|  |  |  |
| --- | --- | --- |
|  |  |  |
| 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 № 3**

**по дисциплине ««Технологии обеспечения информационной безопасностью»**

Тема: «Сбор логов»

Выполнил

Студент 1 курса

Группы ББМО-01-23

Белов Владимир Станиславович

Шифр 23Б1716

Москва 2023

**Цели работы:**

1. Обобщить, закрепить лекционный и теоретический материал по теме.

**Вопросы для самоконтроля и самостоятельной работы:**

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)

Отчёт по практической работе

1. Создадим 2 виртуальные машины на базе ОС Debian 12

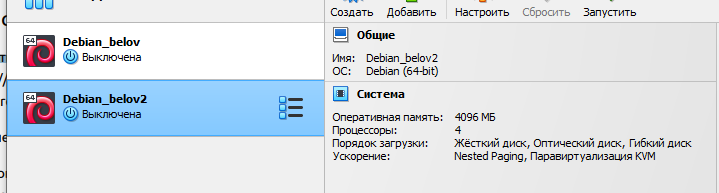


Рис. 1 – Виртуальные машины на базе ОС Debian 12

1. Обеспечим сетевой обмен между двумя виртуальными машинами в соответствии с инструкцией VirtualBox Manual.



Рис. 2 – Обеспечение сетевого обмена между машинами

1. Установим rsyslog на первую машину

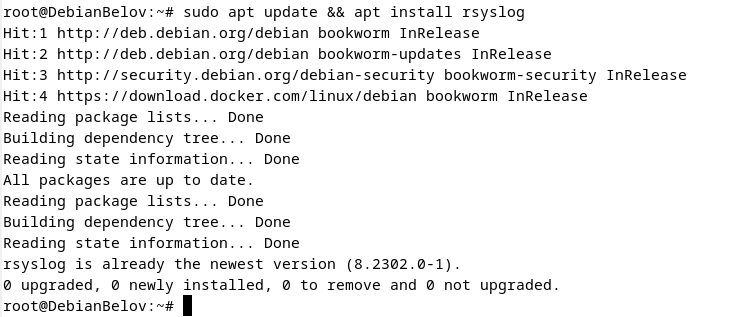


Рис. 3 – Процесс установки

1. После установки rsyslog вам нужно запустить службу, включить ее автоматический запуск при загрузке и проверить ее статус с помощью команды systemctl.

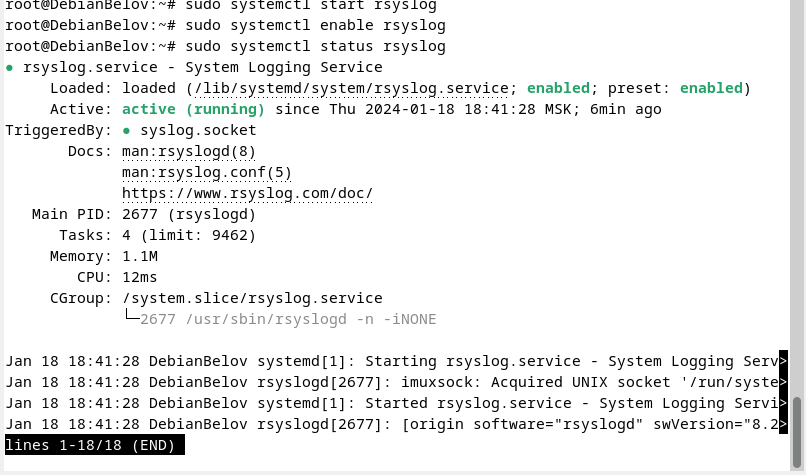


Рис. 4 – Запуск службы и проверка

1. Настроим rsyslog в качестве сетевого/центрального сервера журналирования, установим протокол (**UDP** и **TCP**) который он будет использовать для удаленного приема системного журнала, а также порт (514), который он прослушивает.

