|  |
| --- |
|  |
| 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-02-24

Дмитриев Д.В.

Проверил

Петров К. Е.

Москва

2024

**ПРЗ. Сбор логов**

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>

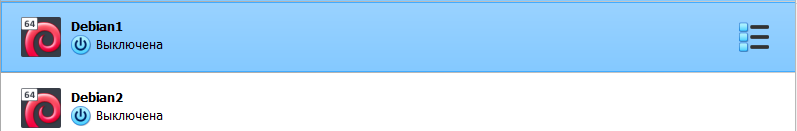
2. Обеспечить между ними сетевой обмен <https://www.virtualbox.org/manual/ch06.html>

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/>

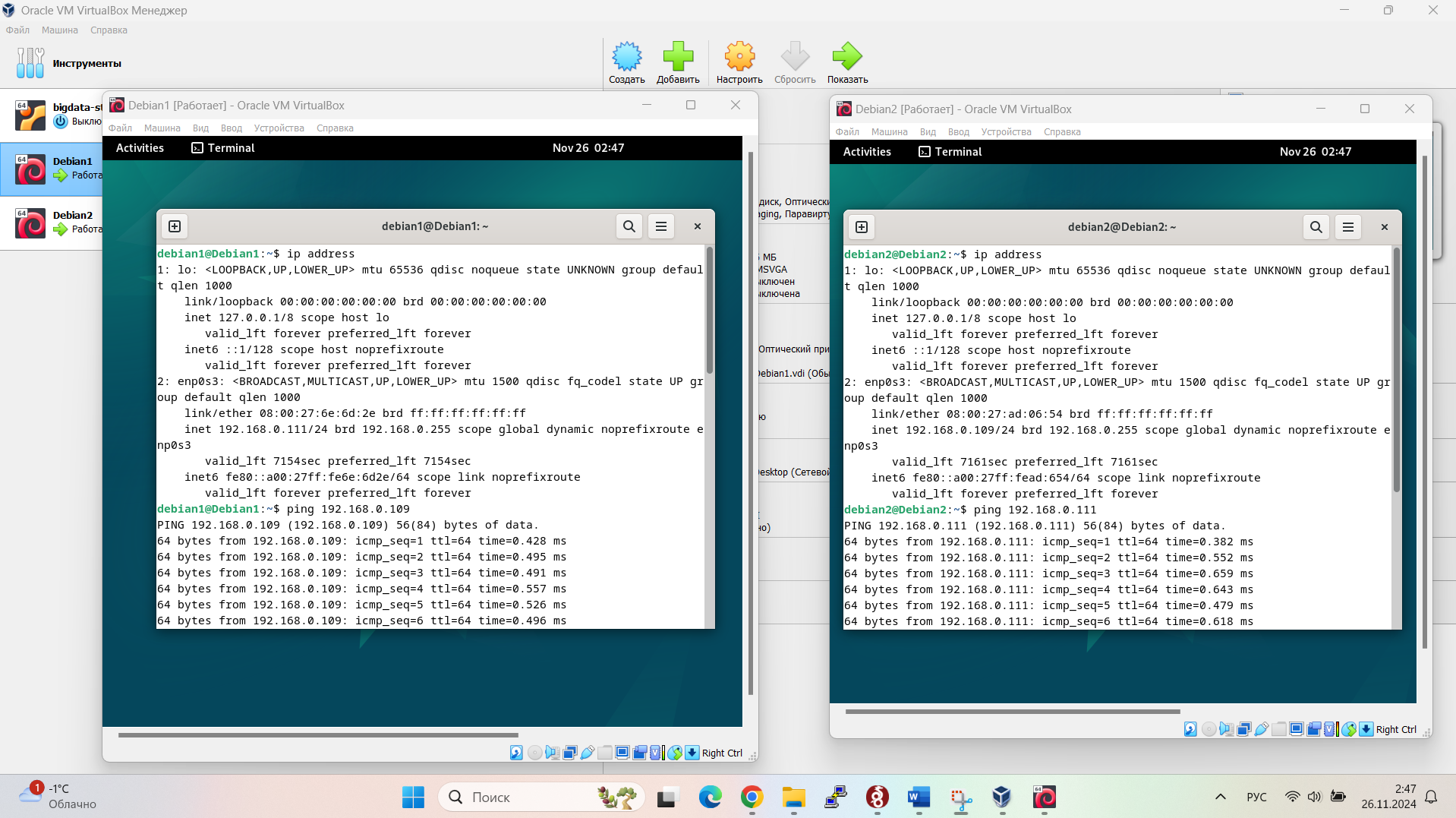
4. Установить и настроить получение логов на сервер с использованием Loki https://github.com/grafana/loki https://docs.google.com/document/d/11tjK\_lvp1-SVsFZjgOTr1vV3- q6vBAsZYIQ5ZeYBkyM/view (источник можно выбрать самостоятельно)

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)

