



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»

Дисциплина «Технологии обеспечения информационной безопасности»

Отчет

о проделанной практической работе №5

Выполнил студент 1 курса
Группы: ББМО-01-24
Фрез Е.С.

Москва 2024

Задачи:

1. Создать 2 виртуальные машины на базе ОС Debian 12

<https://www.virtualbox.org/wiki/Downloads>

<https://cdimage.debian.org/debiancd/current/amd64/iso-cd/debian-12.1.0-amd64-netinst.iso>

2. Обеспечить между ними сетевой обмен

<https://www.virtualbox.org/manual/ch06.html>

3. Включить на 1й из ВМ передачу логов по протоколу rsyslog на 2ю ВМ

<https://www.tecmint.com/install-rsyslog-centralized-logging-in-centos-ubuntu/>

4. Установить и настроить получение логов на сервер с использованием Loki

<https://github.com/grafana/loki> https://docs.google.com/document/d/11tjK_lvp1-SVsFZjgOTr1vV3-q6vBAsZYIQ5ZeYBkyM/view (источник можно выбрать самостоятельно)

5. Установить и настроить получение логов на сервер с использованием

Signoz <https://signoz.io/> <https://signoz.io/blog/loki-vs-elasticsearch/> (источник можно выбрать самостоятельно)

Рис. 1 – Виртуальные машины на базе ОС Debian 12.

