Лабораторная работа №15

Настройка сетевого журналирования

Газизянов Владислав Альбертович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение практических навыков по работе с журналами системных событий, настройке централизованного сетевого журналирования и мониторинга событий в распределённой среде.

2 Задание

1. Настроить сервер сетевого журналирования событий
2. Настроить клиент для передачи системных сообщений в сетевой журнал
3. Просмотреть журналы системных событий с помощью различных инструментов
4. Разработать скрипты автоматизации для развертывания системы журналирования

3 Выполнение лабораторной работы

3.1 Настройка сервера сетевого журнала

3.1.1 Подготовка конфигурации

На серверной машине создан файл конфигурации сетевого хранения журналов в каталоге /etc/rsyslog.d/. Создан файл netlog-server.conf для настройки параметров сервера журналирования.

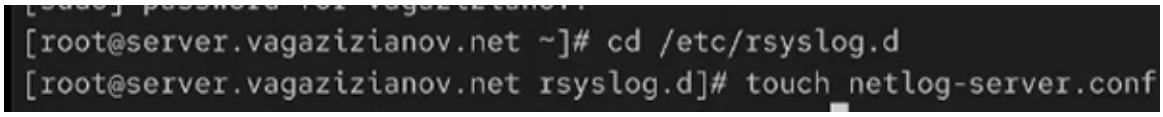

Рисунок 3.1: Создание конфигурационного файла сервера

3.1.2 Конфигурация TCP-приёмника

В файл конфигурации добавлены директивы для включения приёма записей журнала по TCP-порту 514. Загружен модуль imtcp и активирован TCP-сервер на указанном порту.

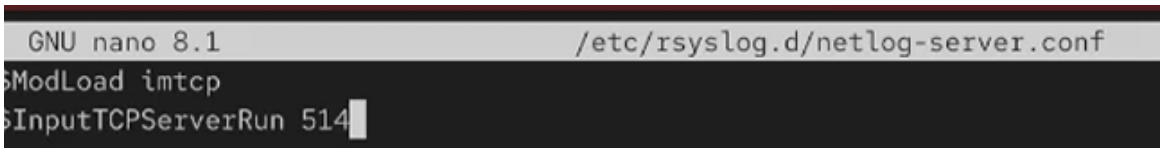

Рисунок 3.2: Конфигурация TCP-приёмника rsyslog

3.1.3 Перезапуск службы rsyslog

Выполнен перезапуск службы rsyslog для применения новых настроек. Проверено состояние службы и прослушиваемые порты, связанные с rsyslog.

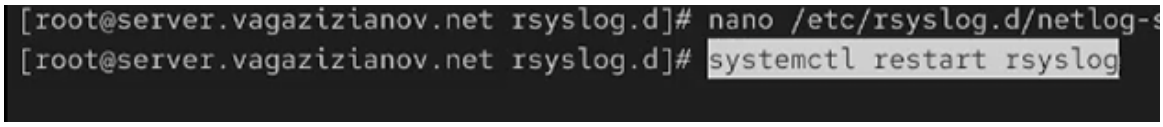

Рисунок 3.3: Перезапуск службы rsyslog

3.1.4 Проверка открытых портов

С помощью команды lsof проверено, что rsyslog прослушивает TCP-порт 514, что подтверждает корректность настройки сервера сетевого журналирования.

