Отчёт по лабораторной работе 7

Управление журналами событий в системе

Вишняков Родион Сергеевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

Получаем полномочия администратора

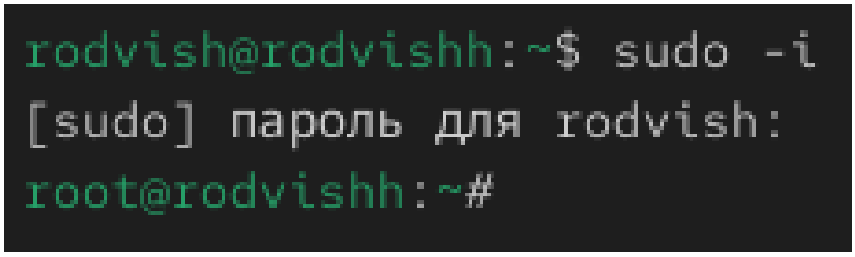

Рис. 2.1: root

Запускаю мониторинг системных событий в реальном времени

Рис. 2.2: Мониторинг системных событий

Ввожу предоставленные команды

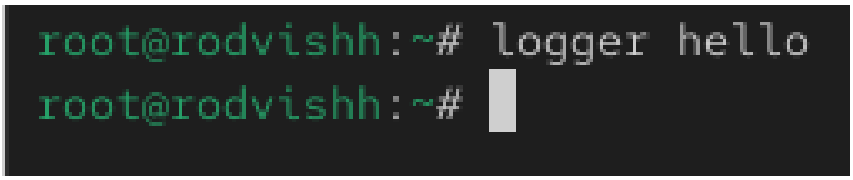

Рис. 2.3: Ввод команд

Получаю сообщение из мониторинга событий

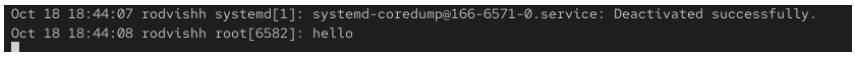

Рис. 2.4: Мониторинг системных событий

Просматриваю последний 20 строк из мониторинга сообщений безопасности

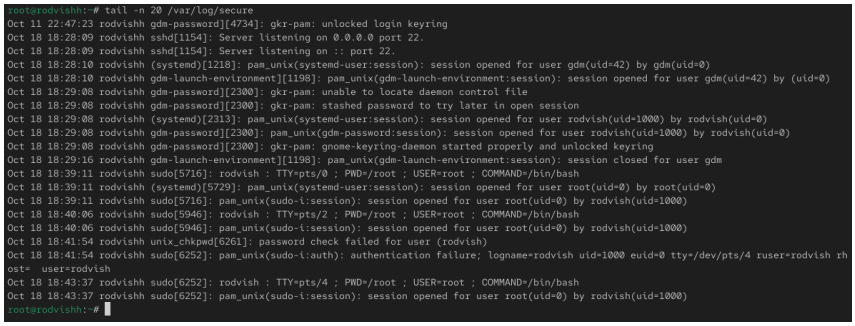

Рис. 2.5: Мониторинг сообщений безопасности

Устанавливаю Apache

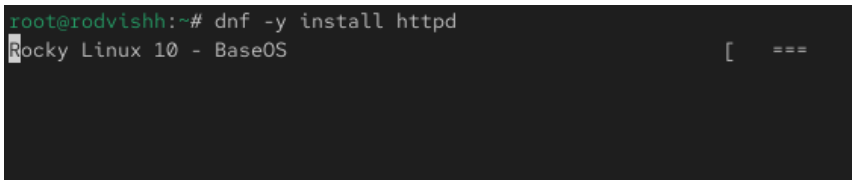

Рис. 2.6: Apache

Запускаю веб-службу

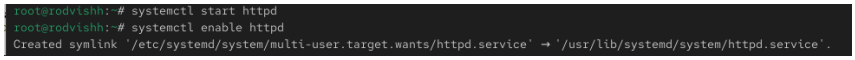

Рис. 2.7: Запуск веб-службы

Просматриваю журнал сообщений об ошибках веб-службы

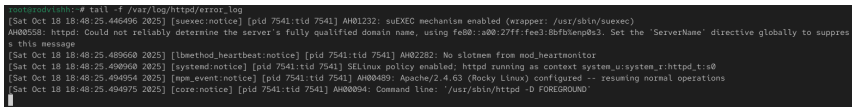

Рис. 2.8: Сообщения об ошибках

Добавляю предоставленную строку в конец

Рис. 2.9: Добавление строки

Создаю файл мониторинга событий веб-службы и прописываю в нем следующую команду

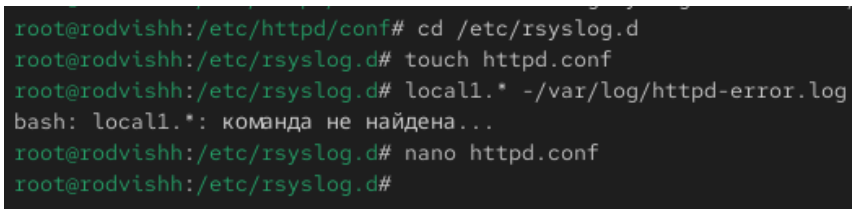

Рис. 2.10: Файл мониторинга

Перезагружаю конфигурацию rsyslogd и веб-службу

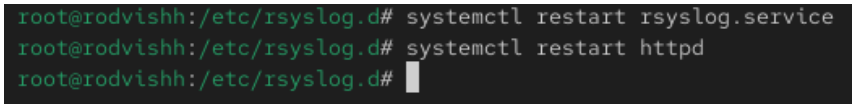

Рис. 2.11: Перезагрузка

Создаю файл конфигурации для мониторинга отладочной информации и ввожу следующую команду