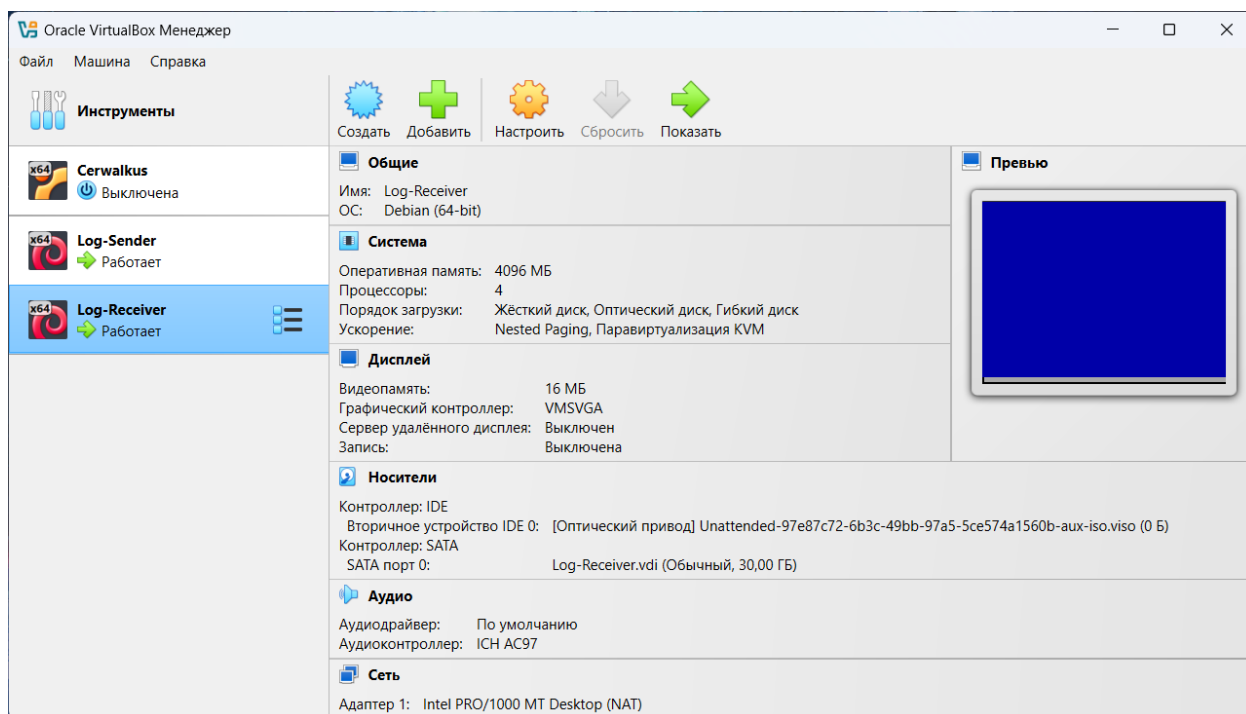


Рис. 2 – Настройки сетевого адаптера для Log-Sender

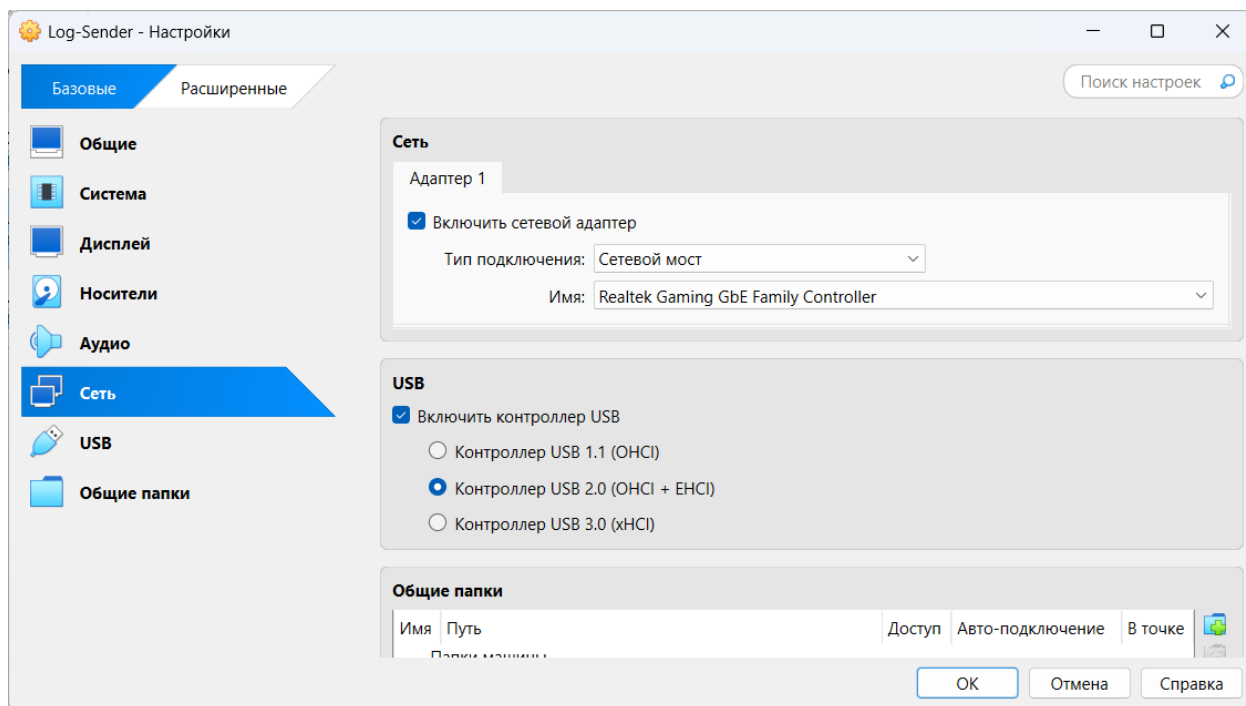


Рис. 3 – Настройки сетевого адаптера для Log-Receiver

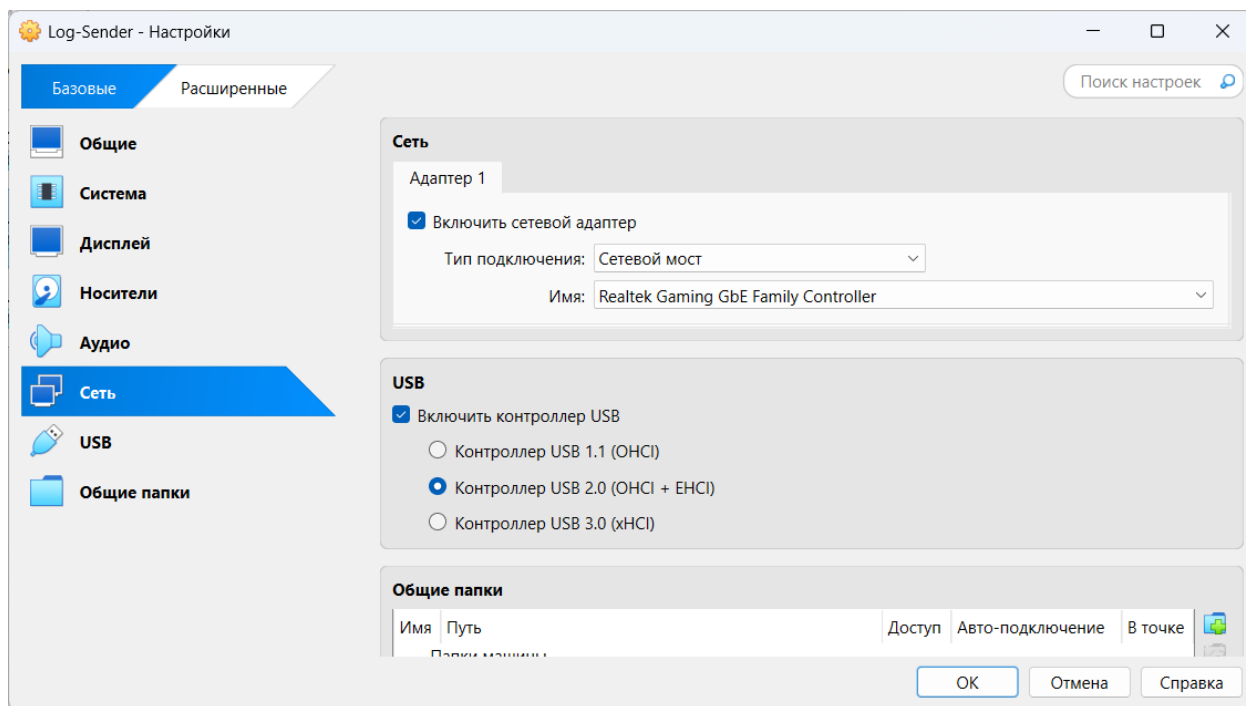


Рис. 4 – IP-адреса каждой машины

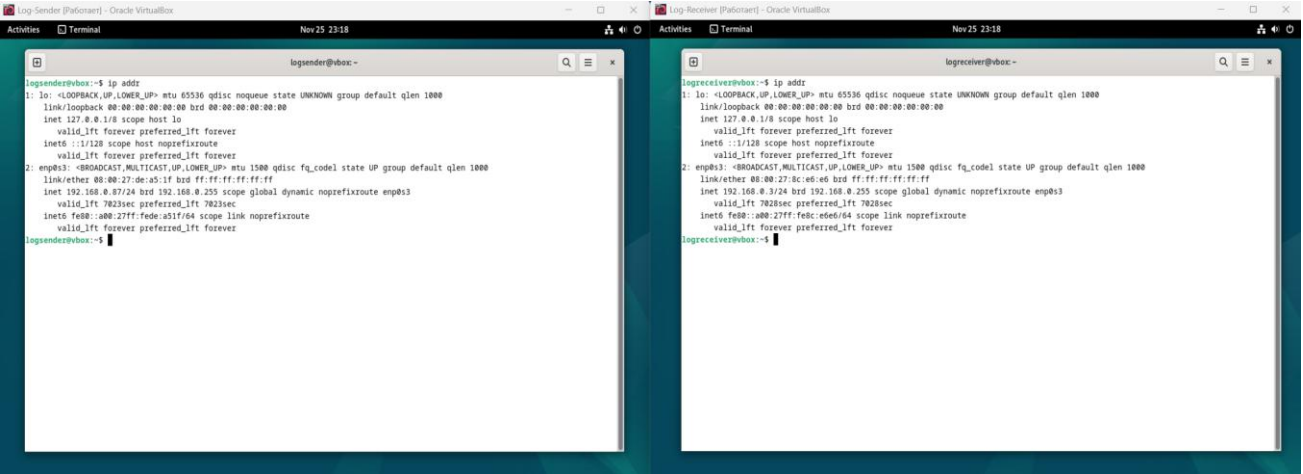


Рис. 5 – Пинг Log-Receiver и Log-Sender

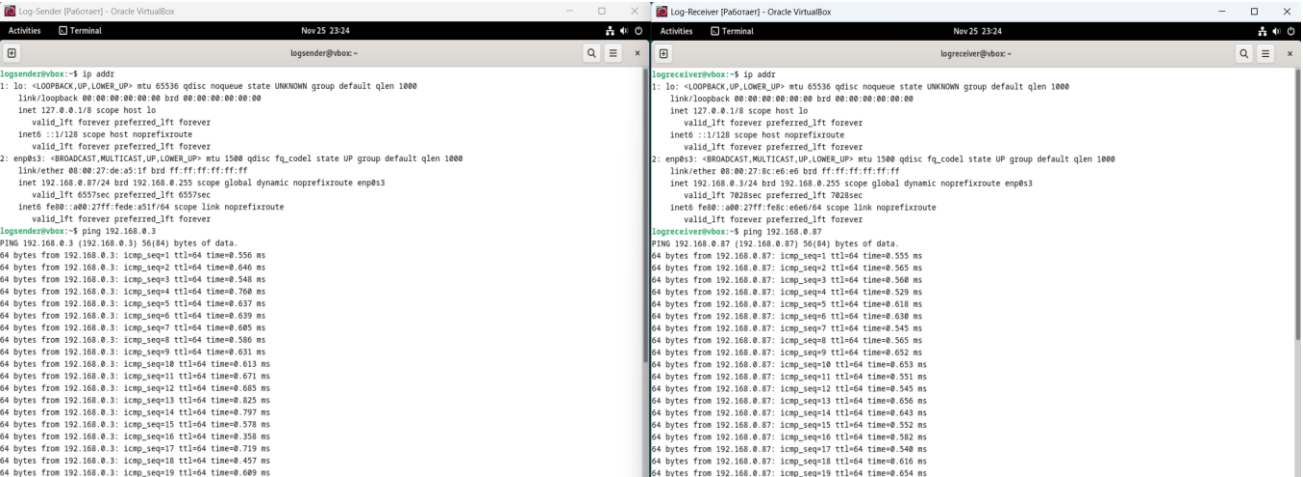


Рис. 6 – Установка rsyslog

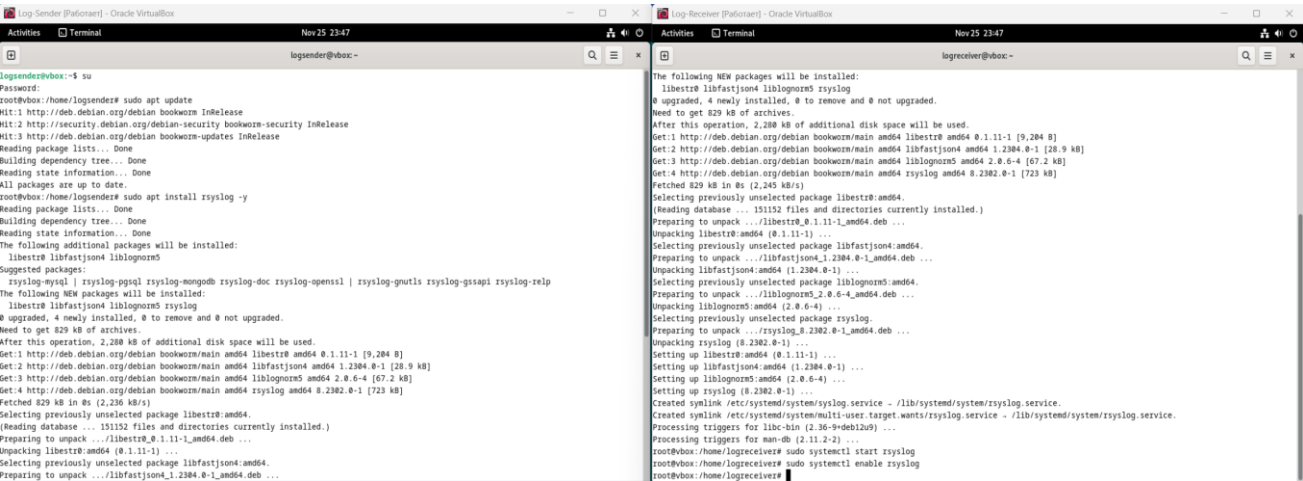


Рис. 7 – Настройка отправки логов по UDP

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

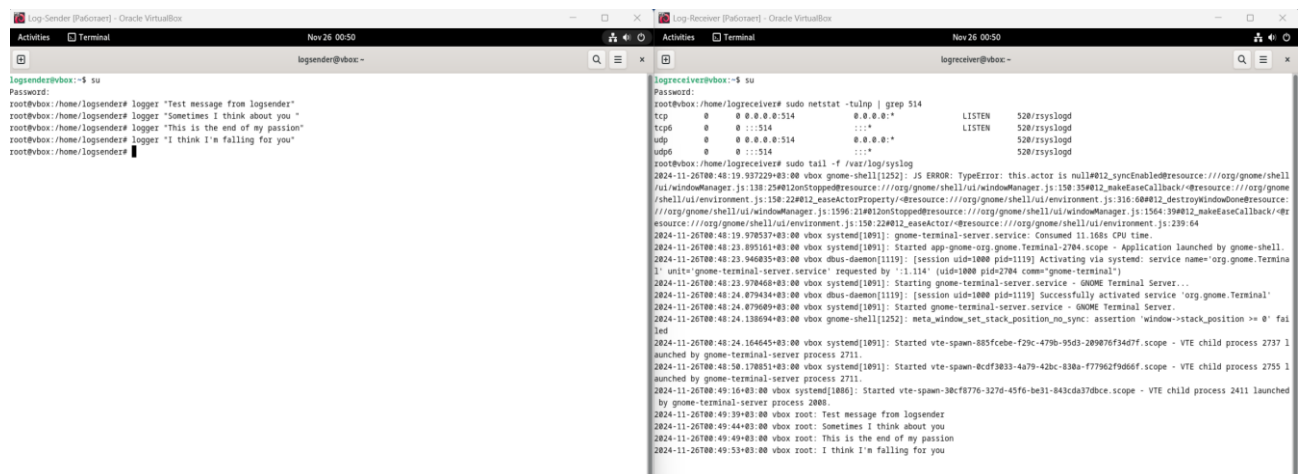
*. * @192.168.0.3:514      # Для отправки через UDP
```

Рис. 8 – Настройка приема логов по UDP

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

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

Рис. 9 – Тестирование передачи логов



```
Log Sender (PaloSant) - Oracle VM VirtualBox
Nov 26 00:50
logsender@vbox:~$ su
Password:
root@vbox:/home/logsender# logger "Test message from logsender"
root@vbox:/home/logsender# logger "Sometimes I think about you"
root@vbox:/home/logsender# logger "This is the end of my passion"
root@vbox:/home/logsender# logger "I think I'm falling for you"
root@vbox:/home/logsender#
```

```
Log Receiver (PaloSant) - Oracle VM VirtualBox
Nov 26 00:50
logreceiver@vbox:~$ su
Password:
root@vbox:/home/logreceiver# sudo netstat -tulnp | grep 514