**1.** Создаем 2виртуальные машины на базе ОС Debian 12

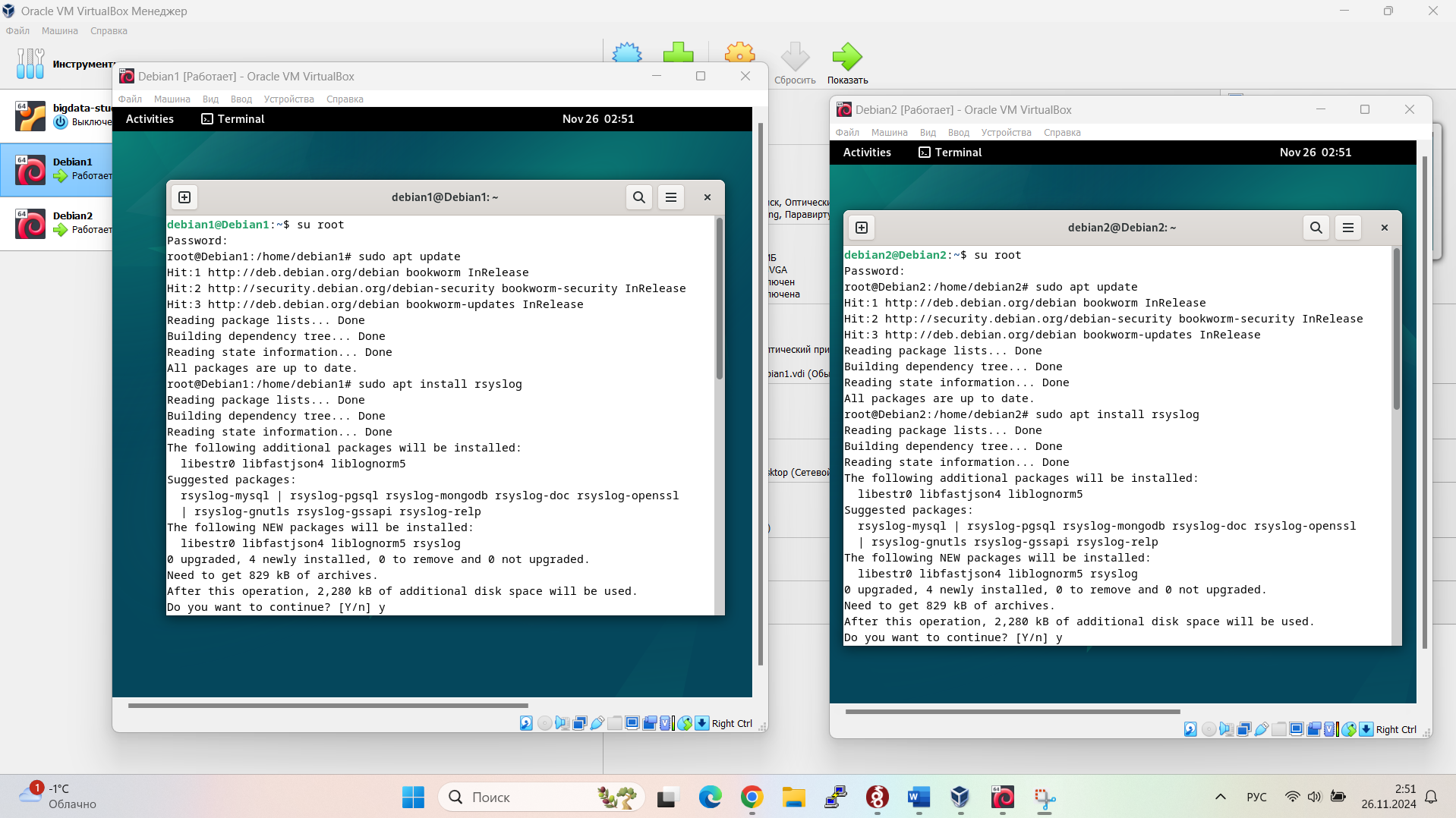
****

**2.** Обеспечим между ними сетевой обмен

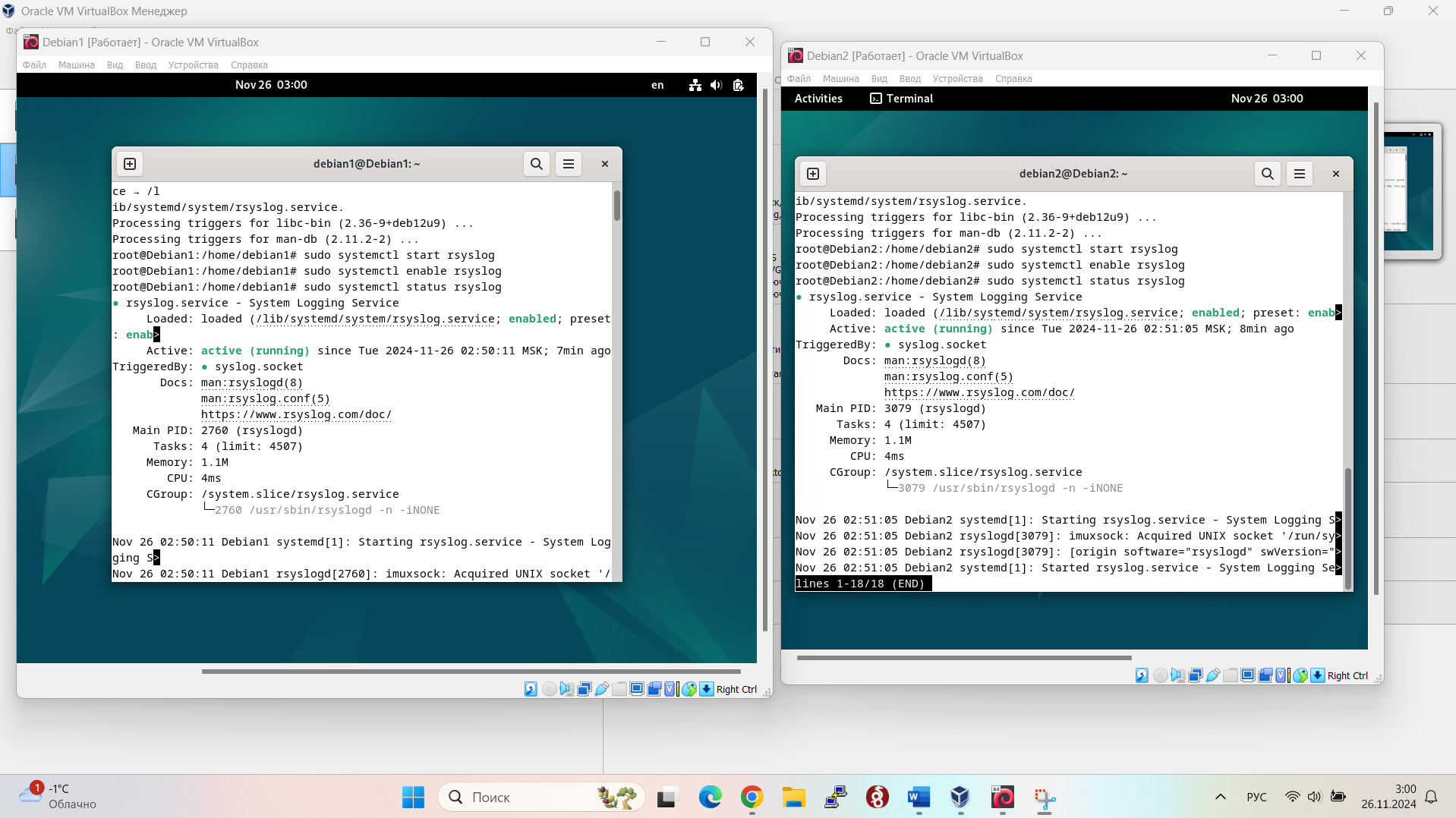


**3.** Включить на 1й ВМ передачу логов по протоколу rsyslog