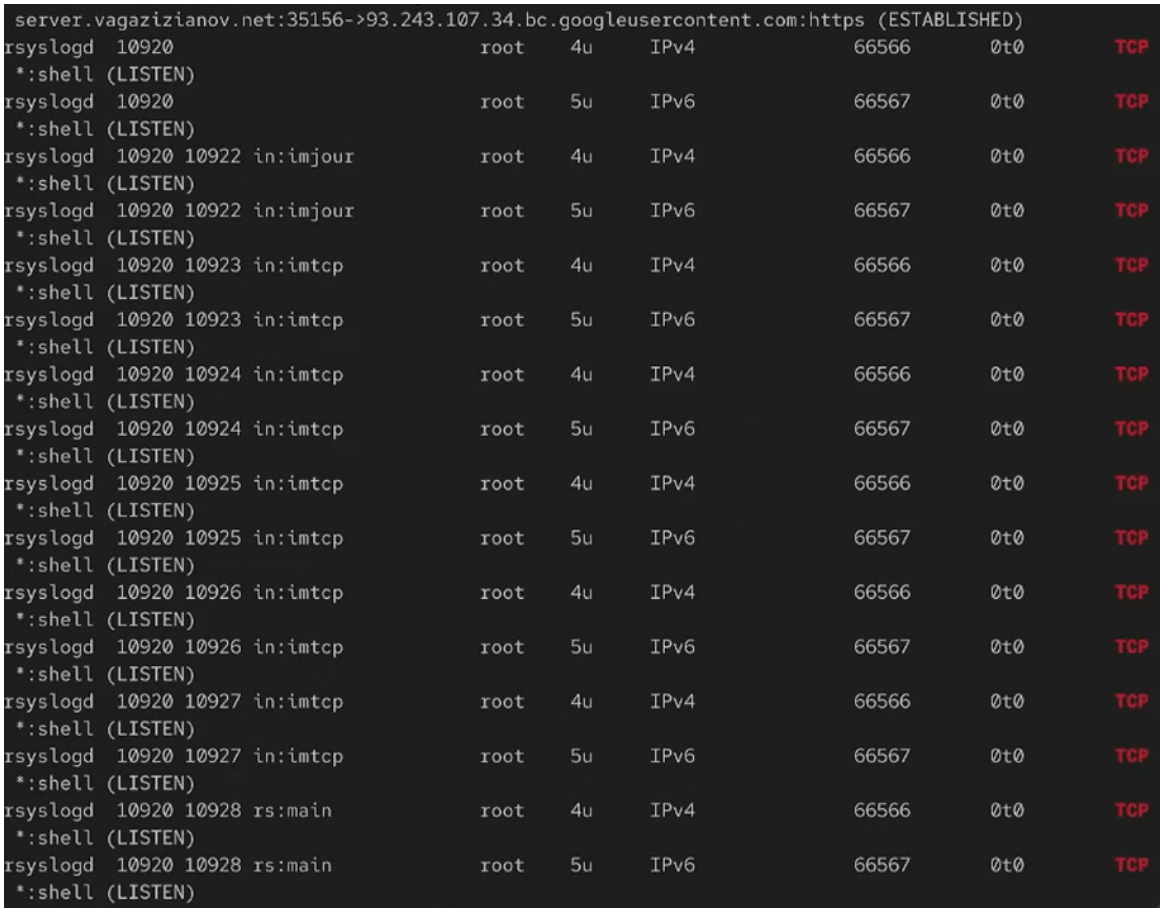

Рисунок 3.4: Проверка открытых портов rsyslog

3.1.5 Настройка межсетевого экрана

Настроены правила firewall для разрешения входящих соединений на TCP-порт 514. Добавлены как временные, так и постоянные правила для обеспечения сетевой безопасности.

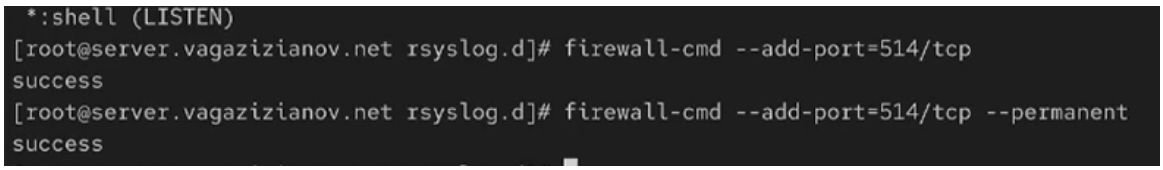

Рисунок 3.5: Настройка firewall для сетевого журналирования

3.2 Настройка клиента сетевого журнала

3.2.1 Подготовка клиентской конфигурации

На клиентской машине создан файл конфигурации netlog-client.conf в каталоге /etc/rsyslog.d/. Файл содержит настройки для перенаправления сообщений журнала.