tcp        0      0 0.0.0.0:514          0.0.0.0:*           LISTEN
tcp6       0      0 :::514              :::*                 LISTEN
udp        0      0 0.0.0.0:514          0.0.0.0:*           LISTEN
udp6       0      0 :::514              :::*                 LISTEN
root@vbox:/home/logreceiver# sudo tail -f /var/log/syslog
2024-11-26T00:48:19.937220+03:00 vbox gnome-shell[1252]: JS ERROR: TypeError: this actor is null@012_syncDisable@resource:///org/gnome/shell/ui/windowManager.js:138:25@012_makeEaseCallback@resource:///org/gnome/shell/ui/environment.js:158:22@012_easeActorProperty@resource:///org/gnome/shell/ui/environment.js:316:6@012_destroyWindowDone@resource:///org/gnome/shell/ui/windowManager.js:1596:21@012_onStopped@resource:///org/gnome/shell/ui/windowManager.js:1564:39@012_makeEaseCallback@resource:///org/gnome/shell/ui/environment.js:158:22@012_easeActorProperty@resource:///org/gnome/shell/ui/environment.js:316:6
2024-11-26T00:48:19.978537+03:00 vbox systemd[109]: gnome-terminal-server.service: Consumed 11.16s CPU time.
2024-11-26T00:48:23.895161+03:00 vbox systemd[109]: Started app-gnome-org.gnome.Terminal-2704.scope - Application launched by gnome-shell.
2024-11-26T00:48:23.946835+03:00 vbox dbus-daemon[1119]: [session uid=1000 pid=1119] Activating via systemd: service name='org.gnome.Terminal' unit='org.gnome-terminal-server.service' requested by ':1.114' (uid=1000 pid=2704 comm='gnome-terminal')
