authpriv.none          -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                 /var/log/auth.log
cron.*                          -/var/log/cron.log
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

template(name="RemoteLogs" type="string" string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log>
*.* ?RemoteLogs
& stop
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line
```

2.5 Установим правила на клиенте

```
 GNU nano 7.2                         /etc/rsyslog.conf *
#
# Log anything besides private authentication messages to a single log file
#
*.*;auth,authpriv.none          -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                 /var/log/auth.log
cron.*                          -/var/log/cron.log
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

*.* @@192.168.31.138:514

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

2.6 Проверим получения логов на сервере

```
root@KUZDEBIANPR3SERV:/home/kuzpr3server# sudo systemctl restart rsyslog
root@KUZDEBIANPR3SERV:/home/kuzpr3server# sudo ss -tulnp | grep "rsyslog"
udp   UNCONN 0      0            0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid
=3420,fd=6))
udp   UNCONN 0      0               [::]:514           [::]:*    users:(("rsyslogd",pid
=3420,fd=7))
tcp   LISTEN 0      25           0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid
=3420,fd=8))
tcp   LISTEN 0      25              [::]:514           [::]:*    users:(("rsyslogd",pid
=3420,fd=9))
root@KUZDEBIANPR3SERV:/home/kuzpr3server#
```

```
TriggeredBy: • syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 3446 (rsyslogd)
      Tasks: 10 (limit: 9454)
     Memory: 3.1M
        CPU: 22ms
     CGroup: /system.slice/rsyslog.service
             └─3446 /usr/sbin/rsyslogd -n -iNONE

Nov 21 17:00:17 KUZDEBIANPR3SERV systemd[1]: Starting rsyslog.service - System Logging>
Nov 21 17:00:17 KUZDEBIANPR3SERV systemd[1]: Started rsyslog.service - System Logging >
Nov 21 17:00:17 KUZDEBIANPR3SERV rsyslogd[3446]: imuxsock: Acquired UNIX socket '/run/>
Nov 21 17:00:17 KUZDEBIANPR3SERV rsyslogd[3446]: [origin software="rsyslogd" swVersion>
lines 1-18/18 (END)
root@KUZDEBIANPR3SERV:/home/kuzpr3server# ls /var/log
alternatives.log  cups            journal             README
apt               dpkg.log        kern.log            speech-dispatcher
auth.log          faillog         KUZDEBIANPR3CLIENT  syslog
boot.log          fontconfig.log  KUZDEBIANPR3SERV    user.log
btmp              gdm3            lastlog             vboxpostinstall.log
cron.log          installer       private             wtmp
root@KUZDEBIANPR3SERV:/home/kuzpr3server#
```

3. Установим и настроим получение логов на сервер с использованием Loki

3.1 Установим и отредактируем docker compose файл на сервере

```
root@KUZDEBIANPR3SERV:/home/kuzpr3server# mkdir /loki
root@KUZDEBIANPR3SERV:/home/kuzpr3server# cd /loki
root@KUZDEBIANPR3SERV:/loki# wget https://raw.githubusercontent.com/grafana/loki/v2.9.1
/production/docker-compose.yaml -O docker-compose.yaml
--2023-11-21 17:04:21--  https://raw.githubusercontent.com/grafana/loki/v2.9.1/producti
on/docker-compose.yaml
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185
.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:44
3... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1073 (1.0K) [text/plain]
Saving to: 'docker-compose.yaml'

docker-compose.yaml   100%[========================>]   1.05K  --.-KB/s    in 0s

2023-11-21 17:04:21 (55.3 MB/s) - 'docker-compose.yaml' saved [1073/1073]

root@KUZDEBIANPR3SERV:/loki# ls -l
total 4
-rw-r--r-- 1 root root 1073 Nov 21 17:04 docker-compose.yaml
root@KUZDEBIANPR3SERV:/loki#
```

```
version: "3"

networks:
  loki:

services:
  loki:
    image: grafana/loki:2.9.0
    ports:
      - "3100:3100"
    command: -config.file=/etc/loki/local-config.yaml
    networks:
      - loki

  grafana:
    environment:
      - GF_PATHS_PROVISIONING=/etc/grafana/provisioning
      - GF_AUTH_ANONYMOUS_ENABLED=true
      - GF_AUTH_ANONYMOUS_ORG_ROLE=Admin
    entrypoint:

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

3.2 Запустим Loki