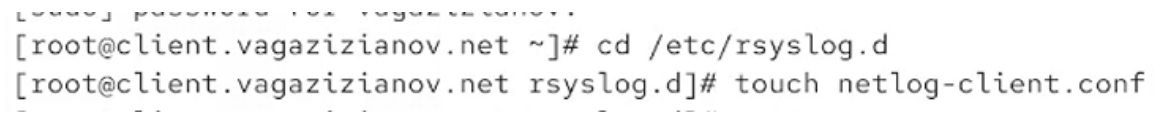

Рисунок 3.6: Создание конфигурационного файла клиента

3.2.2 Конфигурация перенаправления сообщений

В файл конфигурации добавлена директива для перенаправления всех системных сообщений (.) на сервер журналирования через TCP-порт 514 с использованием двойного символа @@ для TCP-соединения.

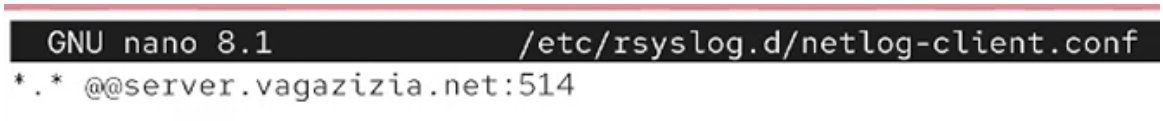

Рисунок 3.7: Настройка перенаправления логов на сервер

3.2.3 Перезапуск клиентской службы

Выполнен перезапуск службы rsyslog на клиенте для применения новой конфигурации. Проверен статус службы для подтверждения корректной работы.

```
[root@client.vagazizianov.net rsyslog.d]# systemctl restart rsyslog
```

Рисунок 3.8: Перезапуск rsyslog на клиенте

3.2.4 Проверка соединения

Проверена возможность установления TCP-соединения между клиентом и сервером журналирования. Убедились в доступности порта 514 на сервере.

3.3 Просмотр журналов событий

3.3.1 Мониторинг системных сообщений

На сервере выполнена проверка файла /var/log/messages с использованием команды tail -f для отслеживания поступающих сообщений в реальном времени. Проанализированы записи с различных хостов.