2024-11-26T00:48:24.079434+03:00 vbox systemd[109]: Starting gnome-terminal-server.service - GNOME Terminal Server...
2024-11-26T00:48:24.079609+03:00 vbox dbus-daemon[1119]: [session uid=1000 pid=1119] Successfully activated service 'org.gnome.Terminal'
2024-11-26T00:48:24.079609+03:00 vbox systemd[109]: Started gnome-terminal-server.service - GNOME Terminal Server.
2024-11-26T00:48:24.136094+03:00 vbox gnome-shell[1252]: meta_window_set_stack_position_no_sync: assertion 'window->stack_position >= 0' failed
2024-11-26T00:48:24.164645+03:00 vbox systemd[109]: Started vte-spawn-885fceb2-f29c-479b-95d3-289876f34d7f.scope - VTE child process 2737 launched by gnome-terminal-server process 2711.
2024-11-26T00:48:50.178515+03:00 vbox systemd[109]: Started vte-spawn-8cdf3033-4a79-42bc-83ba-f77962f9d60f.scope - VTE child process 2755 launched by gnome-terminal-server process 2711.
2024-11-26T00:49:16+03:00 vbox systemd[1086]: Started vte-spawn-38cf8776-327d-45f6-be31-843da37dbce.scope - VTE child process 2411 launched by gnome-terminal-server process 2080.
2024-11-26T00:49:39+03:00 vbox root: Test message from logsender
2024-11-26T00:49:44+03:00 vbox root: Sometimes I think about you
2024-11-26T00:49:49+03:00 vbox root: This is the end of my passion
2024-11-26T00:49:53+03:00 vbox root: I think I'm falling for you
```

Рис. 10 – Установка Loki

