



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
Кафедра КБ-4 «Интеллектуальные системы информационной
безопасности»

Отчёт по практической работе №1
по дисциплине «Система для сбора событий и логов»

Выполнил:
Евдокимов А.М.
Группа: ББМО-02-23

Москва - 2024

Rsyslog. Сервер

1 На виртуальных машинах настроил сеть на Сетевой мост

2 На первой виртуальной машине скачем rsyslog



```
Debian 12 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Terminal - evdokimov@...
Terminal - evdokimov@10: ~
File  Edit  View  Terminal  Tabs  Help

evdokimov@10:~$ sudo apt install rsyslog
[sudo] password for evdokimov:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog is already the newest version (8.2302.0-1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
evdokimov@10:~$ systemctl status rsyslog.service
• rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: en>
   Active: active (running) since Wed 2024-09-11 18:26:12 MSK; 4min 4s ago
   TriggeredBy: • syslog.socket
   Docs: man:rsyslogd(8)
         man:rsyslog.conf(5)
         https://www.rsyslog.com/doc/
   Main PID: 513 (rsyslogd)
   Tasks: 10 (limit: 9462)
   Memory: 3.4M
   CPU: 116ms
   CGroup: /system.slice/rsyslog.service
           └─513 /usr/sbin/rsyslogd -n -iNONE

Warning: some journal files were not opened due to insufficient permissions.
lines 1-15/15 (END)
```

3 Запустим сервис. Проверим работоспособность

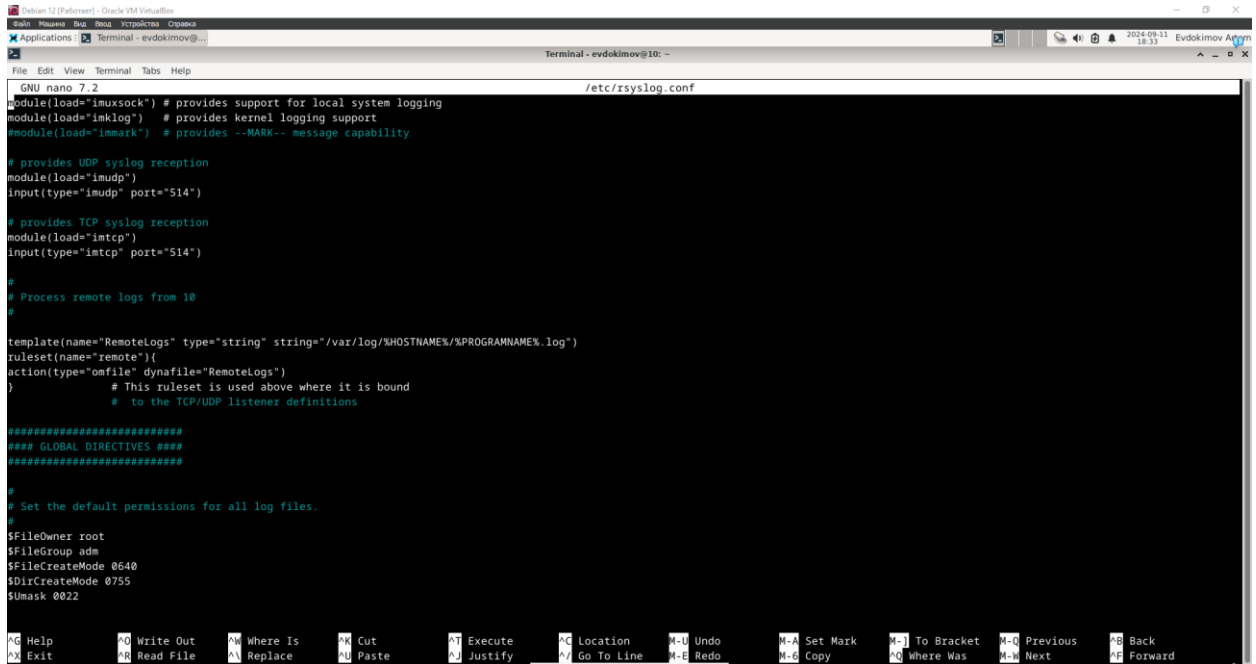


```
Debian 12 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Terminal - evdokimov@...
Terminal - evdokimov@10: ~
File Edit View Terminal Tabs Help

evdokimov@10:~$ sudo apt install rsyslog
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog is already the newest version (8.2302.0-1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
evdokimov@10:~$ sudo systemctl status rsyslog.service
• rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: en>
   Active: active (running) since Wed 2024-09-11 18:26:12 MSK; 4min 48s ago
   TriggeredBy: • syslog.socket
   Docs: man:rsyslogd(8)
         man:rsyslog.conf(5)
         https://www.rsyslog.com/doc/
   Main PID: 513 (rsyslogd)
   Tasks: 10 (limit: 9462)
   Memory: 3.4M
   CPU: 122ms
   CGroup: /system.slice/rsyslog.service
           └─513 /usr/sbin/rsyslogd -n -iNONE

Sep 11 18:26:10 10 systemd[1]: Starting rsyslog.service - System Logging Serv>
Sep 11 18:26:12 10 systemd[1]: Started rsyslog.service - System Logging Servi>
Sep 11 18:26:12 10 rsyslogd[513]: imuxsock: Acquired UNIX socket '/run/system>
Sep 11 18:26:12 10 rsyslogd[513]: [origin software="rsyslogd" swVersion="8.23>
Sep 11 18:26:19 10 systemd[1]: rsyslog.service: Sent signal SIGHUP to main pr>
Sep 11 18:26:19 10 rsyslogd[513]: [origin software="rsyslogd" swVersion="8.23>
lines 1-20/20 (END)
```