```
[+] Running 18/18
 ✔ grafana 10 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿]      0B/0B      Pulled                          45.1s
   ✔ 96526aa774ef Pull complete                                                          3.8s
   ✔ 932a65841cb5 Pull complete                                                          4.0s
   ✔ a486d8a79b5f Pull complete                                                          4.4s
   ✔ 9f17a73c904a Pull complete                                                          5.0s
   ✔ c1ade82e0f62 Pull complete                                                          4.6s
   ✔ 882619e0a642 Pull complete                                                          5.1s
   ✔ 2f0808654570 Pull complete                                                         17.6s
   ✔ df5835f957f7 Pull complete                                                         15.6s
   ✔ b94284e881a5 Pull complete                                                          6.0s
   ✔ 3e944d3294a3 Pull complete                                                          7.6s
 ✔ loki 6 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿]      0B/0B      Pulled                                  12.2s
   ✔ 31e352740f53 Pull complete                                                          1.8s
   ✔ 8b1f00c5e787 Pull complete                                                          1.3s
   ✔ a91d5e9859cb Pull complete                                                          3.5s
   ✔ 970cece5abde Pull complete                                                          2.2s
   ✔ 4afc9154faa4 Pull complete                                                          2.5s
   ✔ 0da8239be4a8 Pull complete                                                          2.9s
[+] Running 3/3
 ✔ Network loki_loki          Created                                                   0.3s
 ✔ Container loki-grafana-1   Started                                                   1.3s
 ✔ Container loki-loki-1      Started                                                   1.3s
root@KUZDEBIANPR3SERV:/loki#
```

3.3 Отредактируем promtail-config на клиенте

```
  GNU nano 7.2                        promtail-config.yaml *
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://192.168.31.138:3100/loki/api/v1/push

scrape_configs:
- job_name: system
  static_configs:
  - targets:
    - localhost
    labels:
      lob: varlogs
      __path__: /var/log/*log


^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

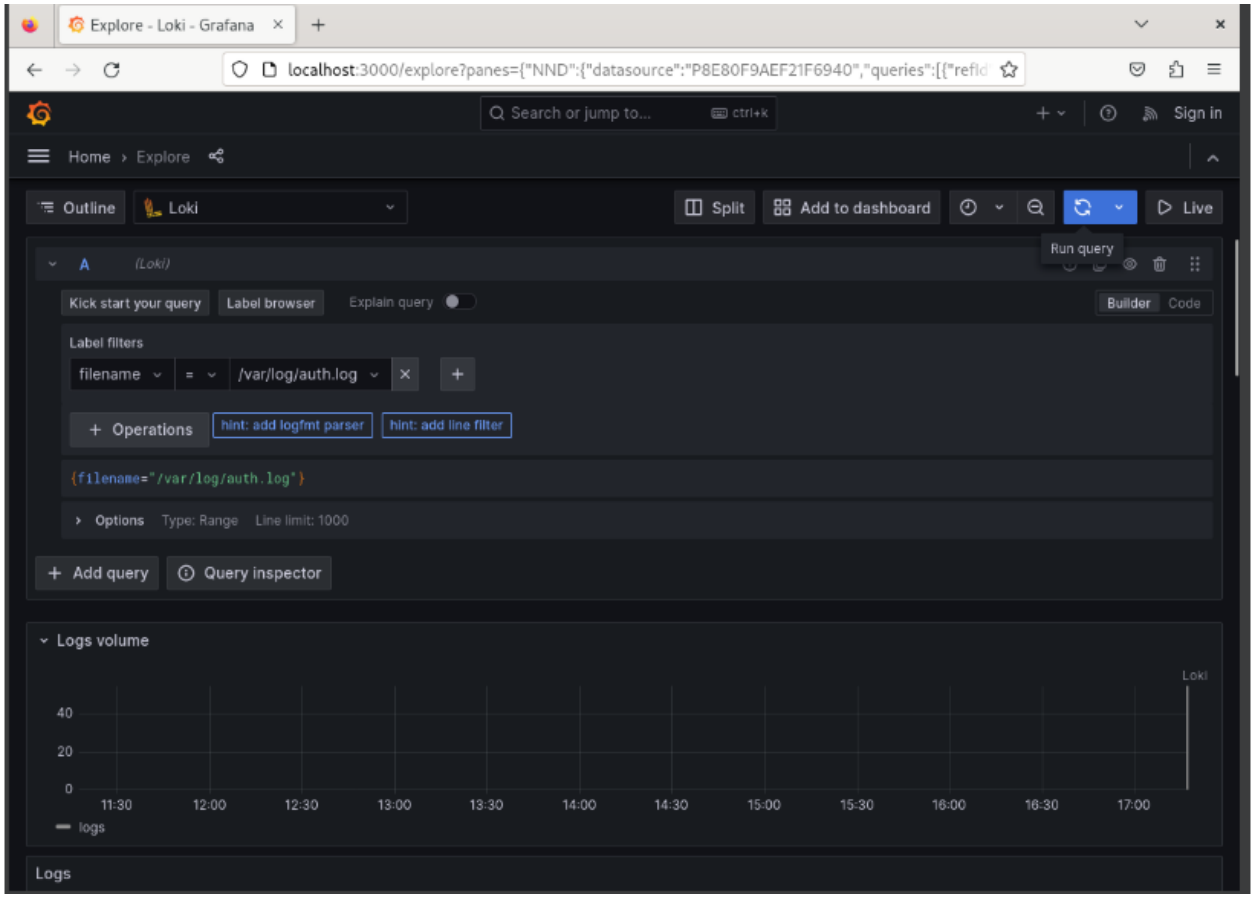
3.4 Отредактируем docker compose файл для promtail