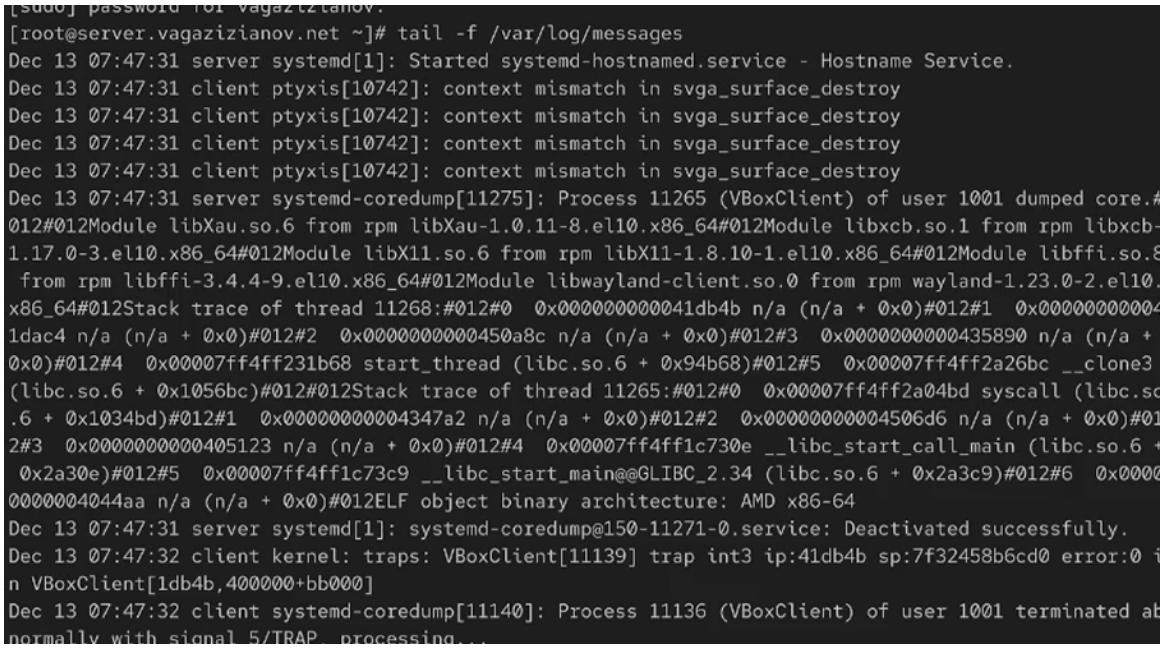

Рисунок 3.9: Мониторинг журнала сообщений в реальном времени

3.3.2 Использование графического монитора

Запущена графическая программа gnome-system-monitor для просмотра системных журналов. Проанализированы различные категории событий и сообщения от клиентских устройств.

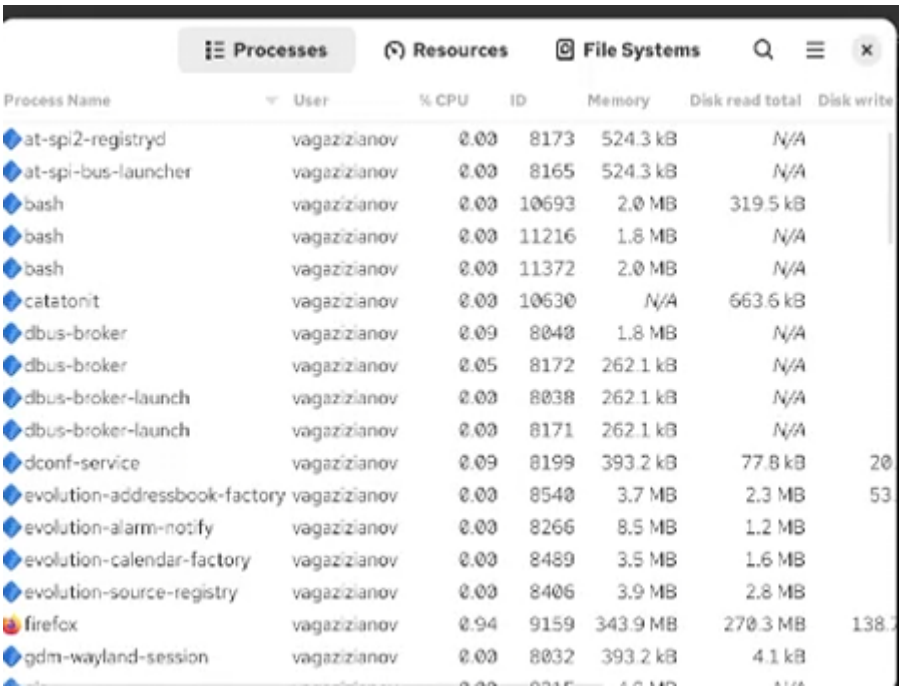

Рисунок 3.10: Просмотр журналов через gnome-system-monitor

3.3.3 Установка специализированного просмотрщика

Установлен просмотрщик журналов lnav, предоставляющий расширенные возможности для анализа и фильтрации системных сообщений.

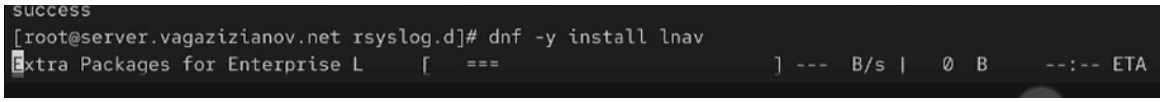

Рисунок 3.11: Установка просмотрщика журналов lnav

3.3.4 Анализ журналов через lnav

Запущен lnav для просмотра и анализа журналов. Использованы возможности цветового выделения, фильтрации и поиска для эффективной работы с большими объёмами логов.