4 Настраиваем rsyslog для удаленного приема системного журнала



```
GNU nano 7.2 /etc/rsyslog.conf
#module(load="imuxsock") # provides support for local system logging
#module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

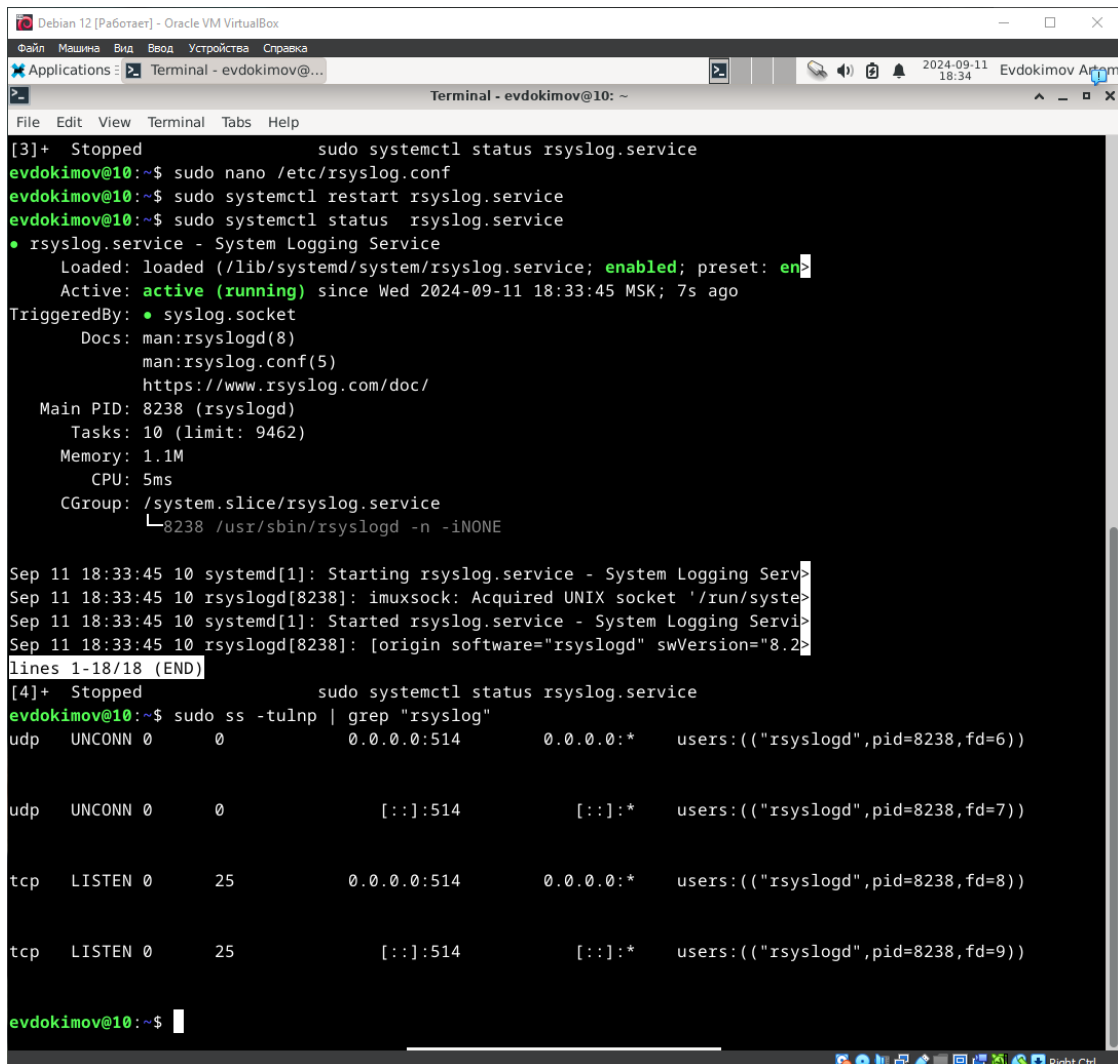
#
# Process remote logs from 10
#

template(name="RemoteLogs" type="string" string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
ruleset(name="remote"){
    action(type="omfile" dynafile="RemoteLogs")
}
# This ruleset is used above where it is bound
# to the TCP/UDP listener definitions

#####
#### GLOBAL DIRECTIVES ####
#####

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
```