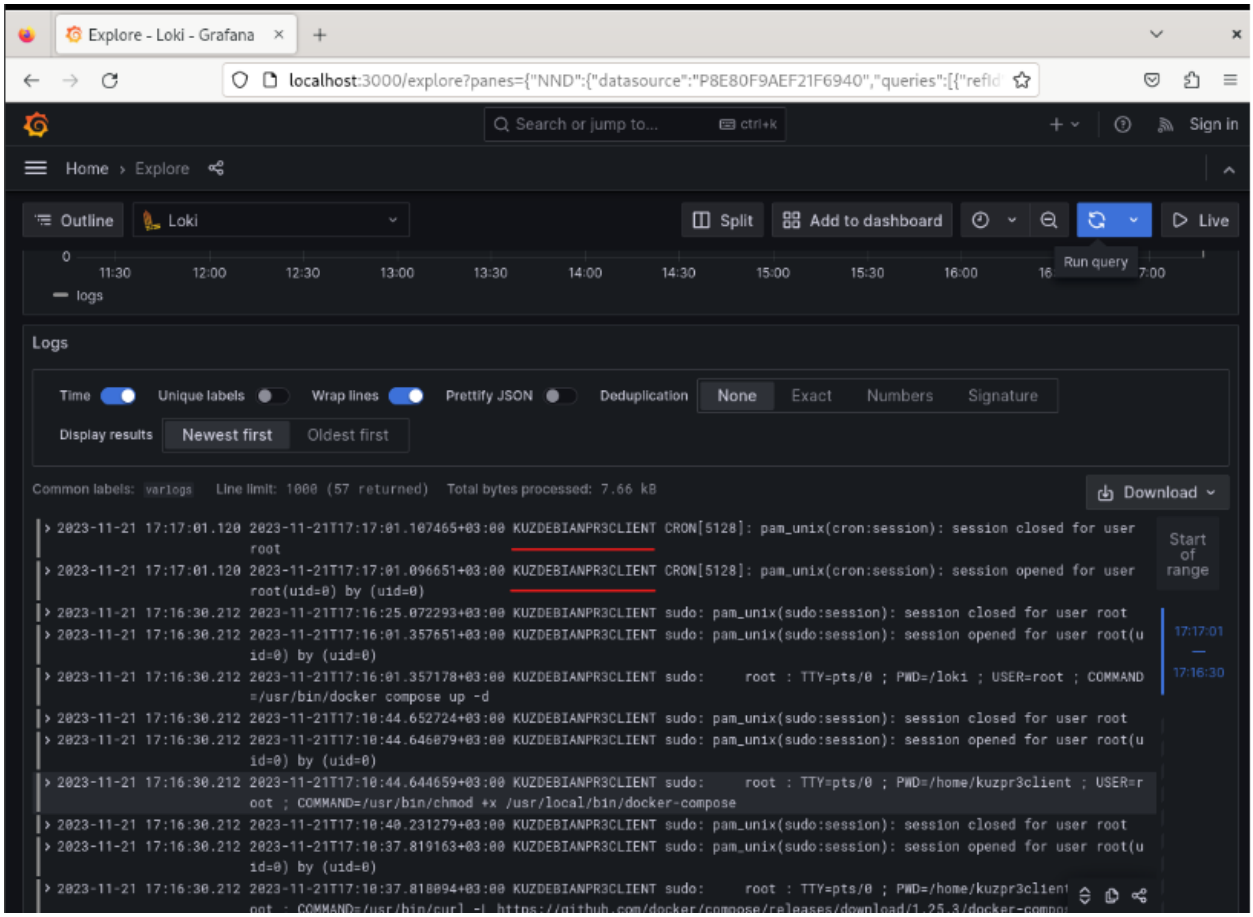
```
 GNU nano 7.2                    docker-compose.yaml *
version: "3"

services:
  promtail:
    image: grafana/promtail:2.9.0
    volumes:
      - /var/log:/var/log
      - ./promtail-config.yaml:/etc/promtail/config.yml
    command: -config.file=/etc/promtail/config.yml

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

3.5 Запустим promtail на клиенте