на 2ю ВМ

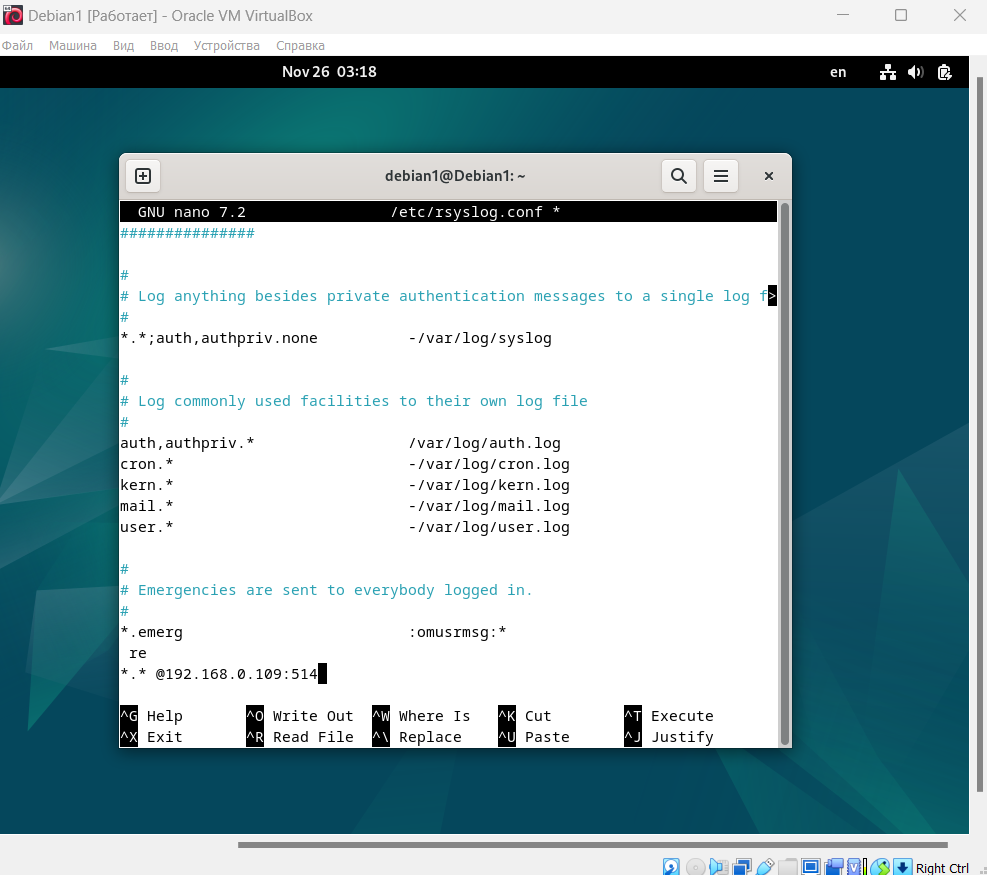
3.1 Установим rsyslog

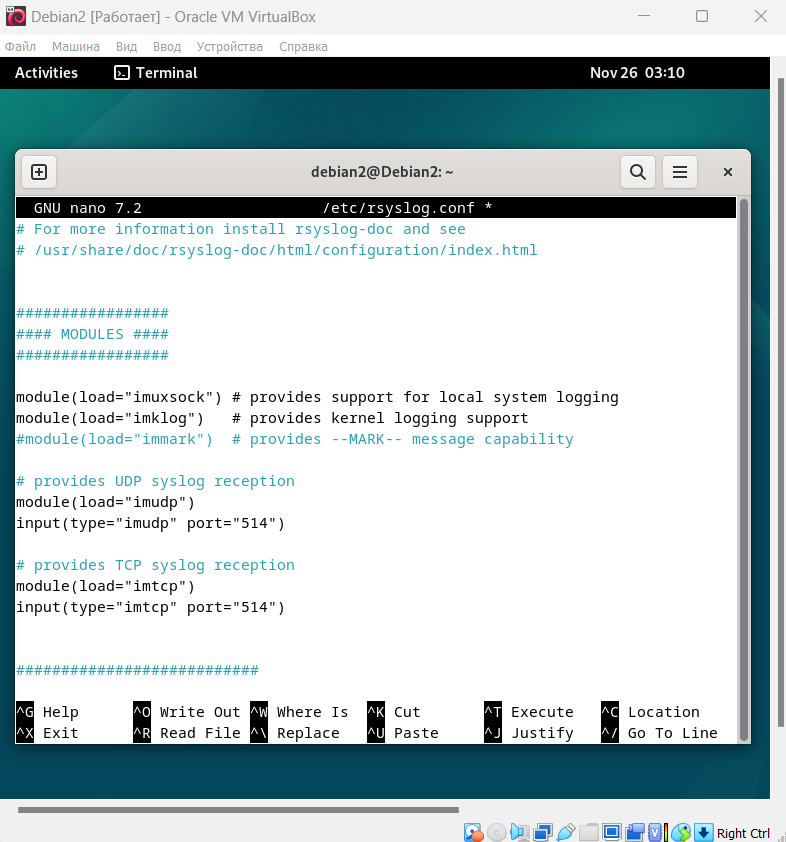


3.2 Проверим работоспособность rsyslog

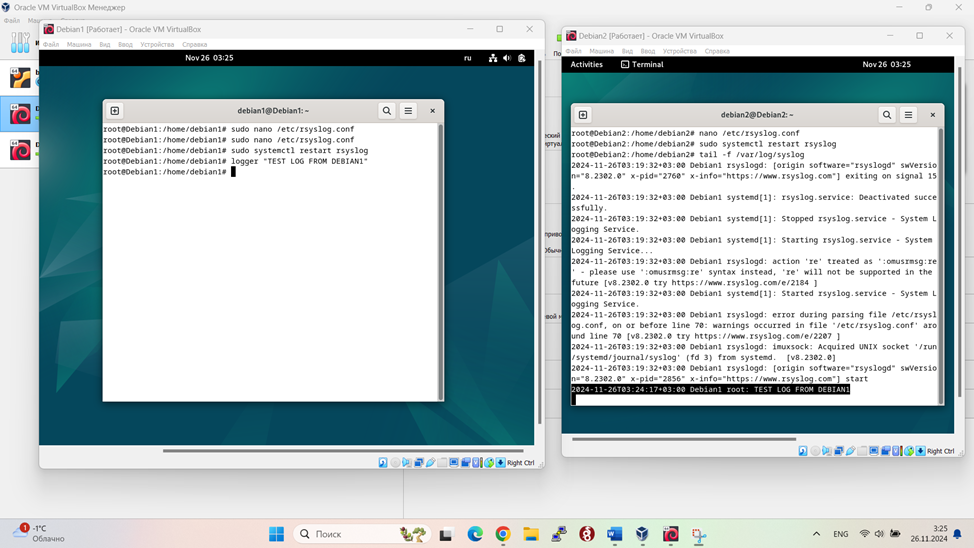


3.3 Отредактируем конфигурационный файл на 1й и 2й ВМ