5 Перезапускаем сервис



```
Debian 12 [Работаer] - Oracle VM VirtualBox
Applications: Terminal - evdokimov@...
Terminal - evdokimov@10: ~

[3]+ Stopped sudo systemctl status rsyslog.service
evdokimov@10:~$ sudo nano /etc/rsyslog.conf
evdokimov@10:~$ sudo systemctl restart rsyslog.service
evdokimov@10:~$ sudo systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: en>
   Active: active (running) since Wed 2024-09-11 18:33:45 MSK; 7s ago
   TriggeredBy: ● syslog.socket
     Docs: man:rsyslogd(8)
           man:rsyslog.conf(5)
           https://www.rsyslog.com/doc/
   Main PID: 8238 (rsyslogd)
     Tasks: 10 (limit: 9462)
    Memory: 1.1M
       CPU: 5ms
    CGroup: /system.slice/rsyslog.service
           └─8238 /usr/sbin/rsyslogd -n -iNONE

Sep 11 18:33:45 10 systemd[1]: Starting rsyslog.service - System Logging Serv>
Sep 11 18:33:45 10 rsyslogd[8238]: imuxsock: Acquired UNIX socket '/run/syste>
Sep 11 18:33:45 10 systemd[1]: Started rsyslog.service - System Logging Servi>
Sep 11 18:33:45 10 rsyslogd[8238]: [origin software="rsyslogd" swVersion="8.2>
lines 1-18/18 (END)
[4]+ Stopped sudo systemctl status rsyslog.service
evdokimov@10:~$ sudo ss -tulnp | grep "rsyslog"
udp UNCONN 0      0      0.0.0.0:514      0.0.0.0:*      users:(("rsyslogd",pid=8238,fd=6))

udp UNCONN 0      0      [::]:514      [::]:*      users:(("rsyslogd",pid=8238,fd=7))

tcp LISTEN 0      25      0.0.0.0:514      0.0.0.0:*      users:(("rsyslogd",pid=8238,fd=8))

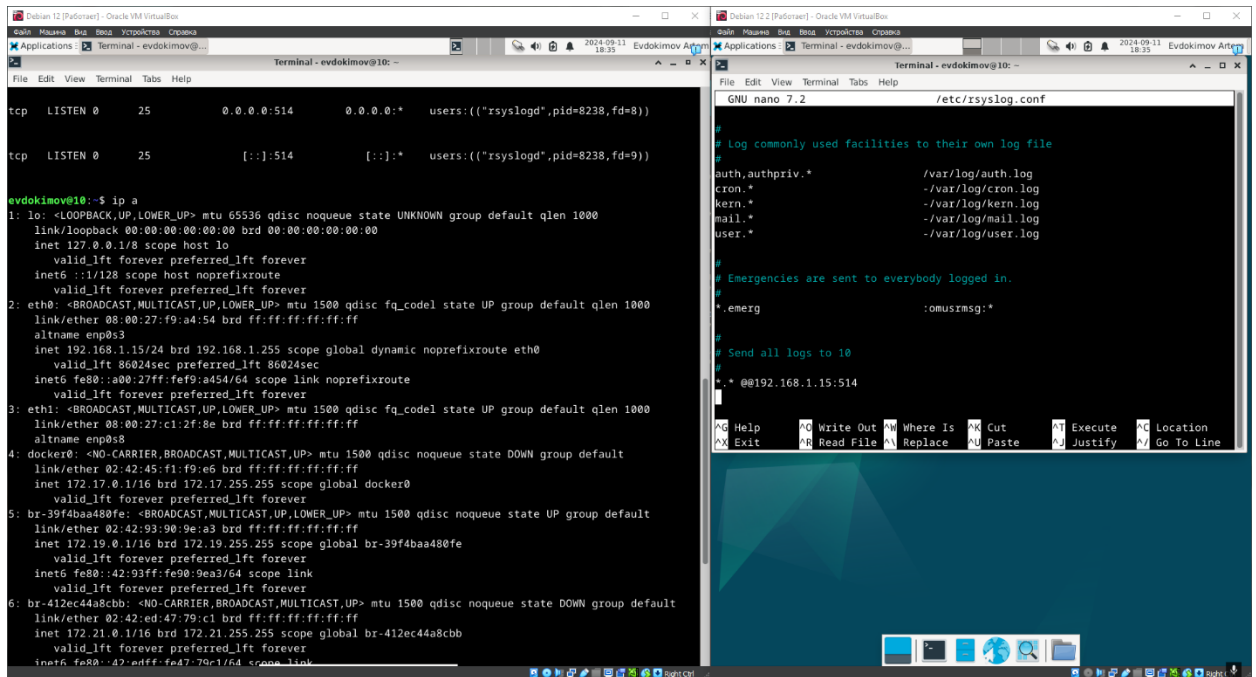
tcp LISTEN 0      25      [::]:514      [::]:*      users:(("rsyslogd",pid=8238,fd=9))

evdokimov@10:~$
```