```
Log-Receiver [Пабогае] - Oracle VirtualBox
Activities Terminal Nov 26 01:14
logreceiver@vbox: ~
--2024-11-26 01:10:44-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/129717717/95f60514-9b6d-4c66-9cc5-fcfc
a9efc5207X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20241125%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=2024
1125T221044Z&X-Amz-Expires=300&X-Amz-Signature=16ae354197fe540e4f7e3e1221733c1c6c5f46d03d92ab87eb7aebb2faf7c0f8&X-Amz-SignedHeaders=host&res
ponse-content-disposition=attachment%3B%20filename%3Dloki-linux-amd64.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)[185.199.110.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20717061 (20M) [application/octet-stream]
Saving to: 'loki-linux-amd64.zip'

loki-linux-amd64.zip      100%[=====] 19.76M  34.1MB/s   in 0.6s

2024-11-26 01:10:46 (34.1 MB/s) - 'loki-linux-amd64.zip' saved [20717061/20717061]

root@vbox:/home/logreceiver# sudo apt install unzip -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unzip is already the newest version (6.0-28).
unzip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@vbox:/home/logreceiver# unzip loki-linux-amd64.zip
Archive:  loki-linux-amd64.zip
  inflating: loki-linux-amd64
root@vbox:/home/logreceiver# sudo mv loki-linux-amd64 /usr/local/bin/loki
root@vbox:/home/logreceiver# loki --version
loki, version 2.9.1 (branch: HEAD, revision: d9d5ed4a1)
  build user:   root@21ab03f17324
  build date:   2023-09-14T16:24:53Z
  go version:   go1.20.6
  platform:    linux/amd64
  tags:        netgo
root@vbox:/home/logreceiver# sudo nano /etc/loki-config.yml
root@vbox:/home/logreceiver#
```

Рис. 11 – Базовая конфигурация Loki

```
Log-Receiver [Пабогае] - Oracle VirtualBox
Activities Terminal Nov 26 01:12
logreceiver@vbox: ~
GNU nano 7.2 /etc/loki-config.yml *
server:
  http_listen_port: 3100

ingester:
  lifecycler:
    ring:
      kvstore:
        store: inmemory
      replication_factor: 1

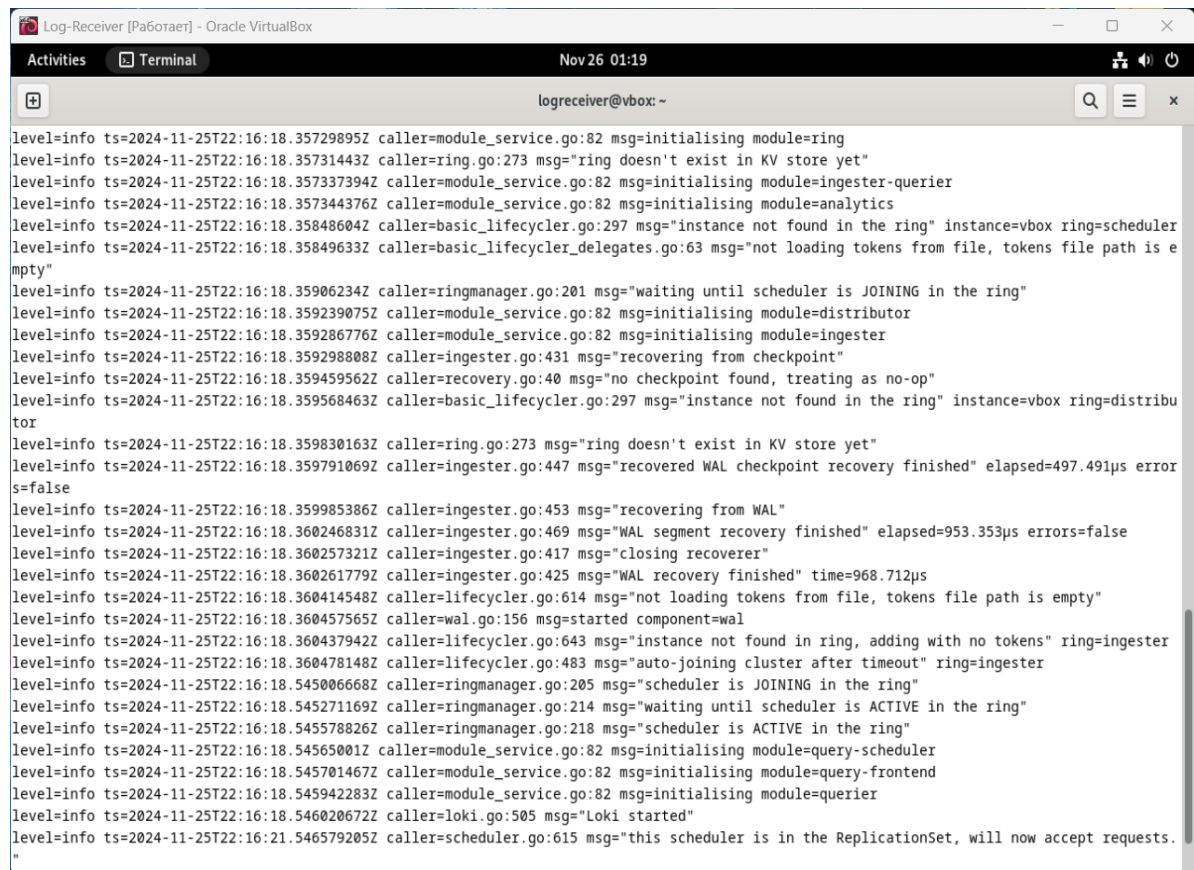
schema_config:
  configs:
    - from: 2020-10-24
      store: boltdb
      object_store: filesystem
      schema: v11
      index:
        prefix: index_
        period: 168h