```
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 16.4M  100 16.4M    0     0  7073k      0  0:00:02  0:00:02 --:--:-- 8135k
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# sudo chmod +x /usr/local/bin/docker-compose
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# docker-compose --version
docker-compose version 1.25.3, build d4d1b42b
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# cd /loki
bash: cd: /loki: No such file or directory
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# mkdir /loki
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# cd /loki
root@KUZDEBIANPR3CLIENT:/loki# nano promtail-config.yaml
root@KUZDEBIANPR3CLIENT:/loki# nano docker-compose.yaml
root@KUZDEBIANPR3CLIENT:/loki# sudo docker compose up -d
[+] Running 7/7
 ✔ promtail 6 layers [⣿⣿⣿⣿⣿⣿]      0B/0B      Pulled                          21.8s
   ✔ 7d97e254a046 Pull complete                                              7.4s
   ✔ 39932bcaa1cc Pull complete                                              0.7s
   ✔ 4059d897dde4 Pull complete                                              3.4s
   ✔ 325d59b59788 Pull complete                                              2.3s
   ✔ 9e9c5b842176 Pull complete                                              9.8s
   ✔ 01befd6b403e Pull complete                                              4.3s
[+] Running 2/2
 ✔ Network loki_default       Created                                       0.2s
 ✔ Container loki-promtail-1  Started                                       0.9s
root@KUZDEBIANPR3CLIENT:/loki#
```

3.6 Просмотрим логи клиента в Grafana





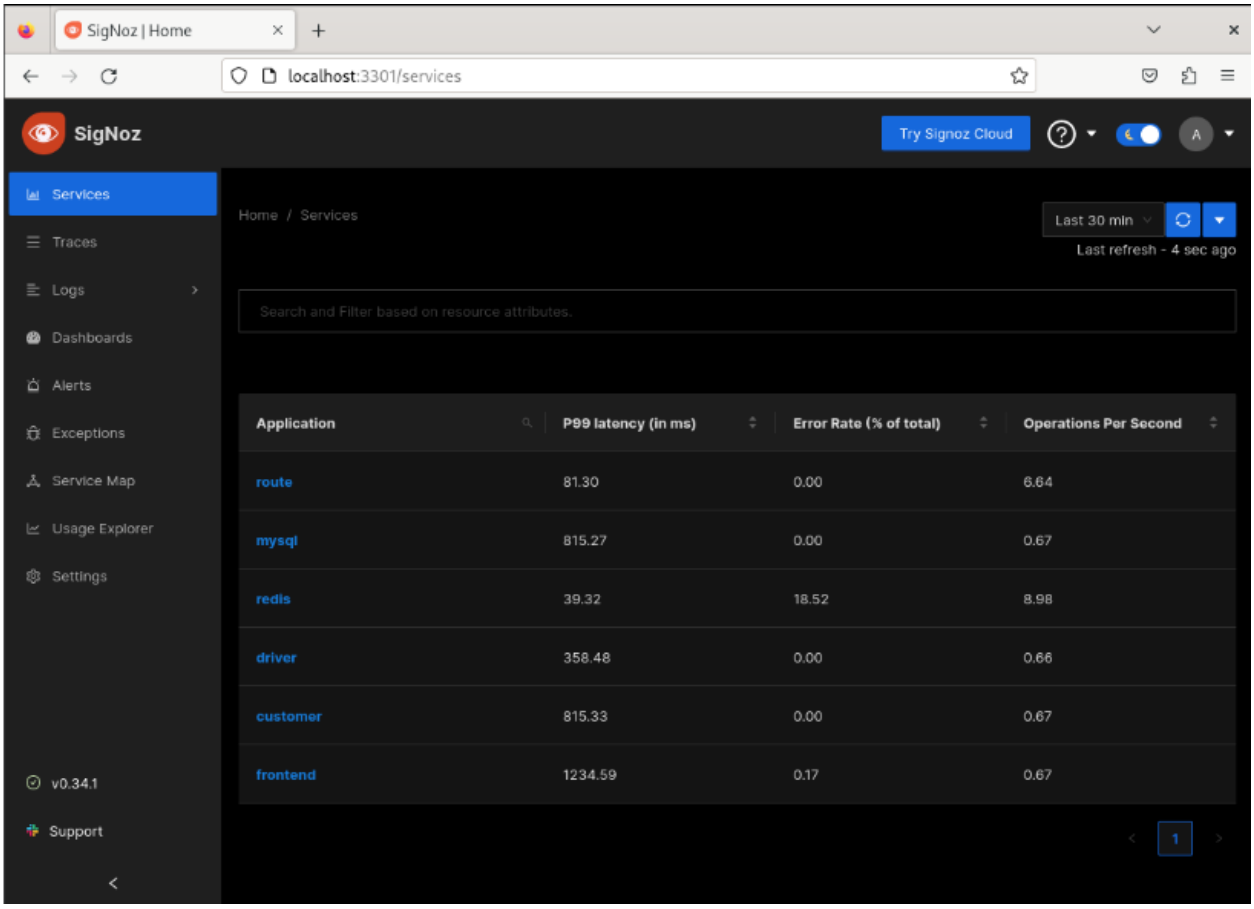
4. Установим и настроим получение логов на сервере с использованием Signoz

   Установка Signoz по инструкции с сайта: https://signoz.io/docs/install/docker/#install-signoz-using-docker-compose

   4.1 Запустим Signoz