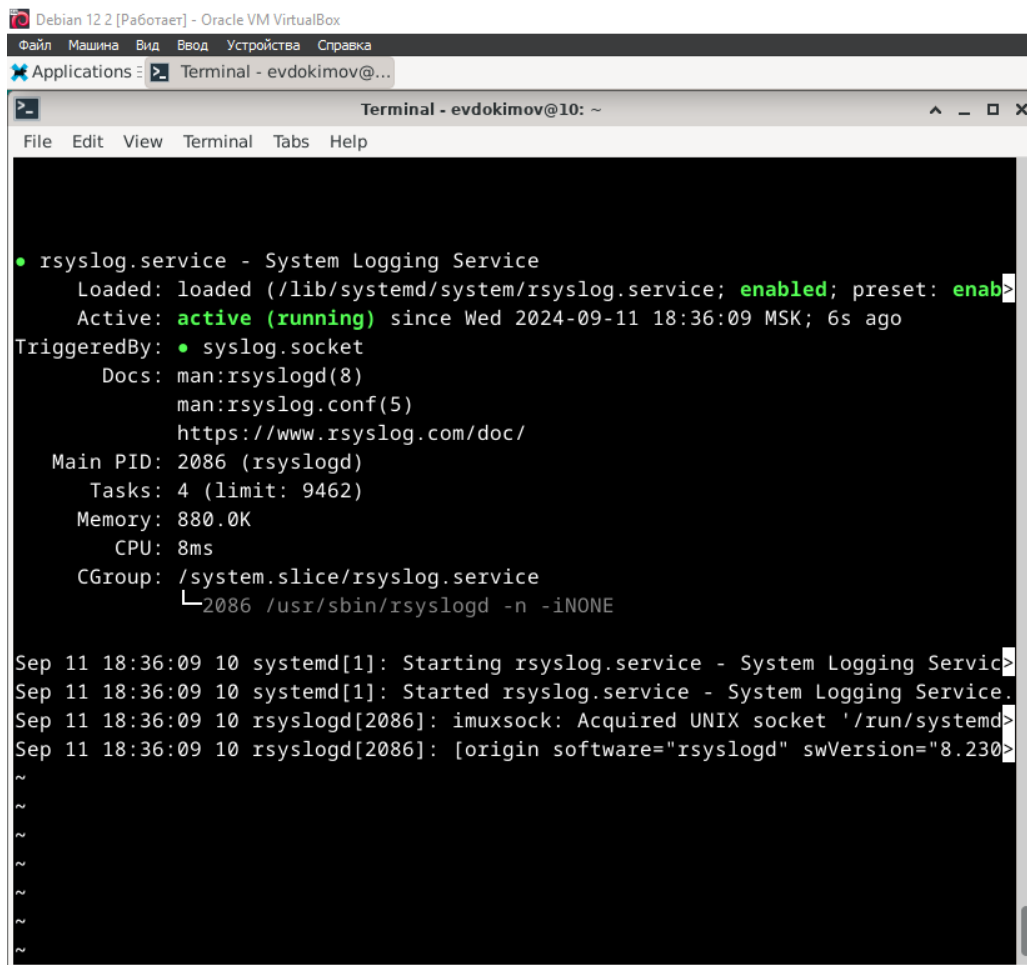
Rsyslog. Клиент

1 На второй виртуальной машине скачаем rsyslog

2 Отредактируем config, добавляем правило для пересылки логов



3 Перезапускаем сервис



LOKI

1 Разворачиваем на сервере Loki

```
Debian 12 [Parrot] - Oracle VM VirtualBox
Applications | Terminal - evdokimov@... | 2024-09-11 18:37 | Evdokimov A...

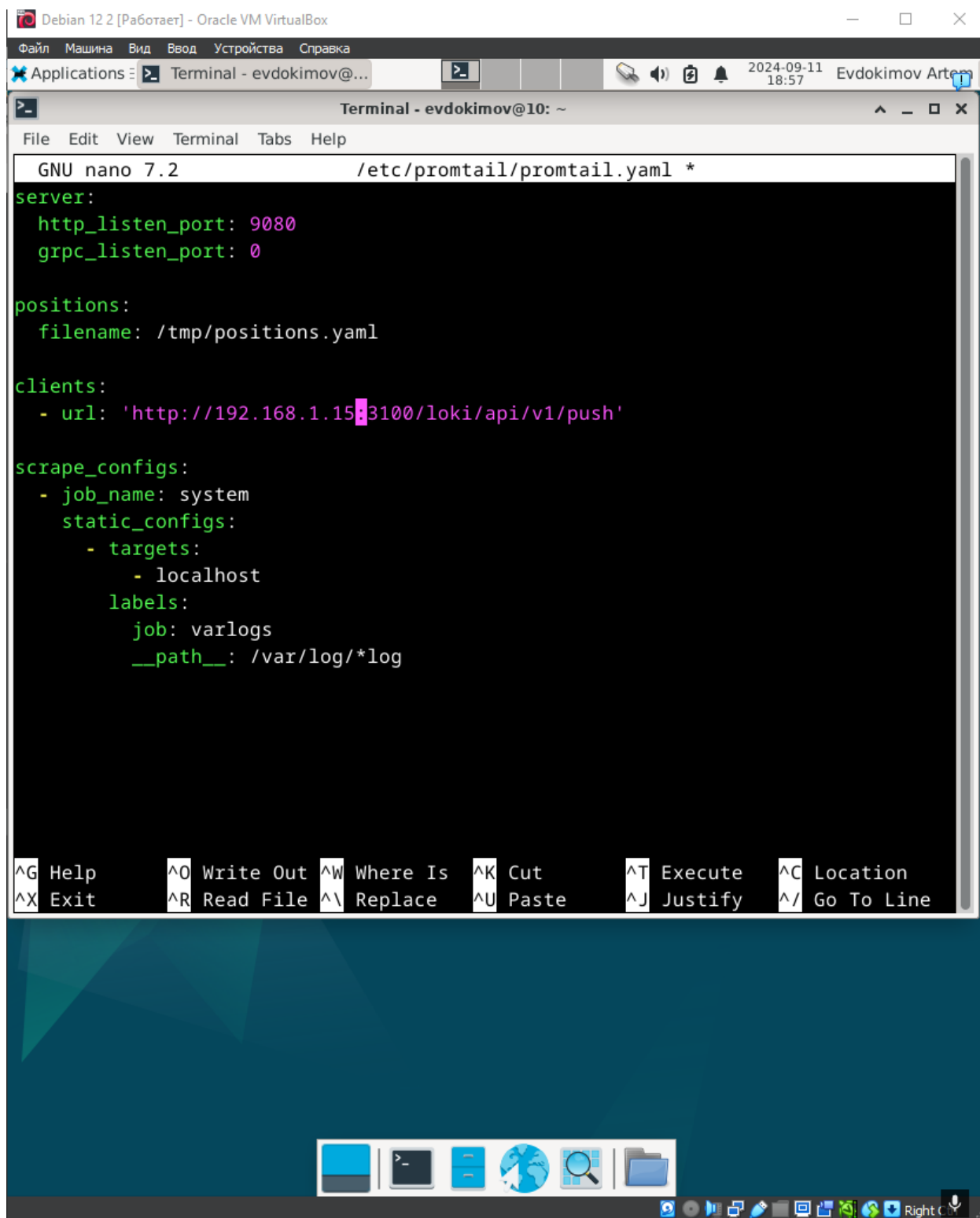
File Edit View Terminal Tabs Help

[5] Stopped sudo docker compose up
evdokimov@10:~/Loki$ sudo docker compose ps
NAME                IMAGE                COMMAND                SERVICE    CREATED      STATUS      PORTS
loki-grafana-1      grafana/grafana:latest  "sh -euc 'mkdir -p /-"  grafana    3 minutes ago  Up 3 minutes  0.0.0.0:3000->3000/tcp, :::3000->3000/tcp
loki-loki-1         grafana/loki:2.9.0    "/usr/bin/loki -conf-"  loki       3 minutes ago  Up 3 minutes  0.0.0.0:3100->3100/tcp, :::3100->3100/tcp
loki-promtail-1     grafana/promtail:2.9.0  "/usr/bin/promtail -"  promtail   3 minutes ago  Up 3 minutes
evdokimov@10:~/Loki$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f9:a4:54 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.1.15/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 84737sec preferred_lft 84737sec
    inet6 fe80::a0b:27ff:fe9:a454/64 scope link noprefixroute
```

2 На клиенте устанавливаем Promtail

```
evdokimov@10:~/Loki$ curl -O -L "https://github.com/grafana/loki/releases/download/v2.4.1/promtail-linux-amd64.zip"
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 20.3M  100 20.3M    0     0  19.7M      0  0:00:01  0:00:01 --:--:-- 32.9M
evdokimov@10:~/Loki$ unzip "promtail-linux-amd64.zip"
Archive:  promtail-linux-amd64.zip
  inflating: promtail-linux-amd64
evdokimov@10:~/Loki$
```