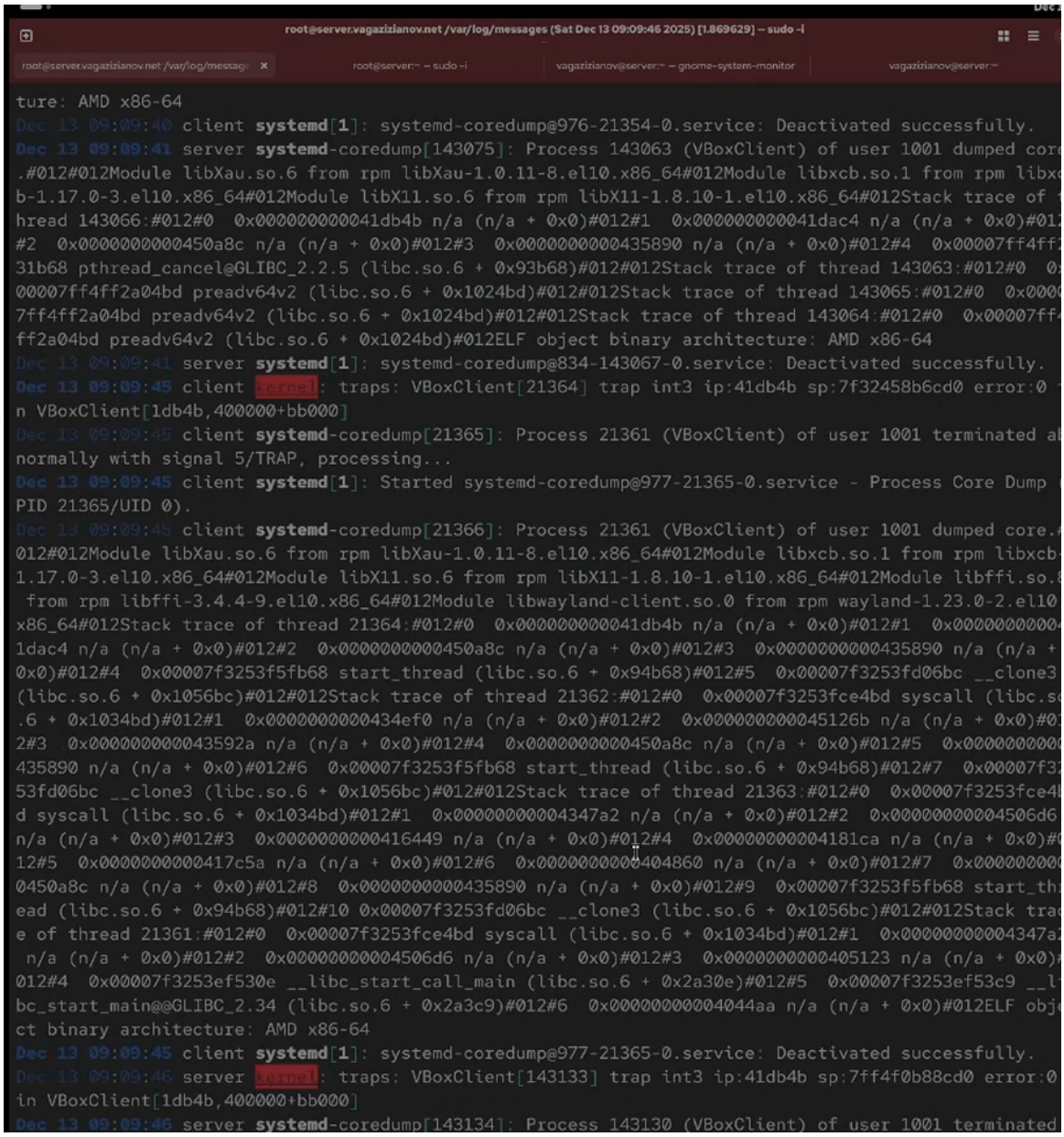

Рисунок 3.12: Анализ журналов с помощью lnav

3.3.5 Диагностика системных проблем

Проанализированы сообщения о некорректной работе сервисов. Выявлены и исправлены ошибки в настройках соответствующих служб на основе информации из журналов.