storage_config:
  boltdb:
    directory: /tmp/loki/index
  filesystem:
    directory: /tmp/loki/chunks

limits_config:
  enforce_metric_name: false
  reject_old_samples: true
  reject_old_samples_max_age: 168h

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   ^U Undo       ^M-A Set Mark  ^M-J To Bracket
^X Exit      ^R Read File  ^A Replace    ^U Paste      ^J Justify    ^_ Go To Line  ^M-E Redo     ^M-G Copy     ^M-Q Where Was
```

Рис. 12 – Loki запущен и работает



The screenshot shows a terminal window titled "Log-Receiver [Пагоагет] - Oracle VirtualBox" with a timestamp of "Nov 26 01:19". The terminal output displays a series of log messages from the Log-Receiver component, including initialization steps, ring management, and recovery processes. The logs are formatted as key-value pairs, such as "level=info ts=2024-11-25T22:16:18.35729895Z caller=module_service.go:82 msg=initialising module=ring".

```
level=info ts=2024-11-25T22:16:18.35729895Z caller=module_service.go:82 msg=initialising module=ring
level=info ts=2024-11-25T22:16:18.35731443Z caller=ring.go:273 msg="ring doesn't exist in KV store yet"
level=info ts=2024-11-25T22:16:18.357337394Z caller=module_service.go:82 msg=initialising module=ingester-querier
level=info ts=2024-11-25T22:16:18.357344376Z caller=module_service.go:82 msg=initialising module=analytics
level=info ts=2024-11-25T22:16:18.35848604Z caller=basic_lifecycle.go:297 msg="instance not found in the ring" instance=vbox ring=scheduler
level=info ts=2024-11-25T22:16:18.35849633Z caller=basic_lifecycle_delegates.go:63 msg="not loading tokens from file, tokens file path is empty"
level=info ts=2024-11-25T22:16:18.35906234Z caller=ringmanager.go:201 msg="waiting until scheduler is JOINING in the ring"
level=info ts=2024-11-25T22:16:18.359239075Z caller=module_service.go:82 msg=initialising module=distributor
level=info ts=2024-11-25T22:16:18.359286776Z caller=module_service.go:82 msg=initialising module=ingester
level=info ts=2024-11-25T22:16:18.359298808Z caller=ingester.go:431 msg="recovering from checkpoint"
level=info ts=2024-11-25T22:16:18.359459562Z caller=recovery.go:40 msg="no checkpoint found, treating as no-op"
level=info ts=2024-11-25T22:16:18.359568463Z caller=basic_lifecycle.go:297 msg="instance not found in the ring" instance=vbox ring=distributor