3 Создаем файл конфигурации



The screenshot shows a terminal window titled "Terminal - evdokimov@10: ~" running GNU nano 7.2. The user is editing the file `/etc/promtail/promtail.yaml`. The configuration is as follows:

```
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: 'http://192.168.1.15:3100/loki/api/v1/push'

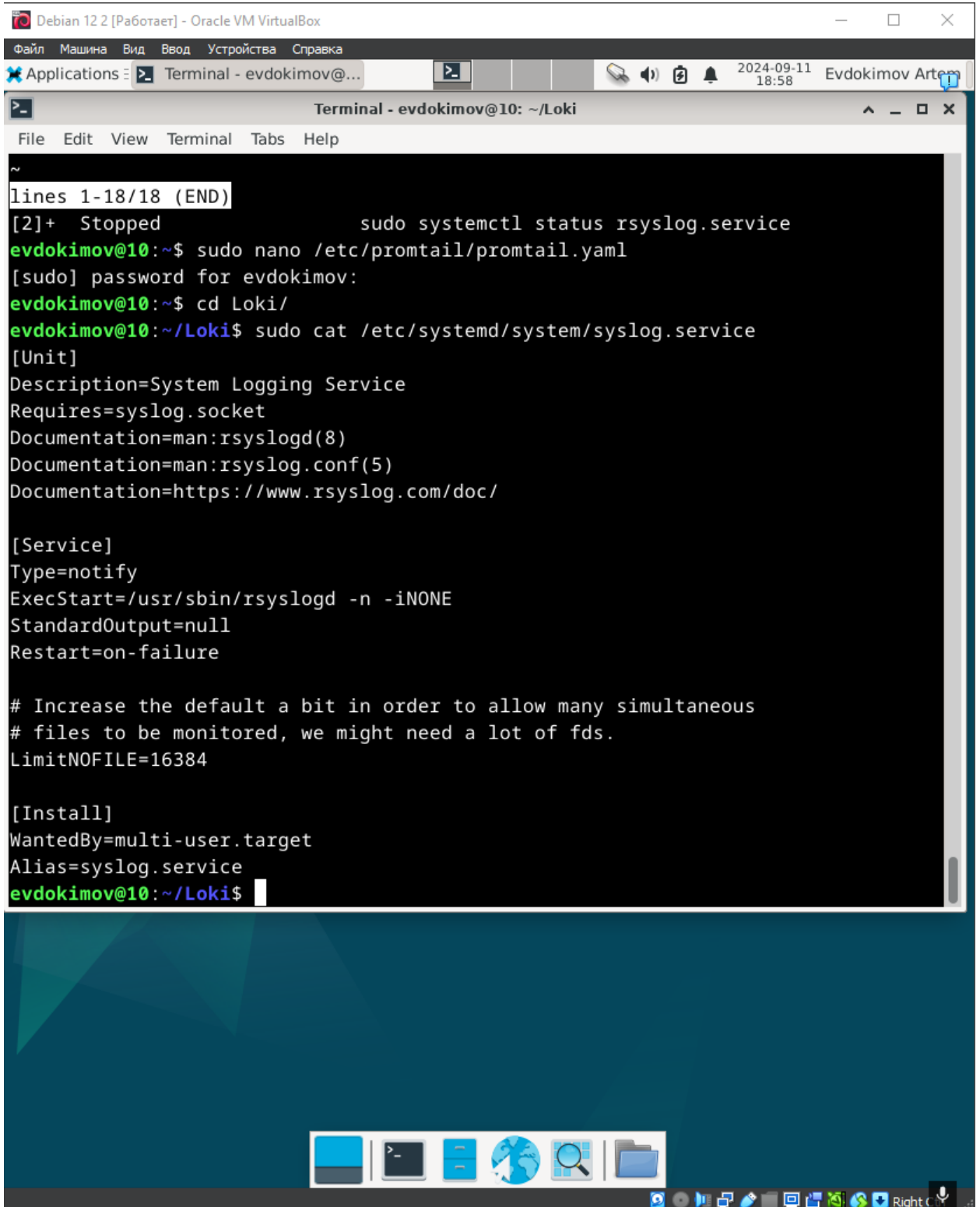
scrape_configs:
  - job_name: system
    static_configs:
      - targets:
          - localhost
        labels:
          job: varlogs
          __path__: /var/log/*log
```

At the bottom of the terminal window, there is a table of nano editor shortcuts:

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

The desktop background is a teal geometric pattern. The taskbar at the bottom contains icons for a terminal, file manager, and other applications. The system tray on the right shows the date and time as 2024-09-11 18:57 and the user name Evdokimov Artem.

4 Создаем Unit



The screenshot shows a terminal window titled "Terminal - evdokimov@10: ~/Loki" within a Debian 12 VM. The user has just finished editing a file in nano. The terminal output shows the status of the rsyslog service, followed by the user running 'sudo nano /etc/promtail/promtail.yaml' and 'cd Loki/'. Then, the user runs 'sudo cat /etc/systemd/system/syslog.service', which displays the contents of the syslog.service unit file. The unit file defines a service that uses rsyslogd, has a notify type, and includes a LimitNOFILE setting. The user is currently at the prompt 'evdokimov@10:~/Loki\$'.

```
~
lines 1-18/18 (END)
[2]+  Stopped                  sudo systemctl status rsyslog.service
evdokimov@10:~$ sudo nano /etc/promtail/promtail.yaml
[sudo] password for evdokimov:
evdokimov@10:~$ cd Loki/
evdokimov@10:~/Loki$ sudo cat /etc/systemd/system/syslog.service
[Unit]
Description=System Logging Service
Requires=syslog.socket
Documentation=man:rsyslogd(8)
Documentation=man:rsyslog.conf(5)
Documentation=https://www.rsyslog.com/doc/

[Service]
Type=notify
ExecStart=/usr/sbin/rsyslogd -n -iNONE
StandardOutput=null
Restart=on-failure

# Increase the default a bit in order to allow many simultaneous
# files to be monitored, we might need a lot of fds.
LimitNOFILE=16384

[Install]
WantedBy=multi-user.target
Alias=syslog.service
evdokimov@10:~/Loki$
```


Debian 12 2 [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Applications Terminal - evdokimov@... 2024-09-11 18:59 Evdokimov Artem