3.4 Автоматизация развертывания

3.4.1 Разработка скриптов provisioning

Созданы исполняемые скрипты для автоматической настройки сервера и клиента системы сетевого журналирования. Скрипты включают копирование конфигурационных файлов и настройку служб.

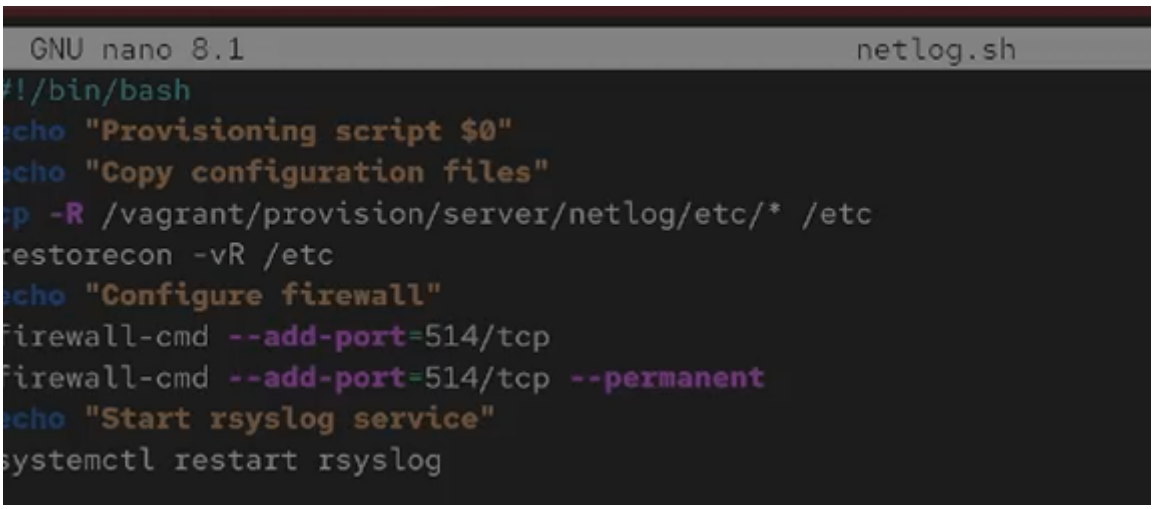

Рисунок 3.13: Скрипт настройки сервера журналирования

3.4.2 Организация конфигурационных файлов

Создана структура каталогов для хранения конфигурационных файлов сервера и клиента. Выполнено копирование рабочих конфигураций в соответствующие директории.

3.4.3 Интеграция с Vagrant

Настроены секции provisioning в конфигурационном файле Vagrant для автоматического выполнения скриптов при развертывании виртуальных машин.