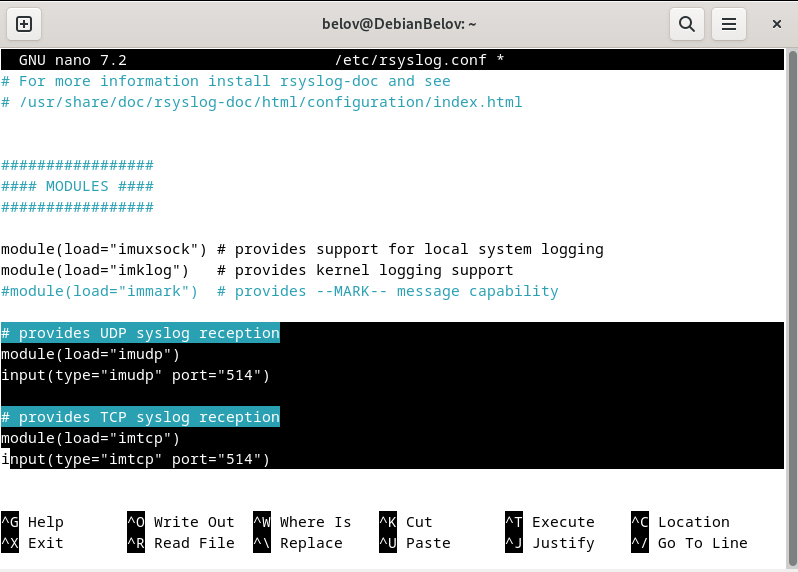


Рис. 5 – Настройки модулей rsyslog

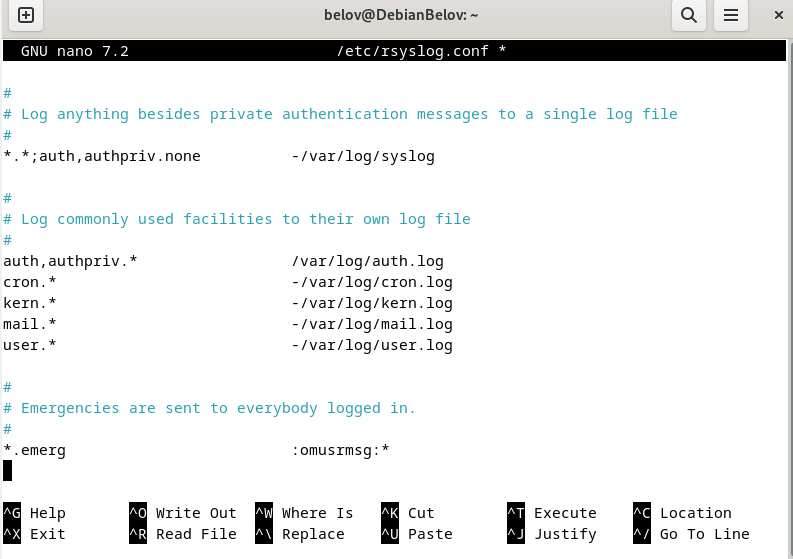


Рис. 6 – Настройки правил rsyslog

1. Теперь применим нашу конфигурацию

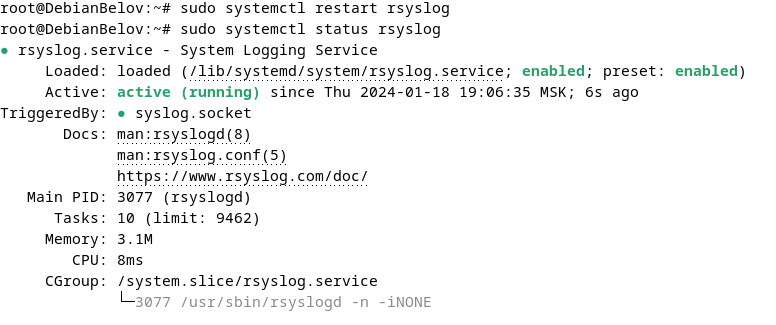


Рис. 7 – Перезапуск rsyslog с новой конфигурацией

1. Установим rsyslog на вторую машину

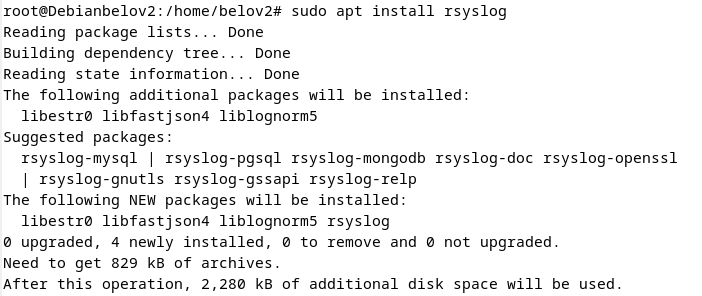
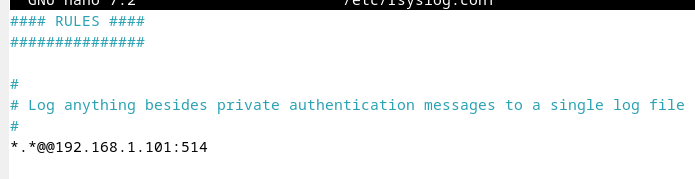


Рис. 8 –Установка rsyslog на вторую машину

1. Установим правило отправки логов на сервер и применим изменения в конфигурации