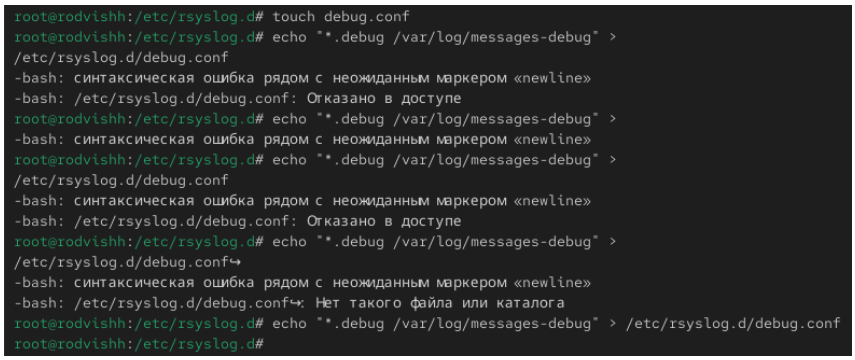

Рис. 2.12: Файл конфигурации

Перезапускаю rsyslogd

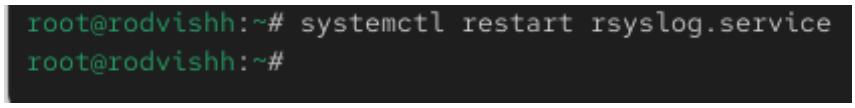

Рис. 2.13: Перезапуск rsyslogd

Запускаю мониторинг отладочной информации

Рис. 2.14: Мониторинг отладочной информации

Ввожу предоставленную команду

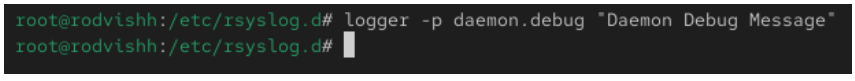

Рис. 2.15: Ввод команды