```
root@KUZDEBIANPR3SERV:/signoz# mkdir /deploy
root@KUZDEBIANPR3SERV:/signoz# cd /deploy
root@KUZDEBIANPR3SERV:/deploy# mkdir /signoz/deploy
root@KUZDEBIANPR3SERV:/deploy# cd /deploy
root@KUZDEBIANPR3SERV:/deploy# cd /signoz/deploy
root@KUZDEBIANPR3SERV:/signoz/deploy# git clone -b main https://github.com/SigNoz/signoz.git && cd signoz/deploy/
Cloning into 'signoz'...
remote: Enumerating objects: 40610, done.
remote: Counting objects: 100% (3664/3664), done.
remote: Compressing objects: 100% (1790/1790), done.
remote: Total 40610 (delta 2084), reused 3218 (delta 1762), pack-reused 36946
Receiving objects: 100% (40610/40610), 53.84 MiB | 3.75 MiB/s, done.
Resolving deltas: 100% (25503/25503), done.
root@KUZDEBIANPR3SERV:/signoz/deploy/signoz/deploy# cd docker
root@KUZDEBIANPR3SERV:/signoz/deploy/signoz/deploy/docker# cd clickhouse-setup
root@KUZDEBIANPR3SERV:/signoz/deploy/signoz/deploy/docker/clickhouse-setup# sudo docker compose up -d
[+] Running 16/27
 ⠸ alertmanager 7 layers [⣿⣿⣿⣿⣿⣿⣿]      0B/0B      Pulling                                                16.2s
 ⠸ otel-collector-metrics 4 layers [⣿⣿⣦⡀] 9.946MB/46.44MB Pulling                                          16.2s
 ⠸ query-service 4 layers [    ]      0B/0B      Pulling                                                    16.2s
 ⠸ load-hotrod 7 layers [       ]      0B/0B      Pulling                                                   16.2s
 ⠸ logspout 3 layers [⣿⣿⣿]      0B/0B      Pulling                                                          16.2s
 ⠸ otel-collector Pulling                                                                                  16.2s
 ⠸ hotrod 1 layers [ ]      0B/0B      Pulling                                                             16.2s
 ⠸ frontend 12 layers [⣿⣿          ]      0B/0B      Pulling                                                16.2s
 ⠸ otel-collector-migrator 3 layers [   ]      0B/0B      Pulling                                           16.2s
 ⠸ zookeeper-1 1 layers [ ] 4.302MB/273.6MB Pulling                                                        16.2s
 ⠸ clickhouse 7 layers [⣿      ]      0B/0B      Pulling                                                    16.2s
```