Terminal - evdokimov@10: ~/Loki

File Edit View Terminal Tabs Help

GNU nano 7.2 /etc/systemd/system/promtail.service

```
[Unit]
Description=Promtail service
After=network.target

[Service]
Type=simple
User=promtail
ExecStart=/usr/local/bin/promtail-linux-amd64 -config.file /usr/local/bin/confi>

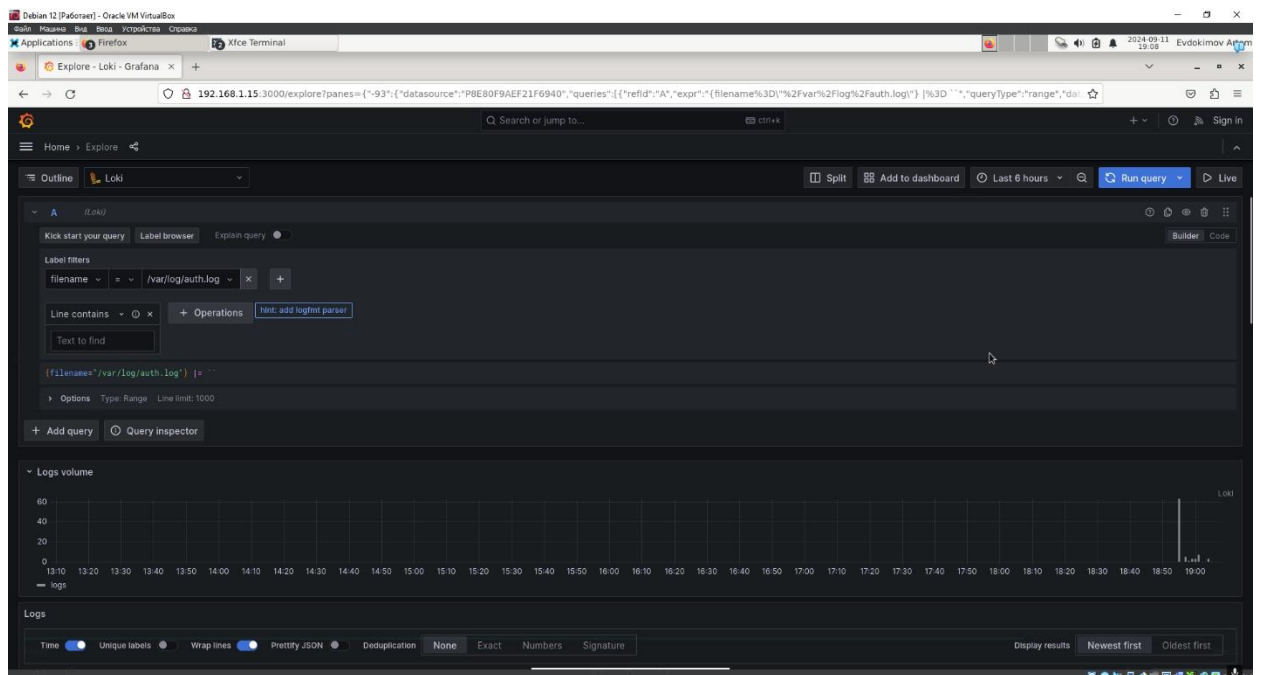
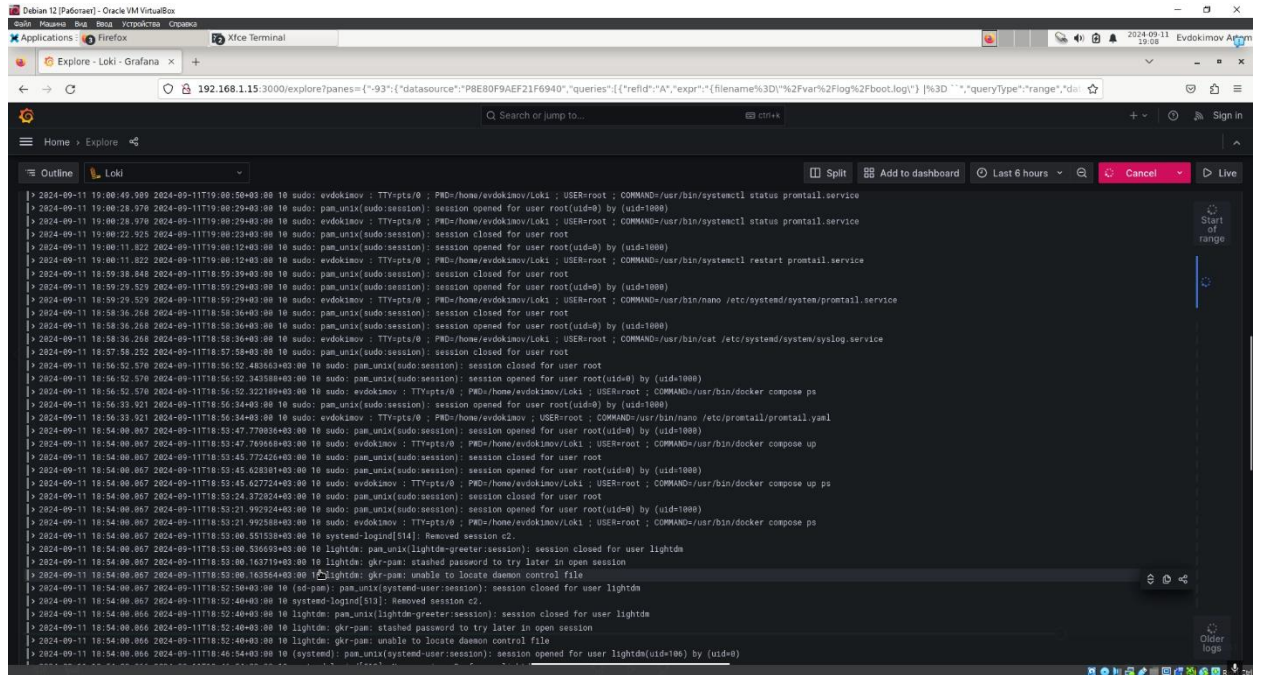
[Install]
WantedBy=multi-user.target
```