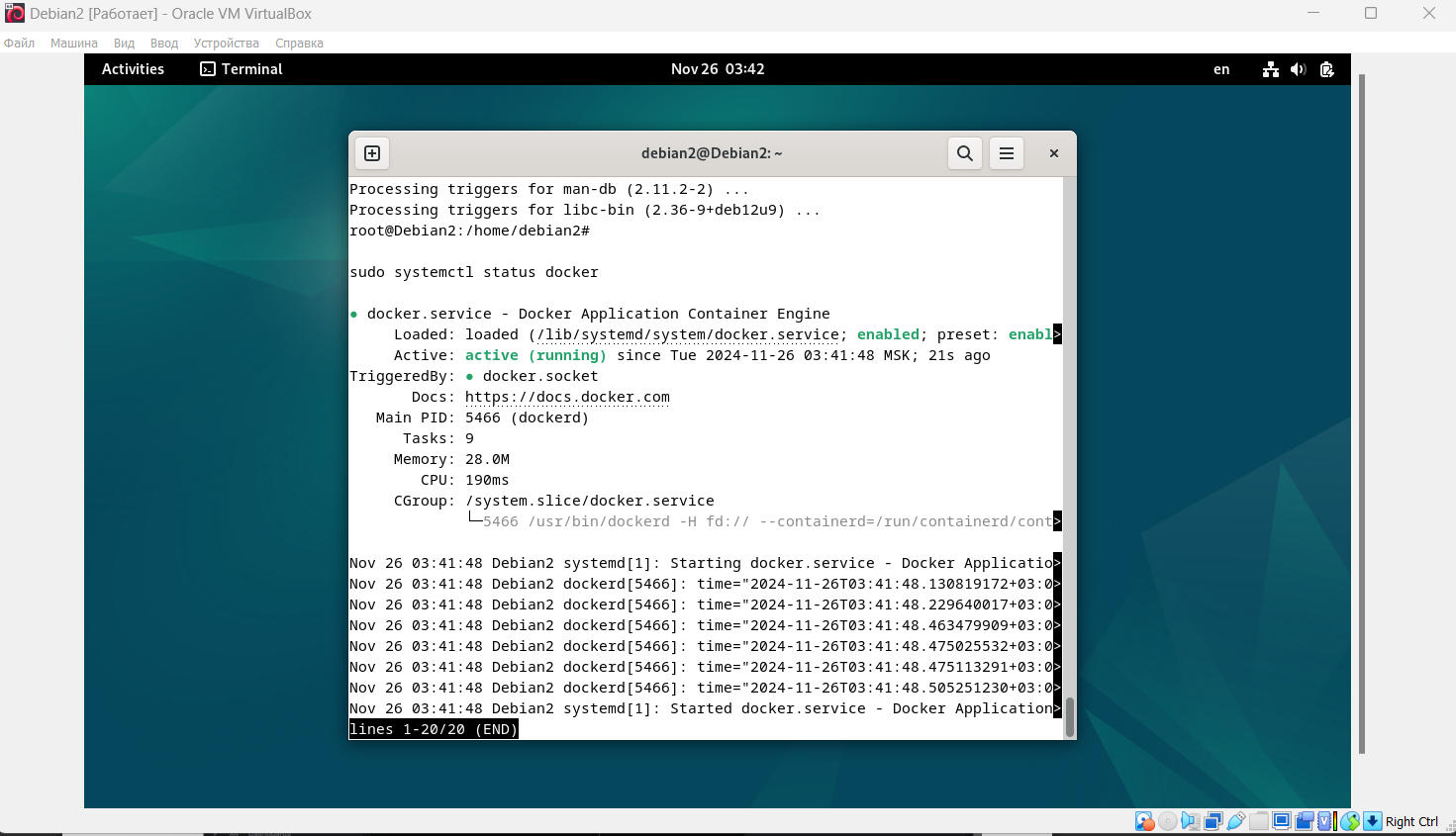


3.4 Проверка получения логов

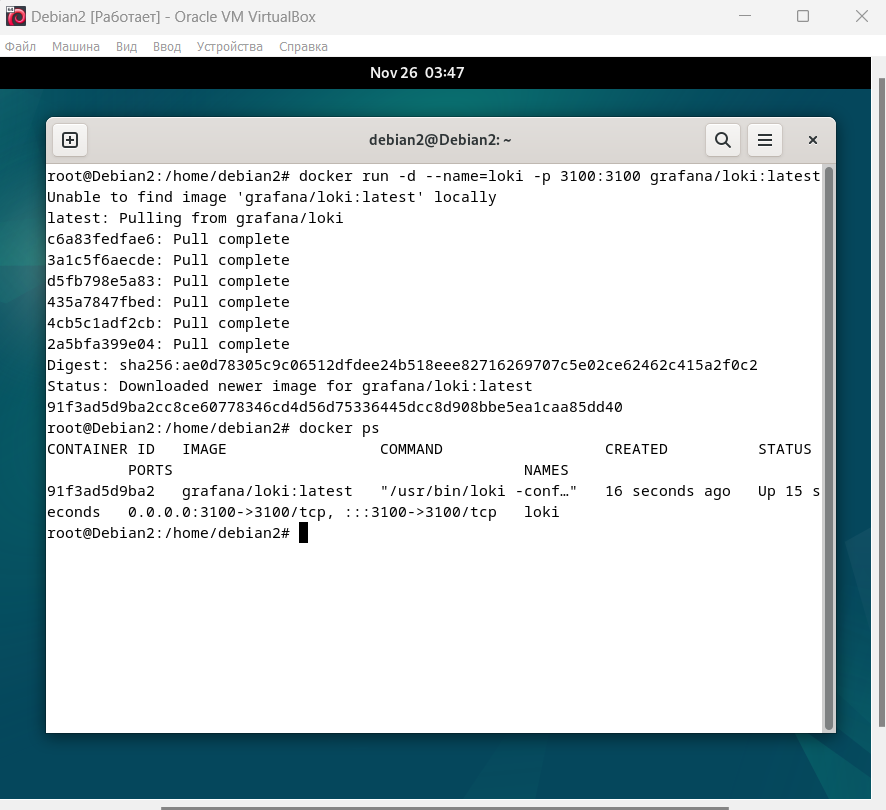


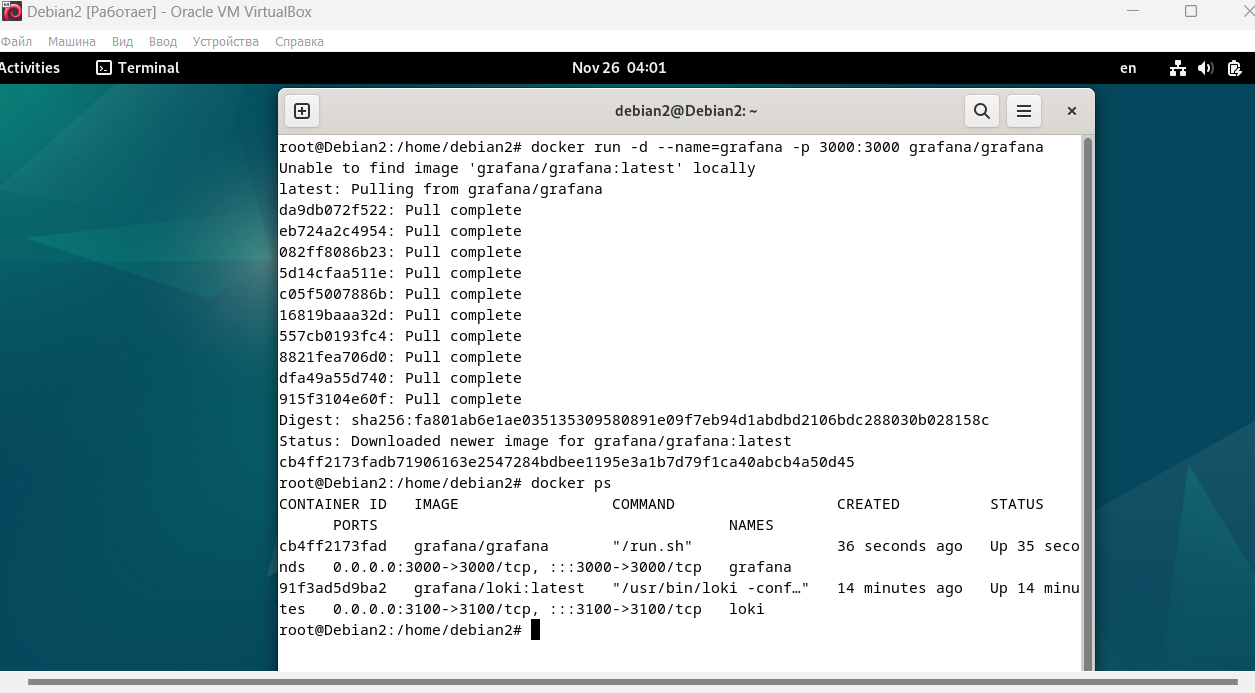
**4.** . Установить и настроить получение логов на сервер с использованием Loki