level=info ts=2024-11-25T22:16:18.359830163Z caller=ring.go:273 msg="ring doesn't exist in KV store yet"
level=info ts=2024-11-25T22:16:18.359791069Z caller=ingester.go:447 msg="recovered WAL checkpoint recovery finished" elapsed=497.491µs errors=false
level=info ts=2024-11-25T22:16:18.359985386Z caller=ingester.go:453 msg="recovering from WAL"
level=info ts=2024-11-25T22:16:18.360246831Z caller=ingester.go:469 msg="WAL segment recovery finished" elapsed=953.353µs errors=false
level=info ts=2024-11-25T22:16:18.360257321Z caller=ingester.go:417 msg="closing recoverer"
level=info ts=2024-11-25T22:16:18.360261779Z caller=ingester.go:425 msg="WAL recovery finished" time=968.712µs
level=info ts=2024-11-25T22:16:18.360414548Z caller=lifecycle.go:614 msg="not loading tokens from file, tokens file path is empty"
level=info ts=2024-11-25T22:16:18.360457565Z caller=wal.go:156 msg="started component=wal"
level=info ts=2024-11-25T22:16:18.360437942Z caller=lifecycle.go:643 msg="instance not found in ring, adding with no tokens" ring=ingester
level=info ts=2024-11-25T22:16:18.360478148Z caller=lifecycle.go:483 msg="auto-joining cluster after timeout" ring=ingester
level=info ts=2024-11-25T22:16:18.545006668Z caller=ringmanager.go:205 msg="scheduler is JOINING in the ring"
level=info ts=2024-11-25T22:16:18.545271169Z caller=ringmanager.go:214 msg="waiting until scheduler is ACTIVE in the ring"
level=info ts=2024-11-25T22:16:18.545578826Z caller=ringmanager.go:218 msg="scheduler is ACTIVE in the ring"
level=info ts=2024-11-25T22:16:18.54565001Z caller=module_service.go:82 msg=initialising module=query-scheduler
level=info ts=2024-11-25T22:16:18.545701467Z caller=module_service.go:82 msg=initialising module=query-frontend
level=info ts=2024-11-25T22:16:18.545942283Z caller=module_service.go:82 msg=initialising module=querier
level=info ts=2024-11-25T22:16:18.546020672Z caller=loki.go:505 msg="Loki started"
level=info ts=2024-11-25T22:16:21.546579205Z caller=scheduler.go:615 msg="this scheduler is in the ReplicationSet, will now accept requests."
```

Рис. 13 – Просмотр логов, отправленных от Log-Sender

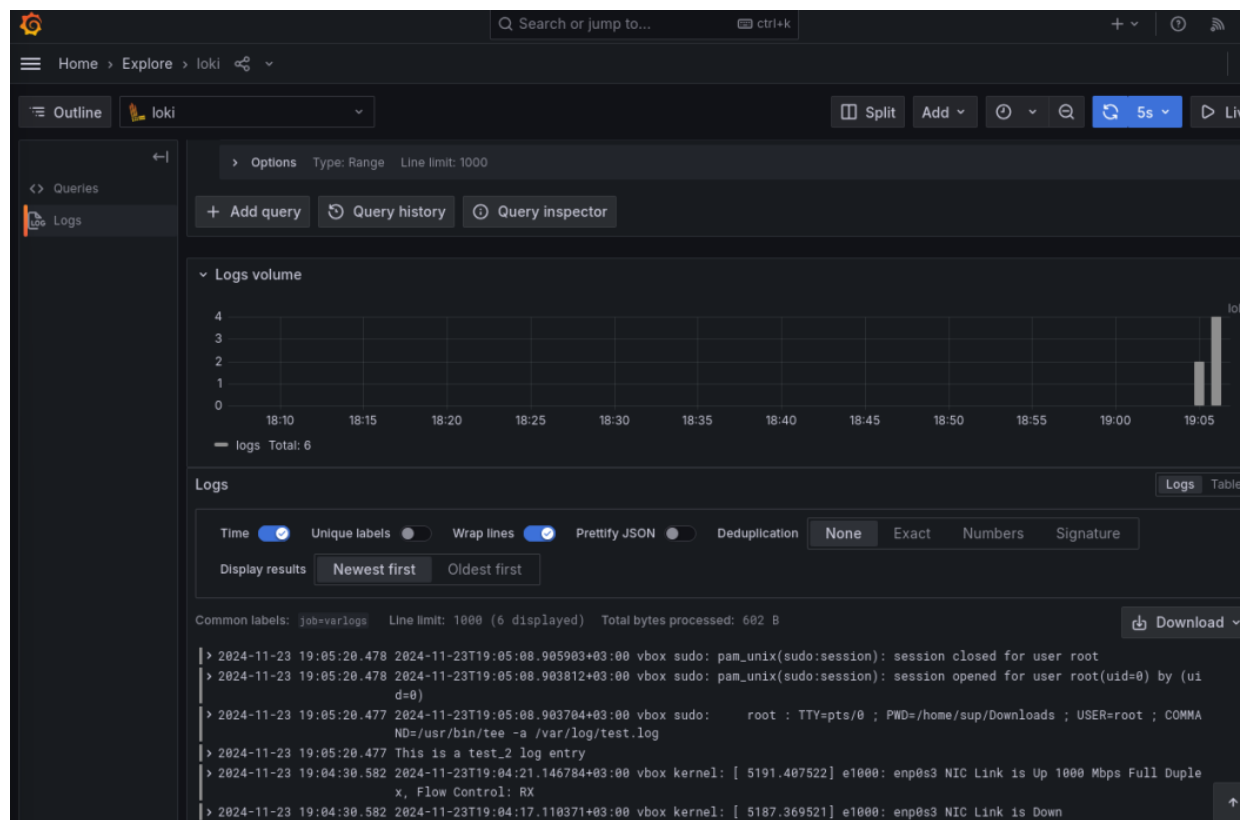
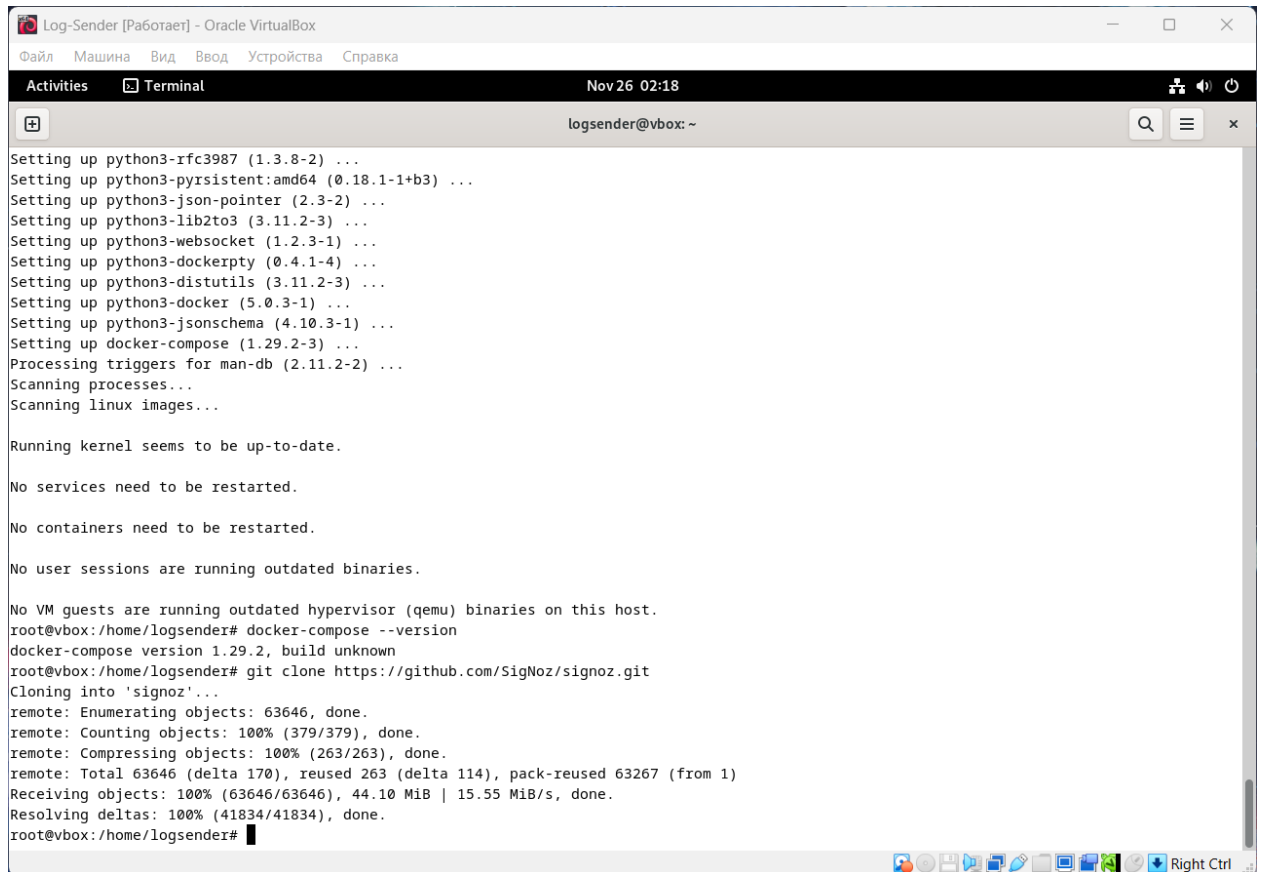


Рис. 13 – Signoz установка