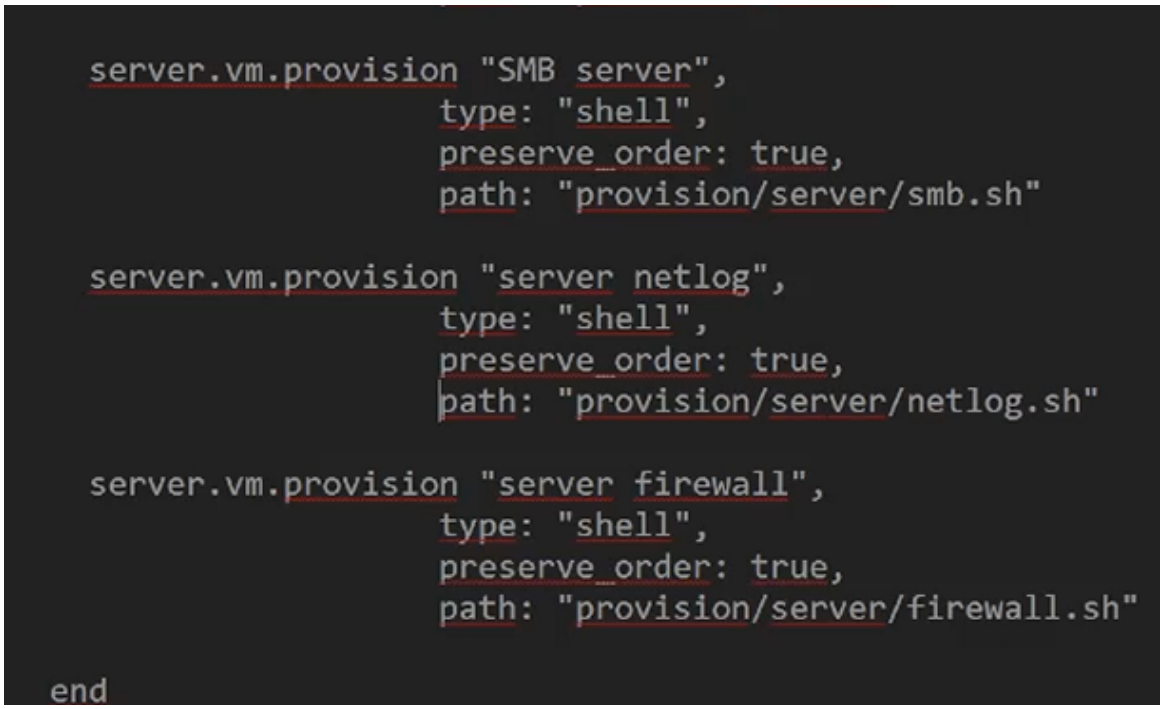

Рисунок 3.14: Конфигурация Vagrantfile для журналирования

3.4.4 Тестирование работы автоматизации

Протестирована работа скриптов автоматизации при создании виртуальных машин. Проверена корректность настройки всех компонентов системы журналирования.

3.4.5 Проверка передачи журналов

Проверена передача сообщений от клиента на сервер журналирования. Убедились в корректной записи клиентских логов в централизованное хранилище.

4 Контрольные вопросы

1. **Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?**
   Модуль imjournal используется для приёма сообщений от journald.

2. **Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?**
   Устаревший модуль - imuxsock.

3. **Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?**
   Следует использовать параметр RateLimit.Interval=0 в конфигурации imjournal.

4. **В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?**
   Настройки содержатся в файле /etc/systemd/journald.conf.

5. **Каким параметром управляется пересылка сообщений из journald в rsyslog?**
   Параметром ForwardToSyslog в файле /etc/systemd/journald.conf.

6. **Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?**
   Модуль imfile позволяет читать сообщения из произвольных файлов.

7. **Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?**

   Модуль ommysql используется для пересылки сообщений в базу данных MariaDB.

8. **Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?**

   $ModLoad imtcp и $InputTCPServerRun 514.

9. **Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?**

   Использовать команды: firewall-cmd –add-port=514/tcp и firewall-cmd –add-port=514/tcp –permanent.

5 Выводы

- Освоены практические навыки настройки сервера сетевого журналирования с использованием rsyslog
- Приобретён опыт конфигурации клиентских устройств для передачи системных сообщений в централизованное хранилище
- Изучены различные инструменты для просмотра и анализа журналов системных событий
- Освоены методы диагностики системных проблем на основе информации из журналов
- Получены навыки настройки сетевой безопасности для системы журналирования
- Разработана система автоматизации развертывания инфраструктуры сетевого журналирования
- Изучены особенности работы с различными форматами журналов и инструментами их анализа
- Приобретён опыт настройки мониторинга системных событий в распределённой сетевой среде