4.1 Установим docker и проверим его работоспособность

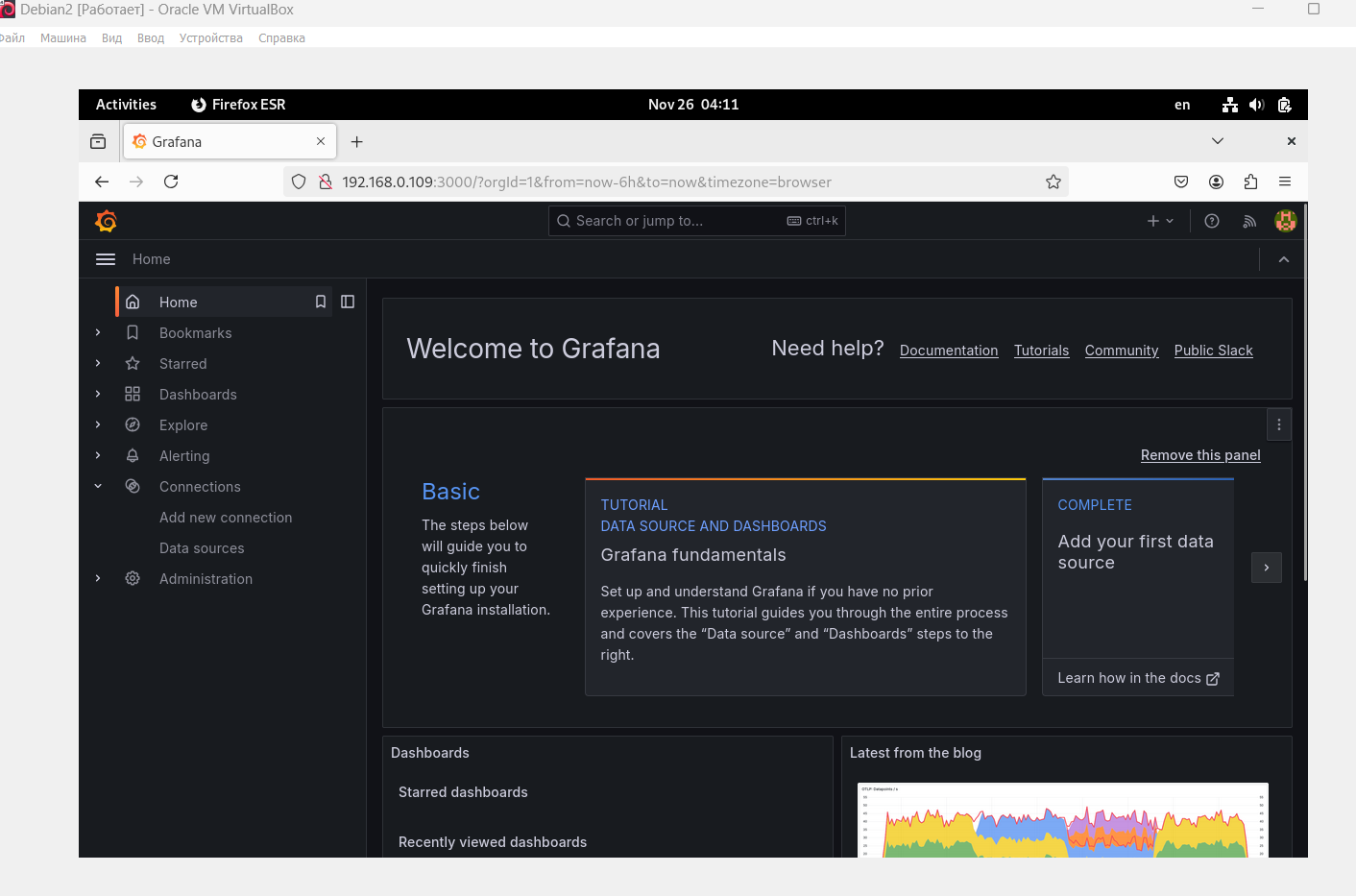


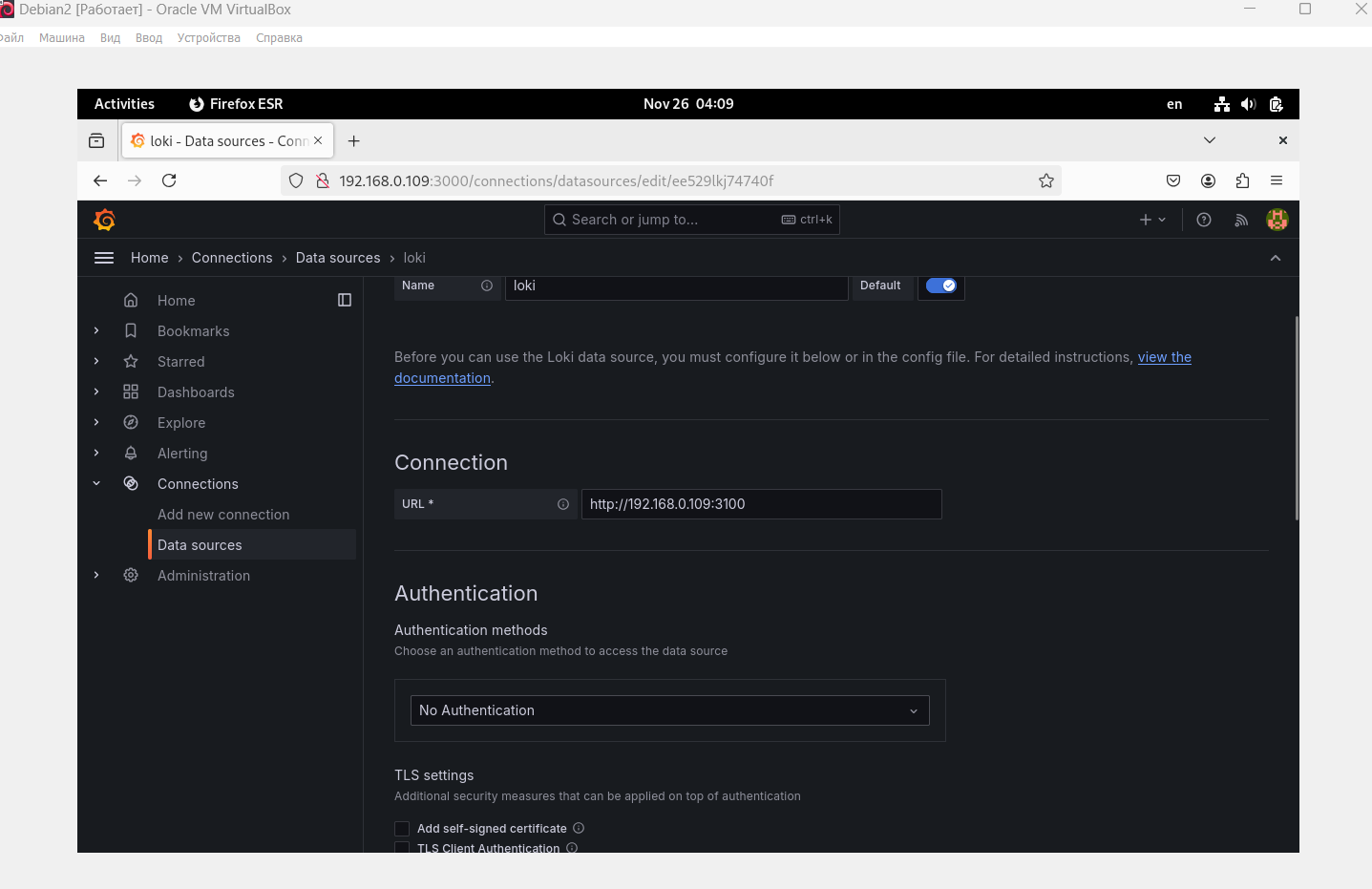
4.2 Запускаем контейнеры

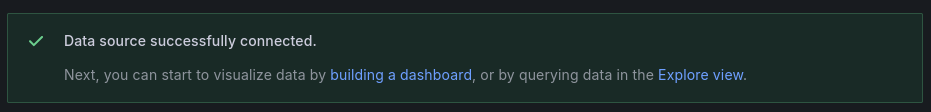




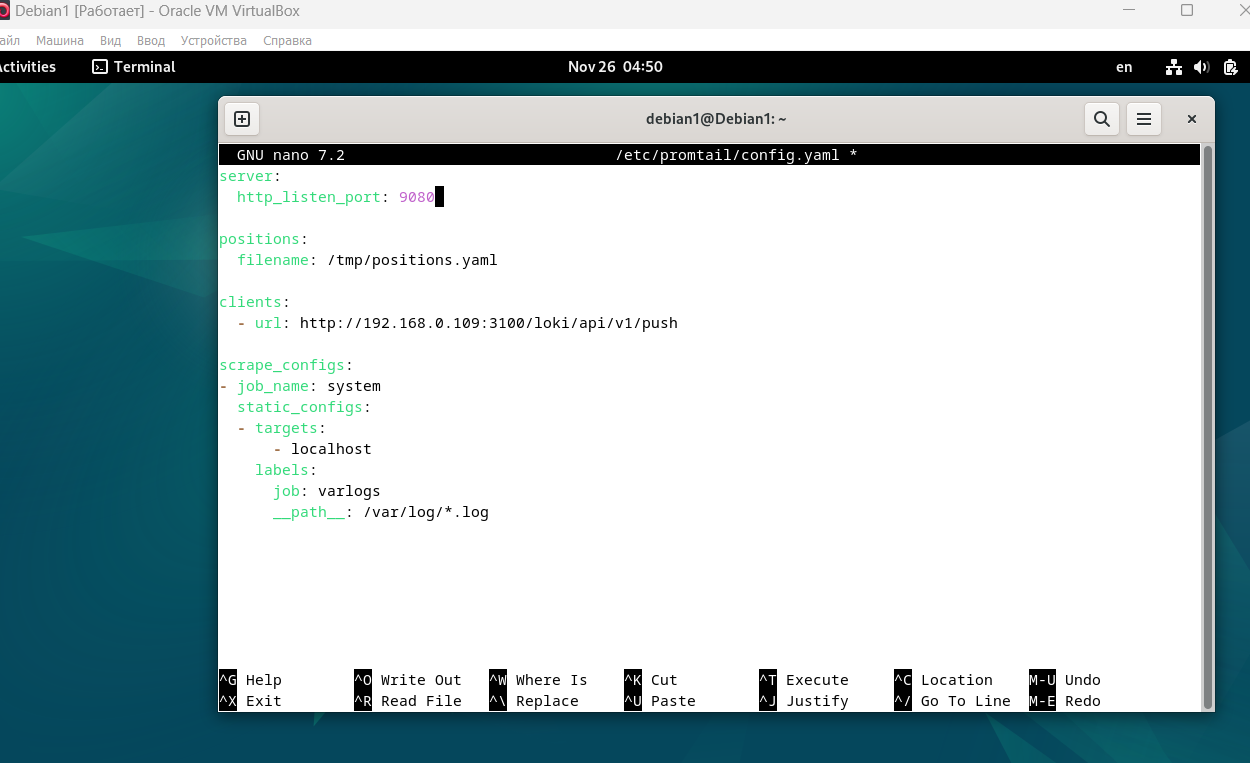
4.3 Заходим на web-интерфейс Grafana и добавляем в Grafana связку с Loki:



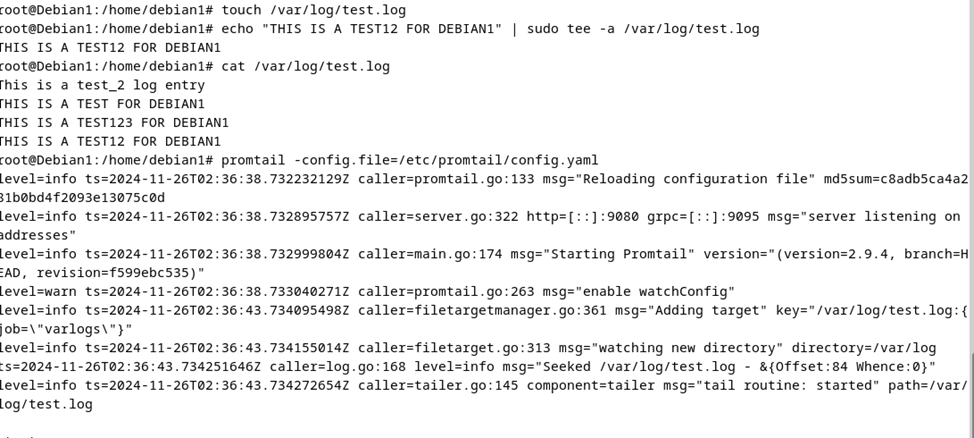




4.4 Для передачи логов устанавливаем утилиту Promtail и редактируем его конфигурационный файл



4.5 Запускаем утилиту Promtail

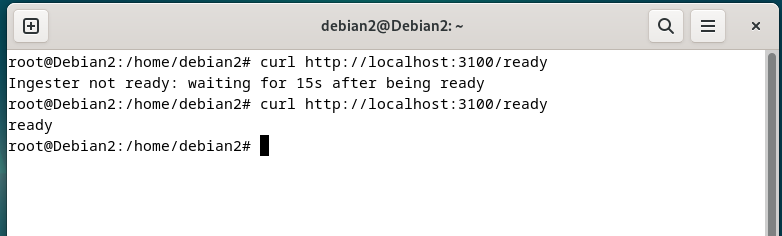


4.6 В файле /tmp/positions.yaml указаны позиции файлообменников для

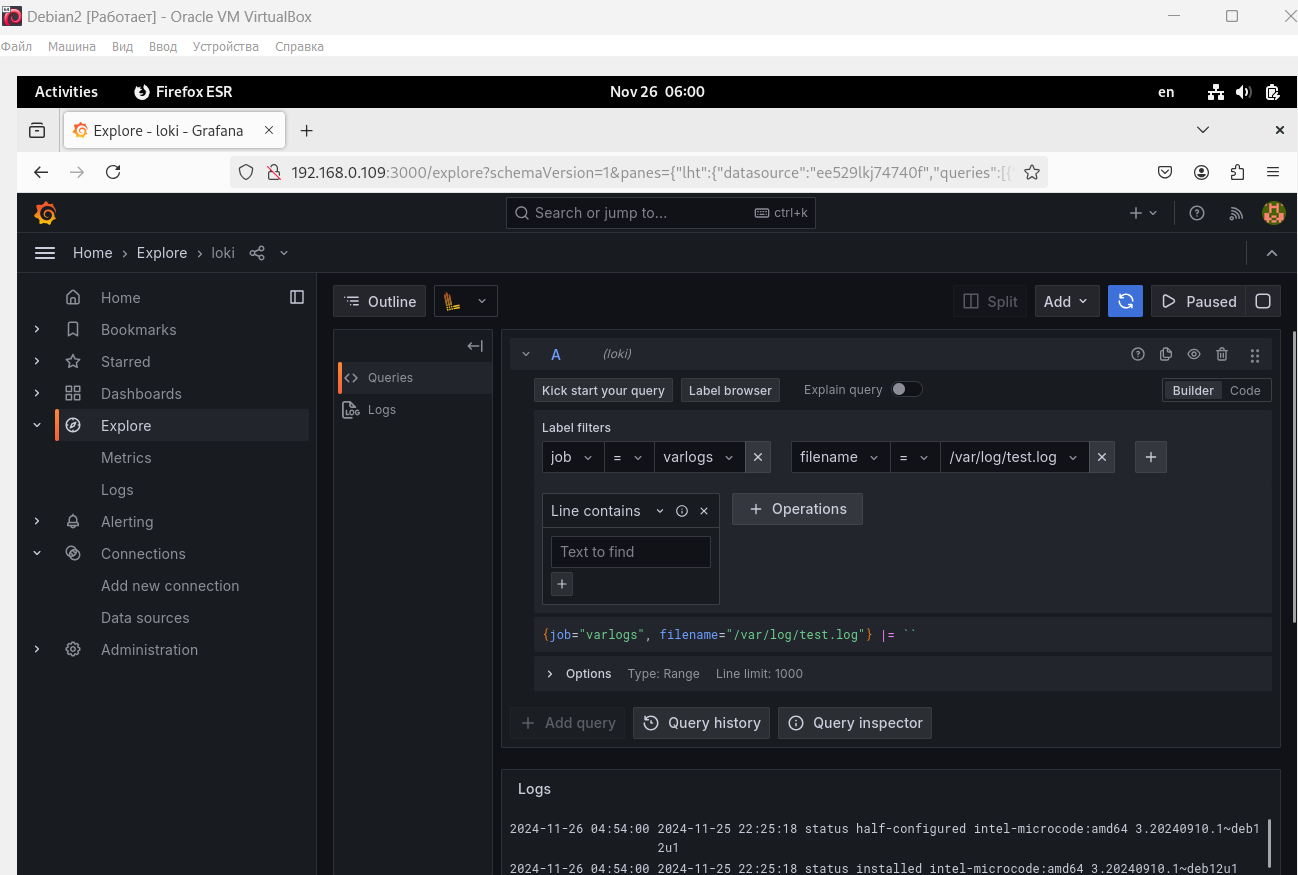
логов, которые будут отправляться с 1й ВМ на 2ю ВМ .