```
[+] Running 12/12
 ✔ Network clickhouse-setup_default          Created                                                       0.5s
 ✔ Container load-hotrod                     Started                                                       2.5s
 ✔ Container signoz-zookeeper-1              Started                                                       2.4s
 ✔ Container hotrod                          Started                                                       2.4s
 ✔ Container signoz-clickhouse               Healthy                                                       0.3s
 ✔ Container otel-migrator                   Exited                                                        0.2s
 ✔ Container signoz-query-service            Healthy                                                       0.3s
 ✔ Container signoz-otel-collector-metrics   Started                                                       0.3s
 ✔ Container signoz-alertmanager             Started                                                       0.4s
 ✔ Container signoz-otel-collector           Started                                                       0.3s
 ✔ Container signoz-logspout                 Started                                                       0.4s
 ✔ Container signoz-frontend                 Started                                                       0.3s
root@KUZDEBIANPR3SERV:/signoz/deploy/signoz/deploy/docker/clickhouse-setup#
```



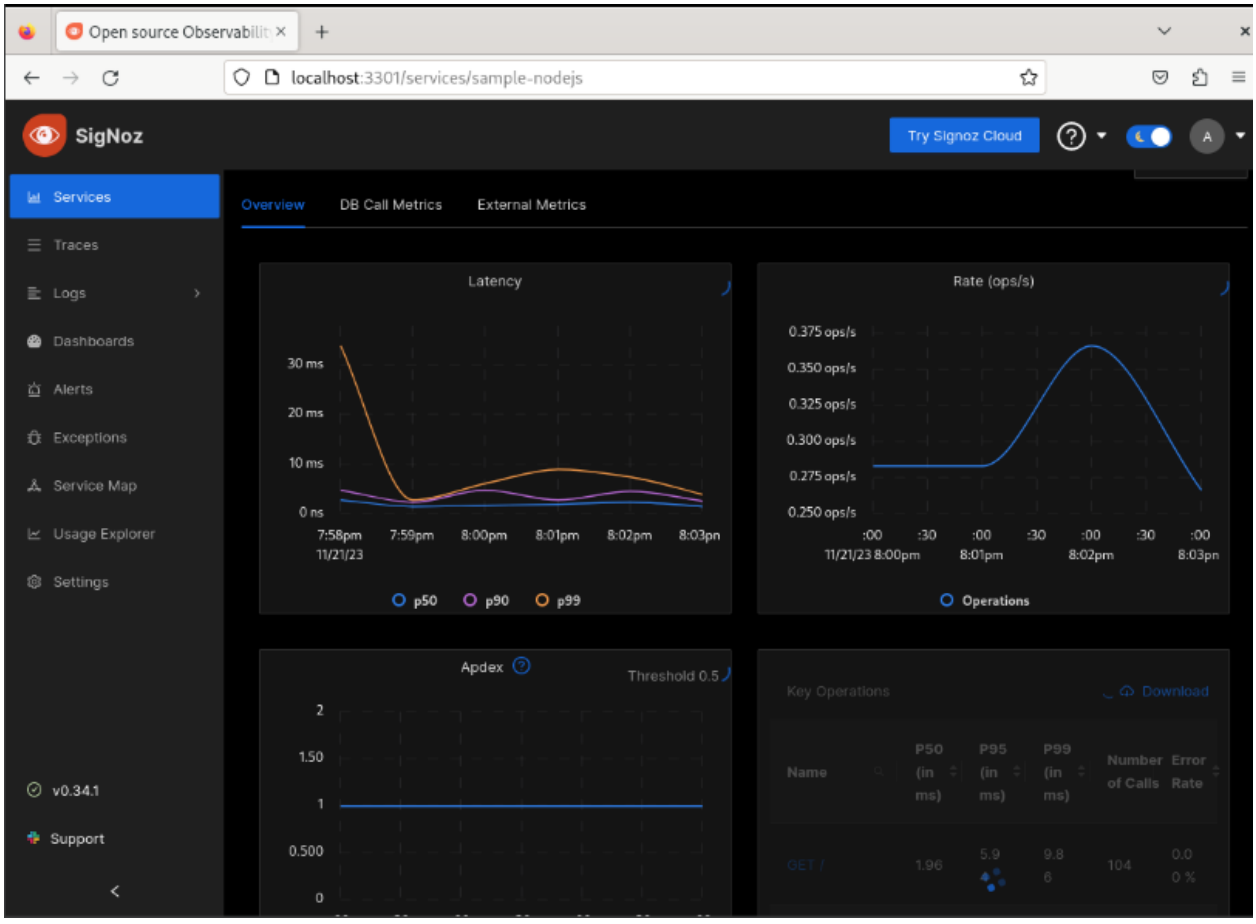
4.2 Отредактируем конфигурации на клиенте для отправки данных в Signoz

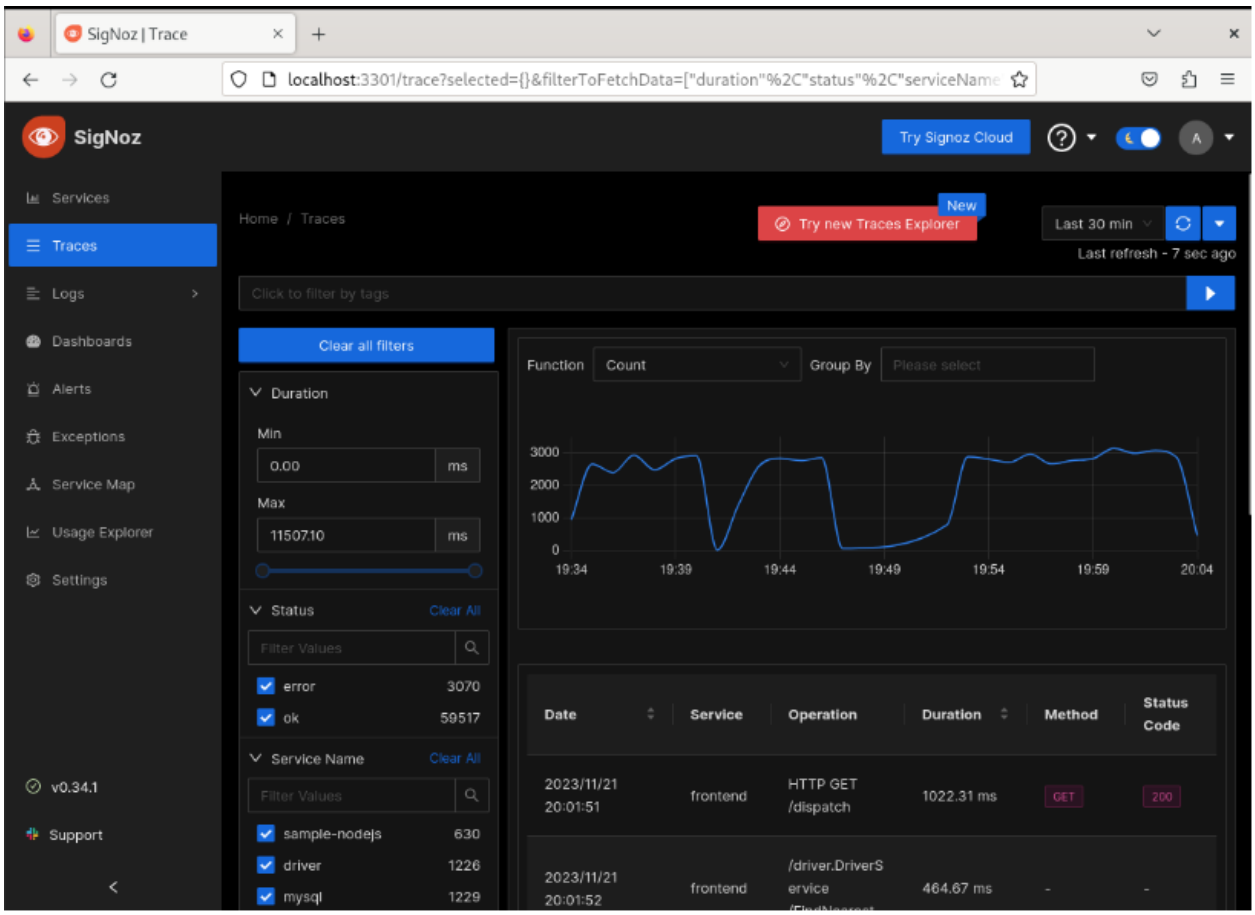
Установка приложения sample-nodejs-app согласно инструкции с сайта: https://github.com/SigNoz/sample-nodejs-app/

4.3 Запустим клиентское приложение sample-nodejs-app