[Read 11 lines]

^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

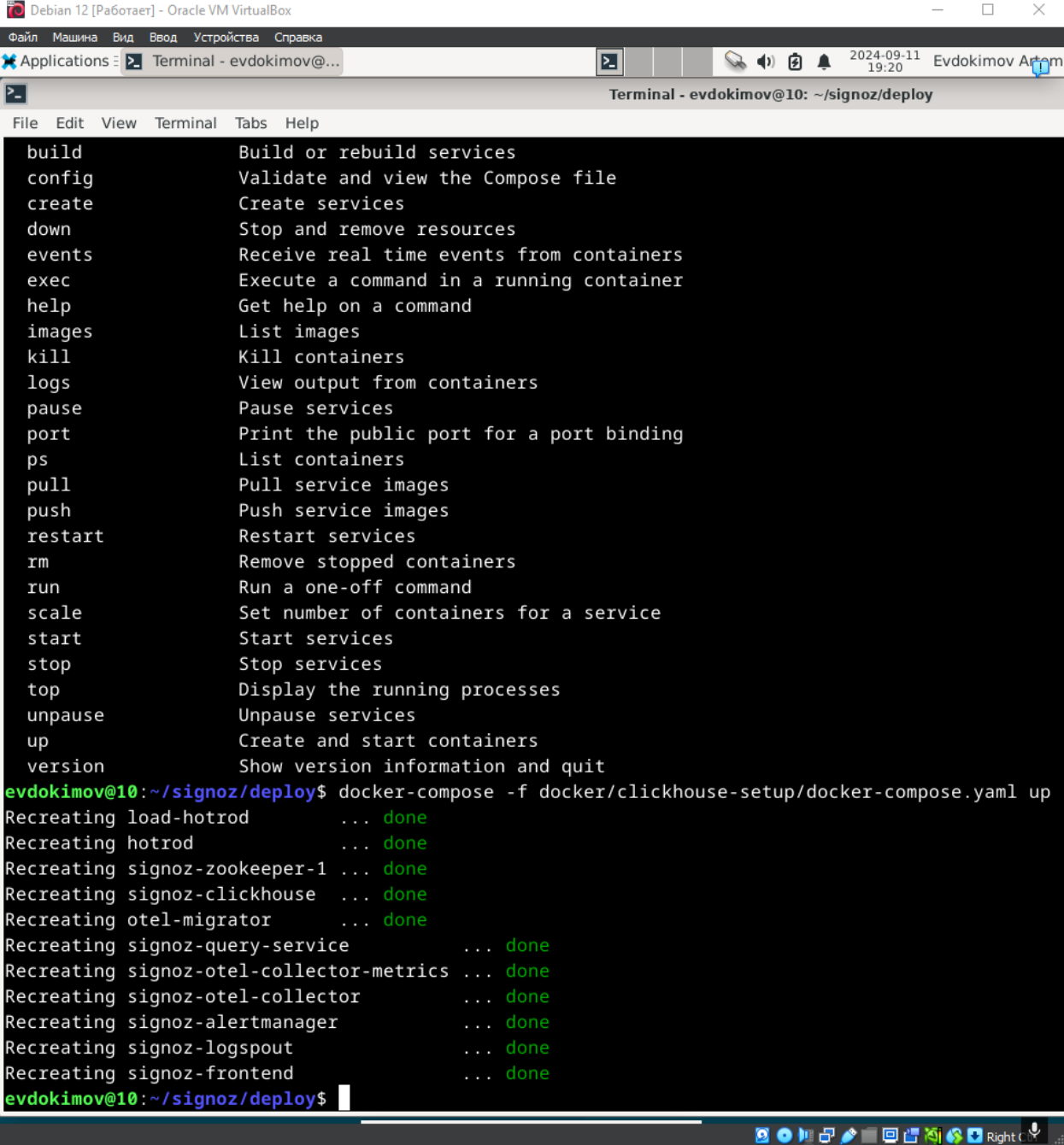
[illegible]