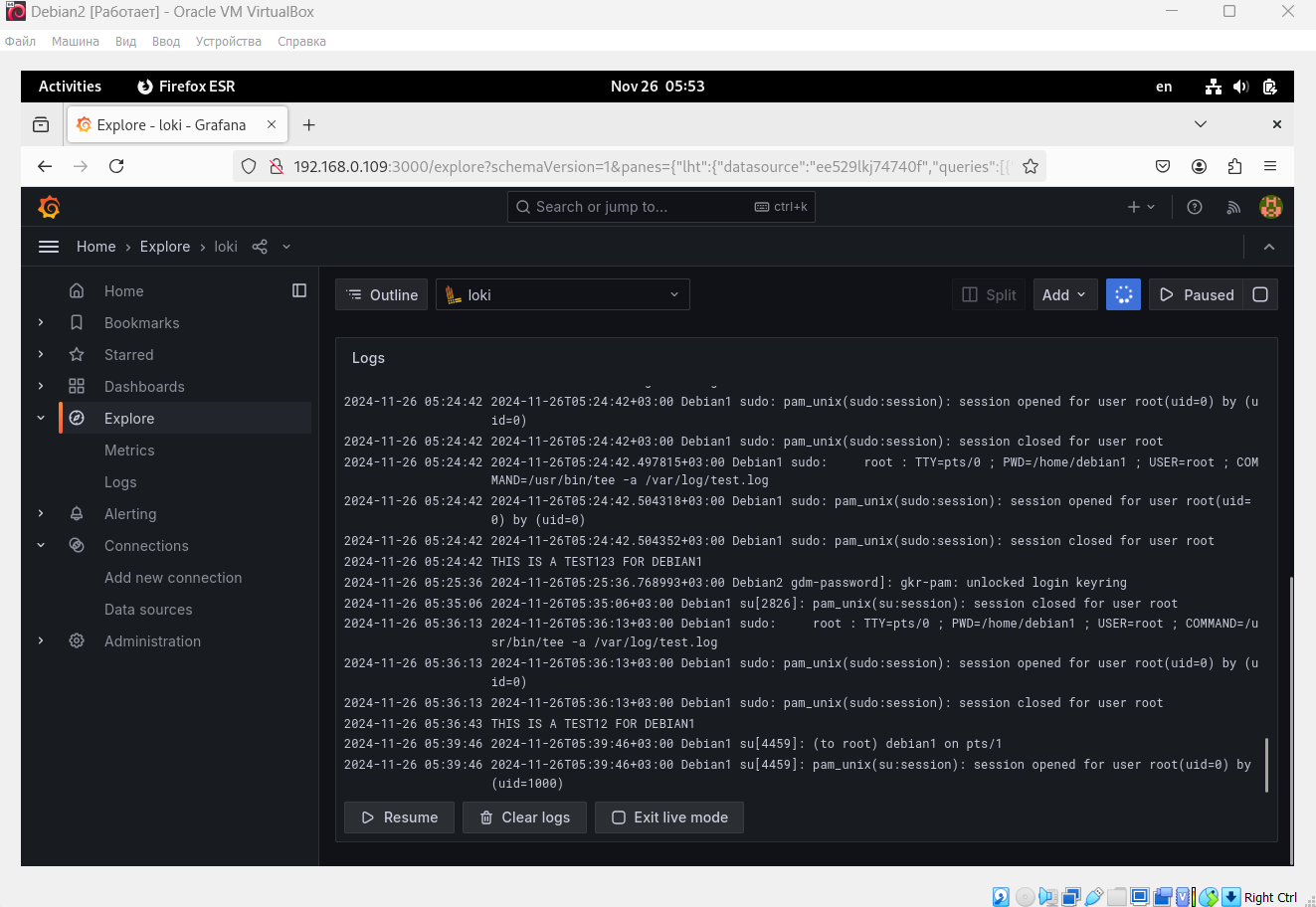


4.7 На ВМ2 проверяем готовность Loki



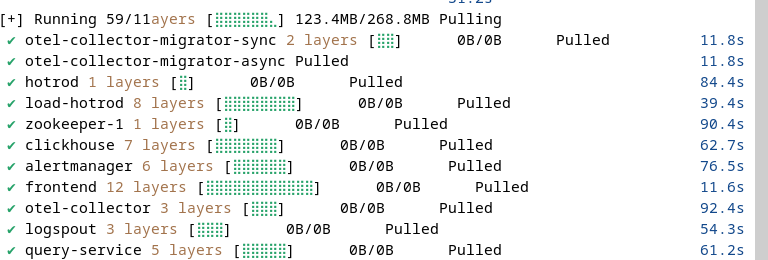
4.8 Просматриваем логи от 1й ВМ

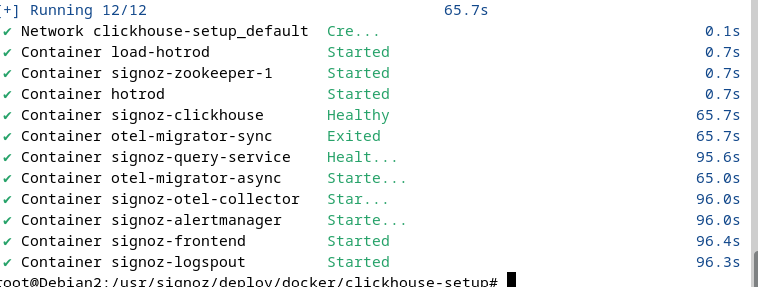




**5.** Установить и настроить получение логов на сервер с использованием Signoz

5.1 Устанавливаем docker-compose и signoz на ВМ2 после чего запускаем контейнеры командой **docker-compose up -d**







1. signoz-zookeeper:

Служит для координации и управления распределенными компонентами

(используется для Kafka).

2. signoz-alertmanager:

Управляет уведомлениями и алертами (например, когда происходят сбои).

3. signoz-otel-collector:

Средство для сбора метрик, логов и трасс; перенаправляет данные в

основной хранилище.

4. signoz-logspout:

Собирает контейнерные логи с Docker и направляет их в Signoz.

5. signoz-query-service:

Выполняет запросы к базе (ClickHouse), отвечает за доставку данных в

интерфейс.

6. signoz-clickhouse:

Хранилище данных (метрики, трассировки и логи сохраняются здесь).

7. signoz-frontend:

Интерфейс для пользователей — отображает метрики, трассы и логи.

8. load-hotrod (Locust):

Генератор нагрузки для тестирования (используется для демонстраций).

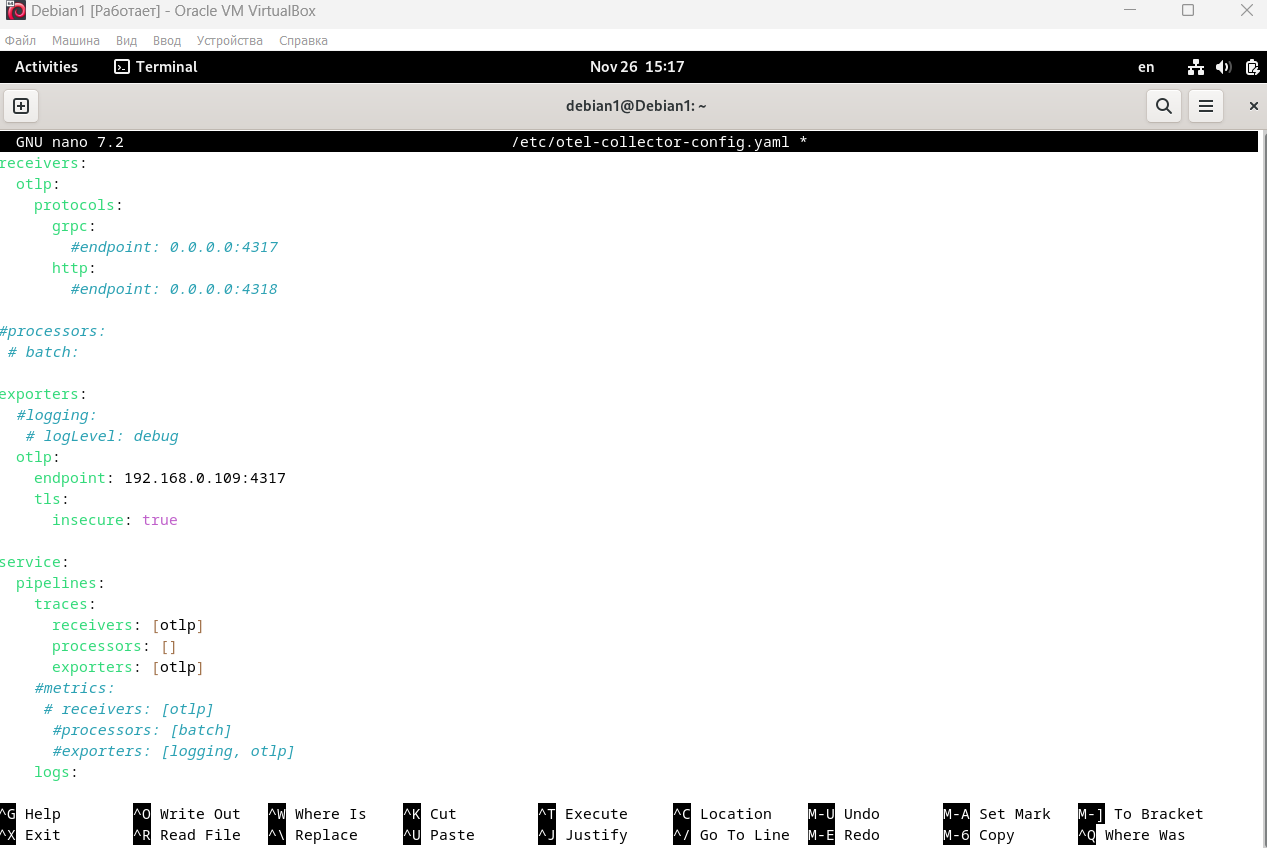
9. hotrod:

Пример микросервиса, чтобы демонстрировать работу трассировки в

Signoz.