Просматриваю содержимое журнала с событиями с момента последнего запуска системы

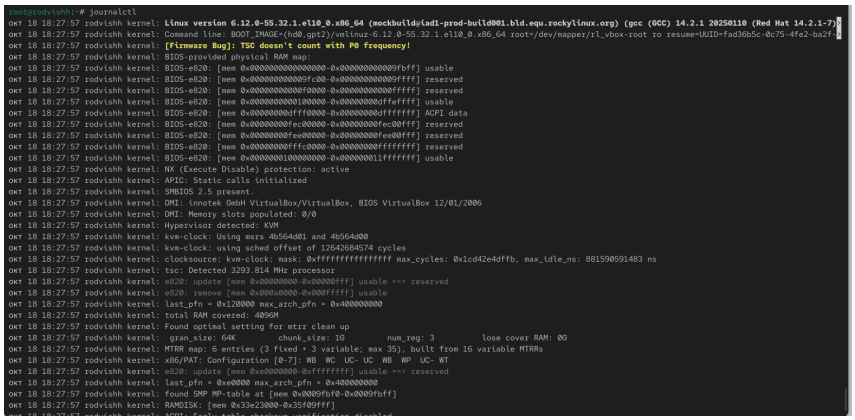

Рис. 2.16: Содержимое журнала

Просматриваю содержимое журнала без использования пейджера

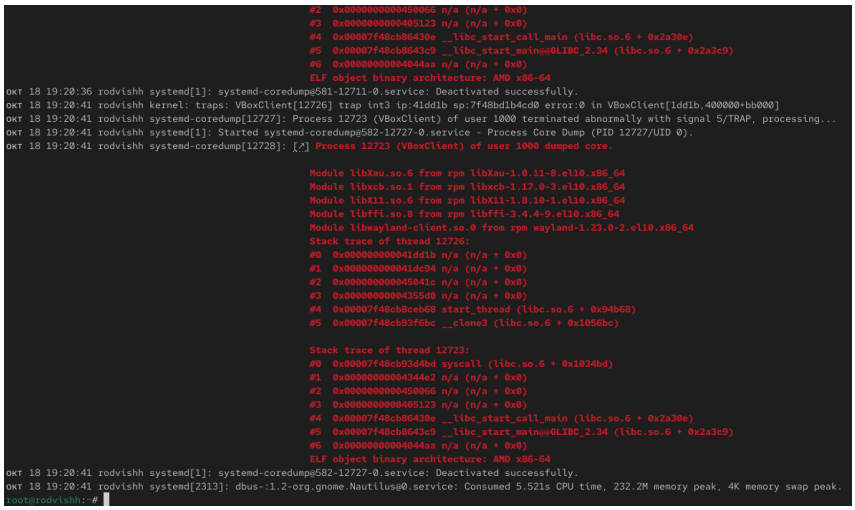

Рис. 2.17: Содержимое журнала

Просматриваю содержимое в реальном времени