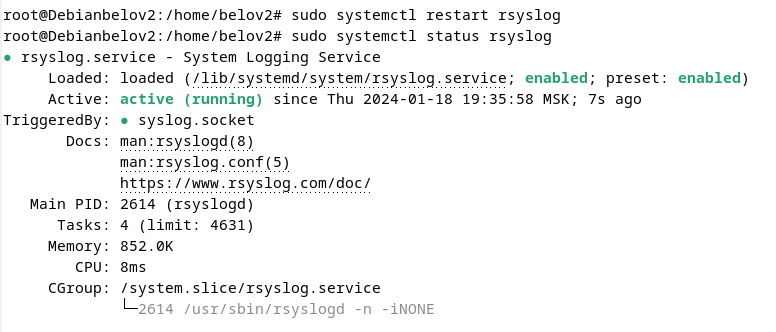
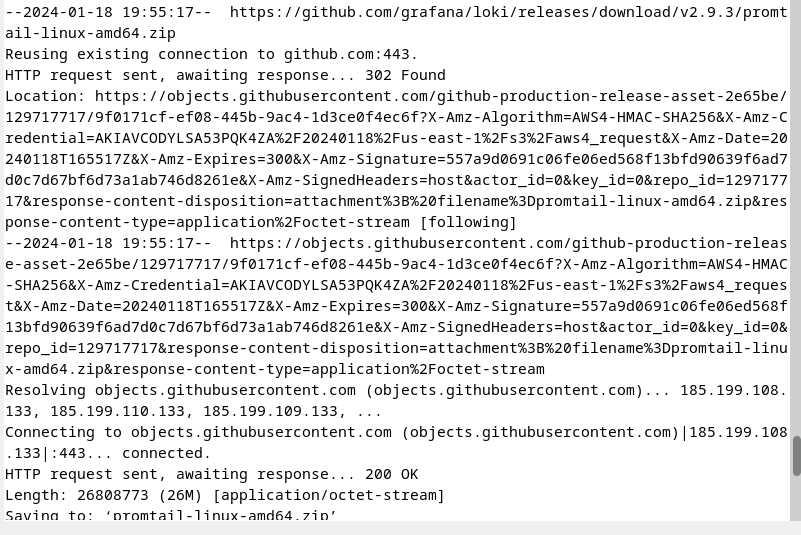


Рис. 9 и 10 – Настройки правил rsyslog и перезапуск конфигурации

1. Установим Grafana Loki и promtail



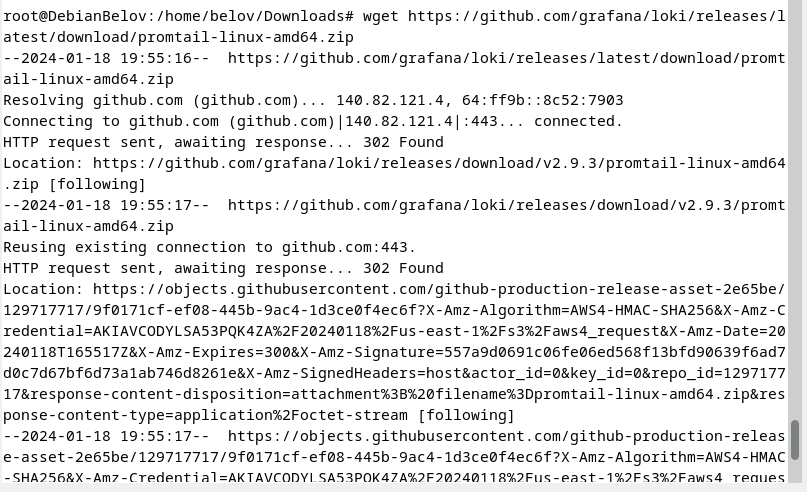


Рис. 11 – Установка Grafana Loki и promtail

Настроим комнфигурации в файле promtail

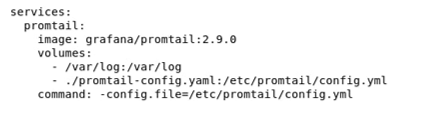
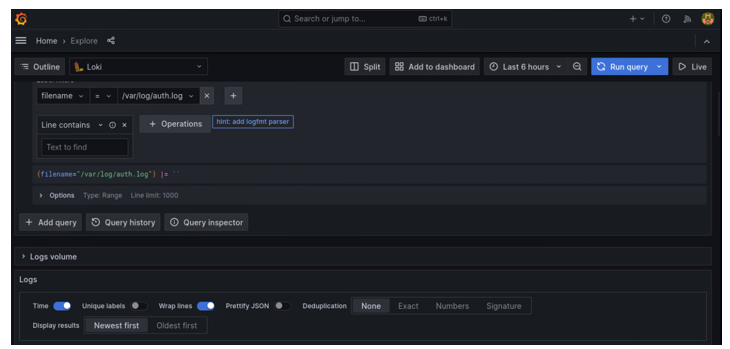


Рис. 12 – Compose файл promtail на клиенте



Рис. 13 – Файл конфигурации promtail на клиенте

****Рис. 14 – Просмотр клиента в Grafana

Установим и настроим получение логов на сервер с использованием Signoz. Установку проведем по инструкции https://signoz.io/docs/install/docker

****

Риc. 15 – Скачивание и установка signoz

Проверим полученые отчет по логам в Signoz

****

Риc 16 – Отчёт в signoz