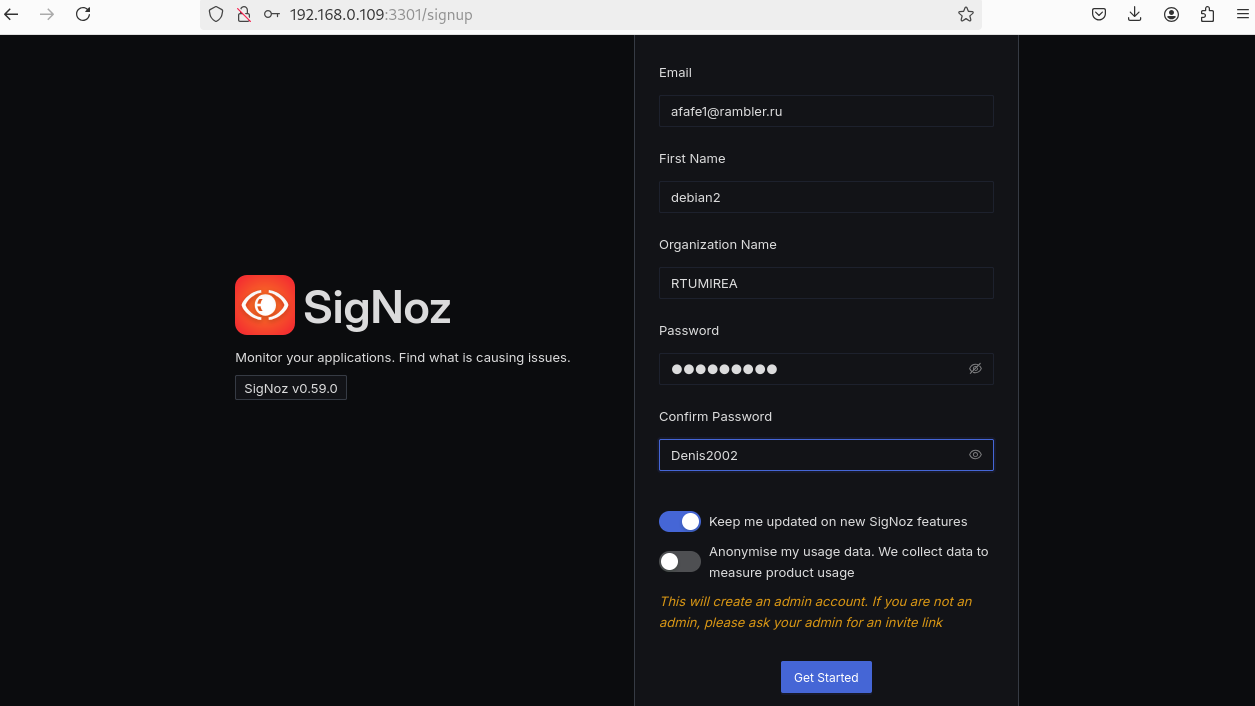
5.2 Устанавливаем утилиту **OpenTelemetry.** Онапредоставляет инструменты и стандарты для сбора, обработки и экспорта данных о телеметрии (метрики, трассировки и логи) в системы мониторинга и анализа.

5.3 Редактируем конфигурационный файл

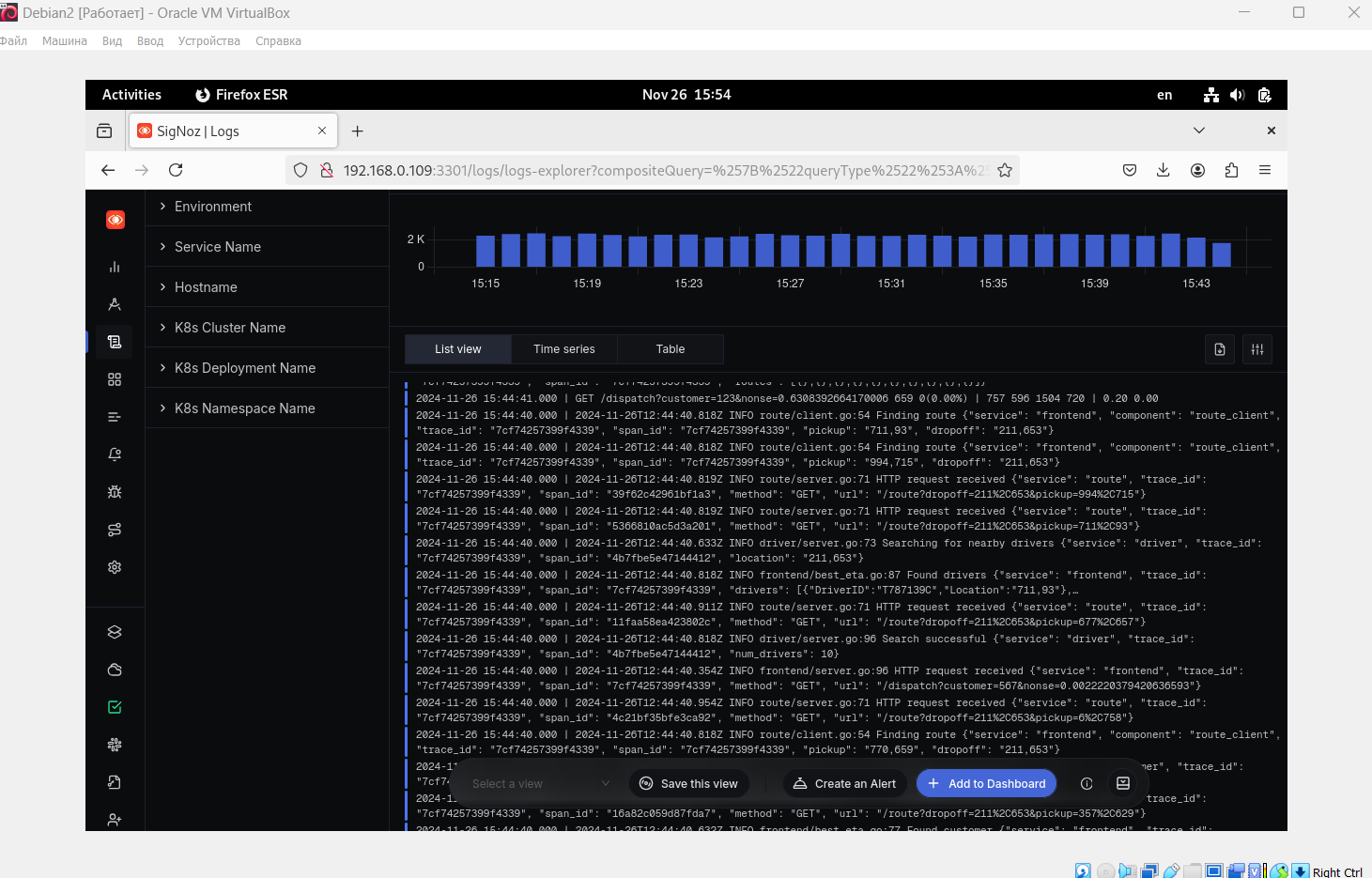


5.4 запускаем утилиту командой **otelcol-contrib --config=/etc/otel-collector-config.yaml**

5.5 Заходим в web-интерфейс Signoz и регистрируемся



5.6 Проверка работоспособности



Вывод:

**Loki** - это система для сбора, хранения и обработки логов, разработанная компанией **Grafana**. Она предназначена для работы с большими объемами логов, обеспечивая их эффективное хранение, поиск и визуализацию. **Promtail** - это утилита сбора логов, которая используется в связке с **Loki** для получения, обработки и отправки логов в систему **Loki**.

**Signoz** - система мониторинга и анализа производительности, которая предоставляет инструменты для сбора, хранения и визуализации телеметрических данных (включая метрики, логи и трассировки) для приложений (**SigNoz** собирает данные через **OpenTelemetry**)