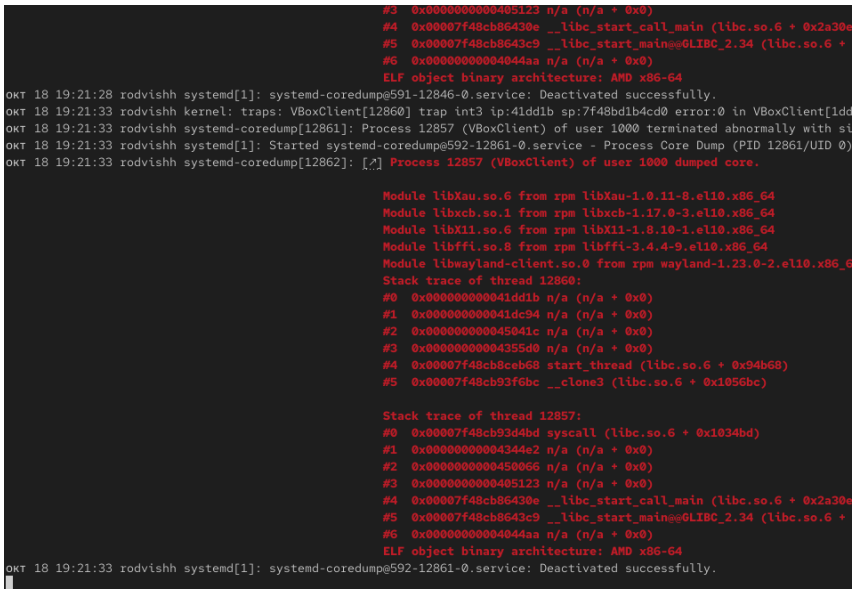

Рис. 2.18: Содержимое журнала

Просматриваю конкретные параметры

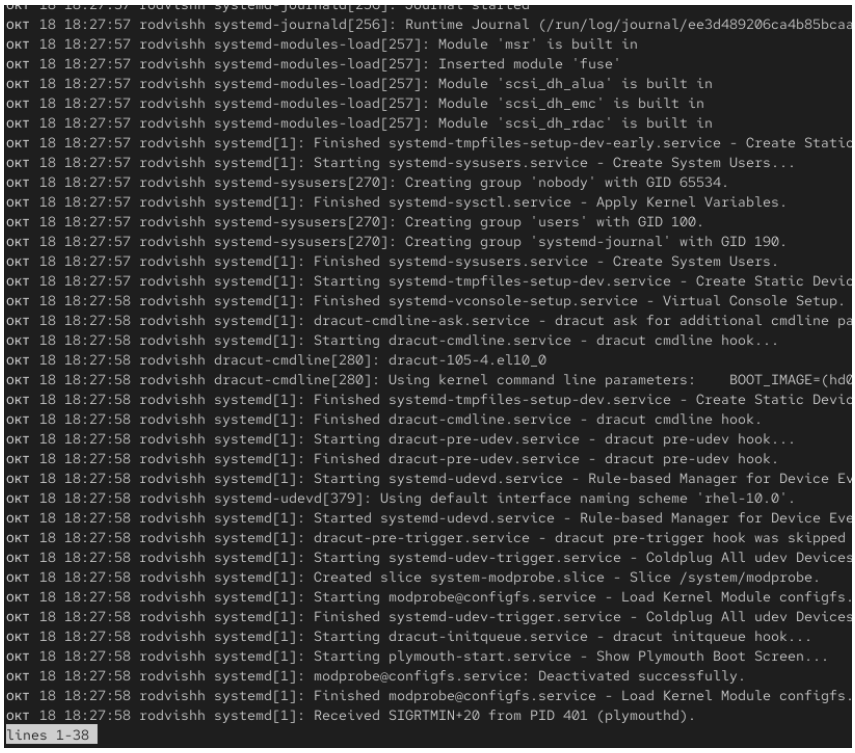

Рис. 2.19: Содержимое журнала

Просматриваю события для UIDO

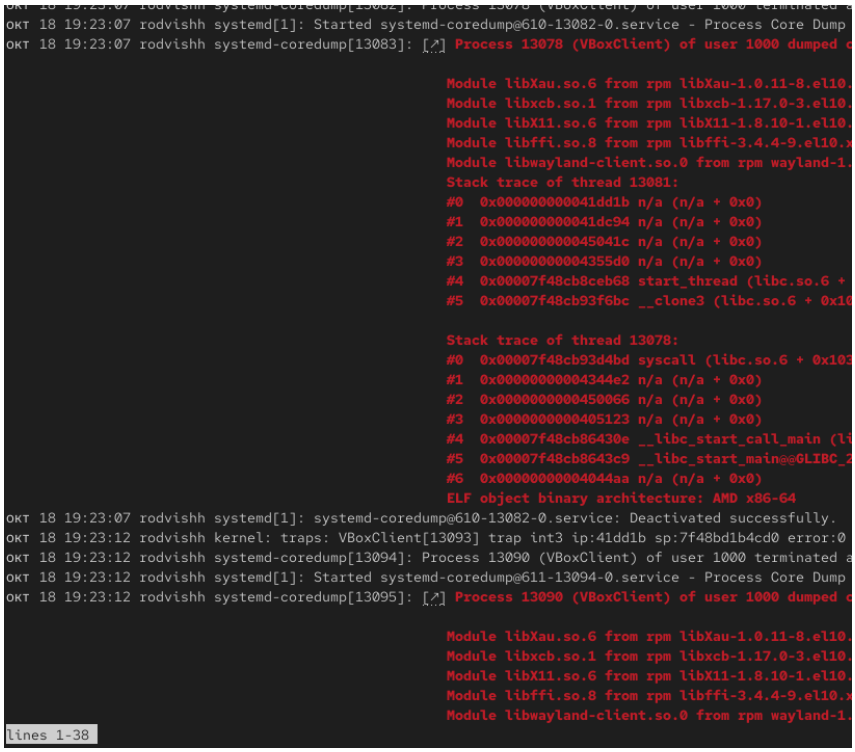

Рис. 2.20: Просмотр событий для UIDO

Просматриваю последний 20 строк журнала