6 Посмотрим логи на сервере



SIGNOZ

1 Запускаем контейнер на сервере

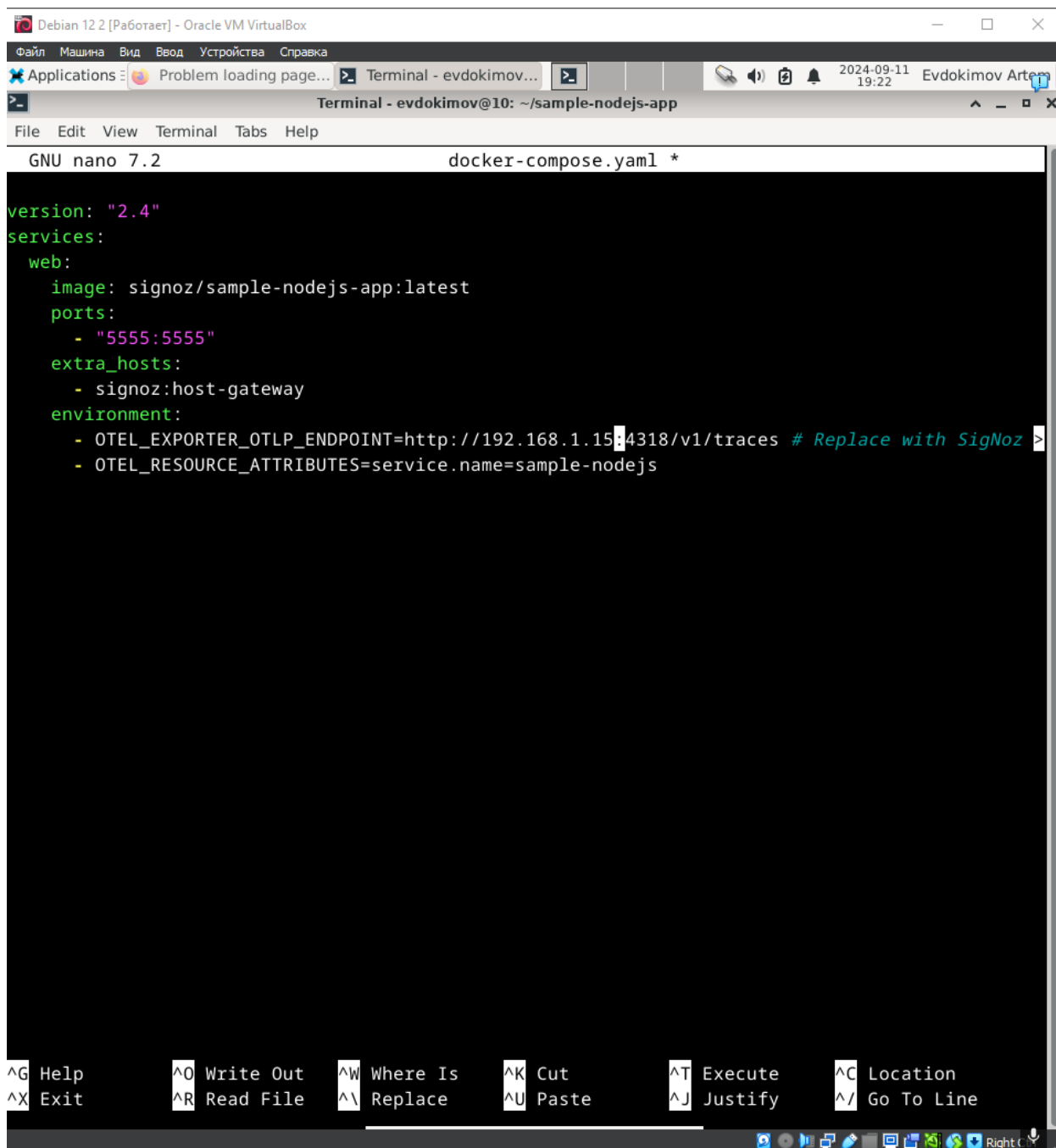


The screenshot shows a terminal window titled "Terminal - evdokimov@10: ~/signoz/deploy" running inside a Debian 12 virtual machine. The terminal displays a list of Docker Compose commands and their descriptions, followed by the execution of the `docker-compose up` command. The output shows the recreation of several services, all of which completed successfully.

```
build          Build or rebuild services
config         Validate and view the Compose file
create         Create services
down           Stop and remove resources
events         Receive real time events from containers
exec           Execute a command in a running container
help           Get help on a command
images         List images
kill           Kill containers
logs           View output from containers
pause          Pause services
port           Print the public port for a port binding
ps             List containers
pull           Pull service images
push           Push service images
restart        Restart services
rm             Remove stopped containers
run            Run a one-off command
scale          Set number of containers for a service
start          Start services
stop           Stop services
top            Display the running processes
unpause        Unpause services
up             Create and start containers
version        Show version information and quit

evdokimov@10:~/signoz/deploy$ docker-compose -f docker/clickhouse-setup/docker-compose.yaml up
Recreating load-hotrod      ... done
Recreating hotrod           ... done
Recreating signoz-zookeeper-1 ... done
Recreating signoz-clickhouse ... done
Recreating otel-migrator    ... done
Recreating signoz-query-service ... done
Recreating signoz-otel-collector-metrics ... done
Recreating signoz-otel-collector ... done
Recreating signoz-alertmanager ... done
Recreating signoz-logspout  ... done
Recreating signoz-frontend  ... done
evdokimov@10:~/signoz/deploy$
```

2 Так же для клиента редактируем docker-compose файл



The screenshot shows a terminal window titled "Debian 12 2 [Работаает] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing a file named "docker-compose.yaml". The content of the file is as follows:


```
version: "2.4"
services:
  web:
    image: signoz/sample-nodejs-app:latest
    ports:
      - "5555:5555"
    extra_hosts:
      - signoz:host-gateway
    environment:
      - OTEL_EXPORTER_OTLP_ENDPOINT=http://192.168.1.15:4318/v1/traces # Replace with SigNoz
      - OTEL_RESOURCE_ATTRIBUTES=service.name=sample-nodejs
```

The terminal window also shows the nano editor's help menu at the bottom, which includes shortcuts for various actions like Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, and Go To Line.




3 Запускаем контейнер

```
evdokimov@10:~/sample-nodejs-app$ sudo nano docker-compose.yaml
evdokimov@10:~/sample-nodejs-app$ sudo docker compose up -d
[+] Running 10/10
✔ web 9 layers [██████████] 0B/0B Pulled 29.2s
✔ f56be85fc22e Pull complete 1.0s
✔ 931b0e865bc2 Pull complete 3.7s
✔ 60542df8b663 Pull complete 0.9s
✔ 062e26bc2446 Pull complete 1.7s
✔ aebace558f25 Pull complete 1.8s
✔ 4f4fb700ef54 Pull complete 2.4s
✔ 02b799cff739 Pull complete 2.7s
✔ d4f1f08cb98d Pull complete 7.3s
✔ 91fc9829d156 Pull complete 3.4s
[+] Running 2/2
✔ Network sample-nodejs-app_default Created 2.3s
✔ Container sample-nodejs-app-web-1 Started 9.4s
evdokimov@10:~/sample-nodejs-app$
```

4 Наблюдаем логи в SigNoz

 **SigNoz**

[Try SigNoz Cloud](#)

Services

Traces

Logs

Dashboards

Alerts

Exceptions

Service Map



Usage Explorer

Settings

v0.33.1

Support


Home / Services

Last 30 min  

Last refresh - 10 sec ago

Search and Filter based on resource attributes.

Application	P99 latency (in ms)	Error Rate (% of total)	Operations Per Second
sample-nodejs	15.30	0.00	0.00
route	83.68	0.00	7.97
customer	9888.56	0.00	0.81
redis	37.96	18.52	10.89
frontend	10678.02	1.19	0.80
mysql	9886.17	0.00	0.81
driver	1632.81	0.00	0.81

 1 