```
Log-Sender [Работает] - Oracle VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  Terminal  Nov 26 02:18
logsender@vbox: ~

Setting up python3-rfc3987 (1.3.8-2) ...
Setting up python3-pyrsistent:amd64 (0.18.1-1+b3) ...
Setting up python3-json-pointer (2.3-2) ...
Setting up python3-lib2to3 (3.11.2-3) ...
Setting up python3-websocket (1.2.3-1) ...
Setting up python3-dockerpty (0.4.1-4) ...
Setting up python3-distutils (3.11.2-3) ...
Setting up python3-docker (5.0.3-1) ...
Setting up python3-jsschema (4.10.3-1) ...
Setting up docker-compose (1.29.2-3) ...
Processing triggers for man-db (2.11.2-2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@vbox:/home/logsender# docker-compose --version
docker-compose version 1.29.2, build unknown
root@vbox:/home/logsender# git clone https://github.com/SigNoz/signoz.git
Cloning into 'signoz'...
remote: Enumerating objects: 63646, done.
remote: Counting objects: 100% (379/379), done.
remote: Compressing objects: 100% (263/263), done.
remote: Total 63646 (delta 170), reused 263 (delta 114), pack-reused 63267 (from 1)
Receiving objects: 100% (63646/63646), 44.10 MiB | 15.55 MiB/s, done.
Resolving deltas: 100% (41834/41834), done.
root@vbox:/home/logsender#
```

Рис. 14 – Signoz запущен и работает

```
[+] Running 59/39
✓ query-service 7 layers [#####] 0B/0B Pulled
✓ zookeeper-1 1 layers [##] 0B/0B Pulled
✓ alertmanager 6 layers [#####] 0B/0B Pulled
✓ load-hotrod 7 layers [#####] 0B/0B Pulled
✓ hotrod 1 layers [##] 0B/0B Pulled
✓ otel-collector-migrator-async 2 layers [###] 0B/0B Pulled
✓ frontend 11 layers [#####] 0B/0B Pulled
✓ otel-collector 3 layers [###] 0B/0B Pulled
✓ otel-collector-migrator-sync Pulled
✓ clickhouse 7 layers [#####] 0B/0B Pulled
✓ logspout 3 layers [###] 0B/0B Pulled

[+] Running 12/12
✓ Network clickhouse-setup_default Created
✓ Container signoz-zookeeper-1 Started
✓ Container hotrod Started
✓ Container load-hotrod Started
✓ Container signoz-clickhouse Healthy
✓ Container otel-migrator-sync Exited
✓ Container signoz-query-service Healthy
✓ Container otel-migrator-async Started
✓ Container signoz-otel-collector Started
✓ Container signoz-alertmanager Started
✓ Container signoz-logspout Started
✓ Container signoz-frontend Started
```


Рис. 15 – Signoz проверка работоспособности