```
root@KUZDEBIANPR3CLIENT:/loki# cd /home/kuzpr3client
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# mrdir /sample-nodejs
bash: mrdir: command not found
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# mkdir /sample-nodejs
root@KUZDEBIANPR3CLIENT:/home/kuzpr3client# cd /sample-nodejs
root@KUZDEBIANPR3CLIENT:/sample-nodejs# nano docker-compose.yaml
root@KUZDEBIANPR3CLIENT:/sample-nodejs# sudo docker compose up -d
[+] Running 10/10
 ✔ web 9 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿]      0B/0B      Pulled                                33.3s
   ✔ f56be85fc22e Pull complete                                                                  2.1s
   ✔ 931b0e865bc2 Pull complete                                                                 12.5s
   ✔ 60542df8b663 Pull complete                                                                  1.6s
   ✔ 062e26bc2446 Pull complete                                                                  2.3s
   ✔ aebace558f25 Pull complete                                                                  2.7s
   ✔ 4f4fb700ef54 Pull complete                                                                  2.9s
   ✔ 02b799cff739 Pull complete                                                                  3.5s
   ✔ d4f1f08cb98d Pull complete                                                                 10.8s
   ✔ 91fc9829d156 Pull complete                                                                  5.6s
[+] Running 2/2
 ✔ Network sample-nodejs_default  Created                                                        0.2s
 ✔ Container sample-nodejs-web-1  Started                                                        1.1s
root@KUZDEBIANPR3CLIENT:/sample-nodejs#
```

4.4 Проверим получение логов в Signoz




SigNoz | Trace
localhost:3301/trace?selected={}&filterToFetchData=["duration"%2C"status"%2C"serviceName
SigNoz
Try Signoz Cloud
Services
Traces
Logs
Dashboards
Alerts
Exceptions
Service Map
Usage Explorer
Settings
v0.34.1
Support
Home / Traces
New
Try new Traces Explorer
Last 30 min
Last refresh - 7 sec ago
Click to filter by tags
Clear all filters
Duration
Min
0.00
ms
Max
11507.10
ms
Status
Clear All
Filter Values
error 3070
ok 59517
Service Name
Clear All
Filter Values
sample-nodejs 630
driver 1226
mysql 1229
Function
Count
Group By
Please select
3000
2000
1000
0
19:34
19:39
19:44
19:49
19:54
19:59
20:04
Date
Service
Operation
Duration
Method
Status Code
2023/11/21 20:01:51
frontend
HTTP GET /dispatch
1022.31 ms
GET
200
2023/11/21 20:01:52
frontend
/driver.DriverService
464.67 ms
-
-