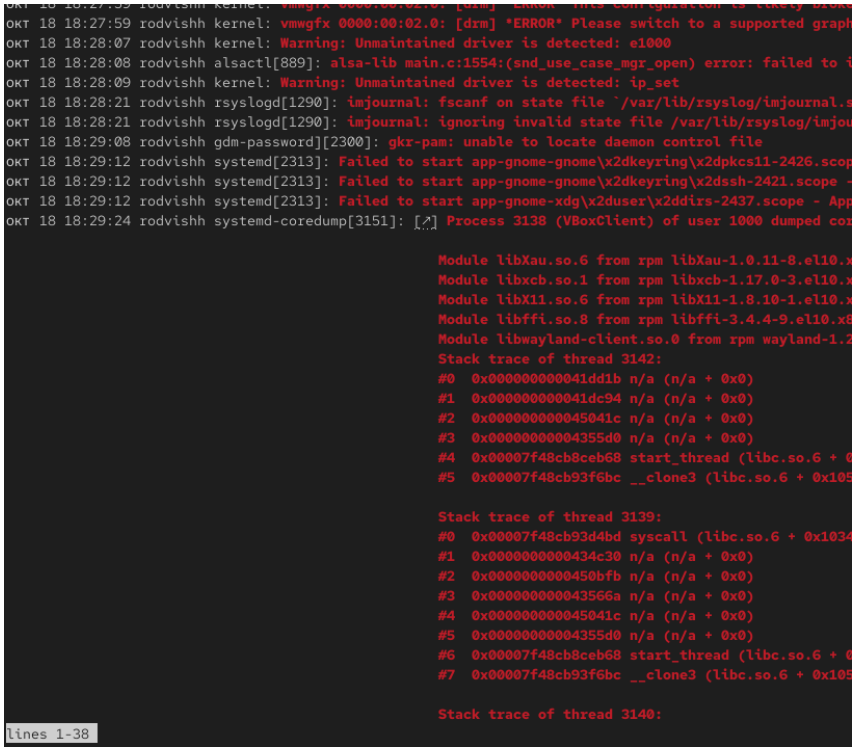

Рис. 2.21: Содержимое журнала

Просматриваю только сообщения об ошибках

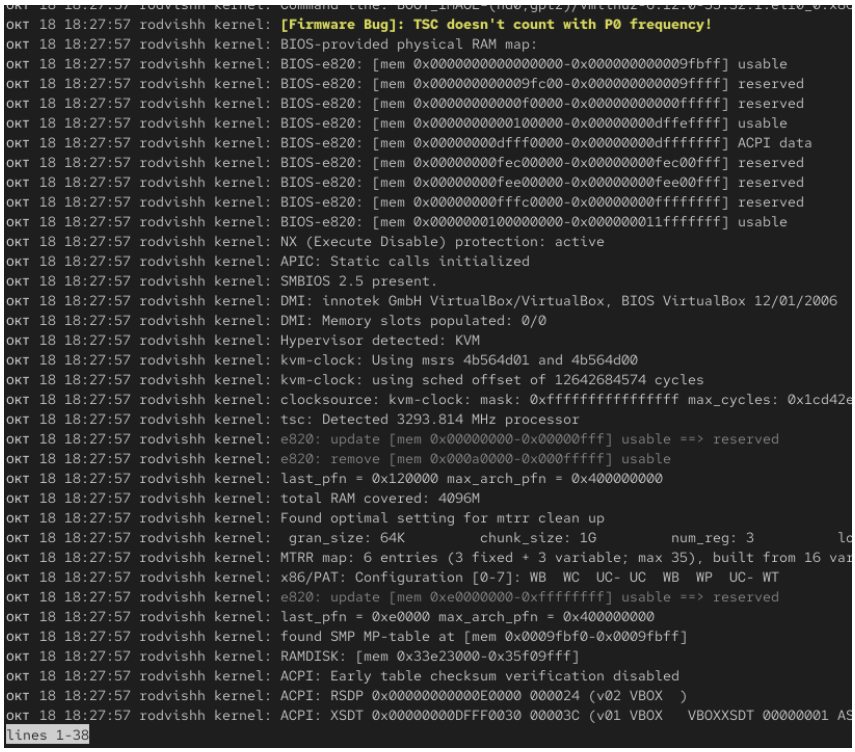

Рис. 2.22: Содержимое журнала

Просматриваю все сообщения вчерашнего дня

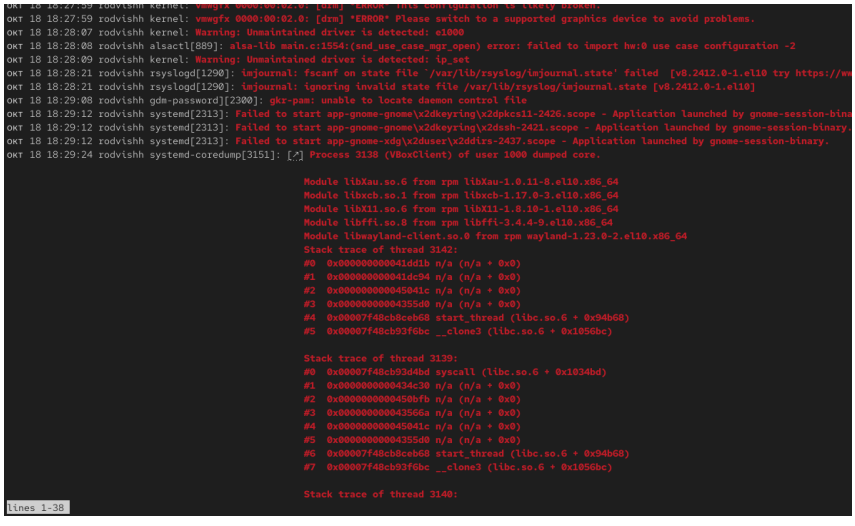

Рис. 2.23: Содержимое журнала

Просматриваю сообщения с ошибкой приоритета со вчерашнего дня

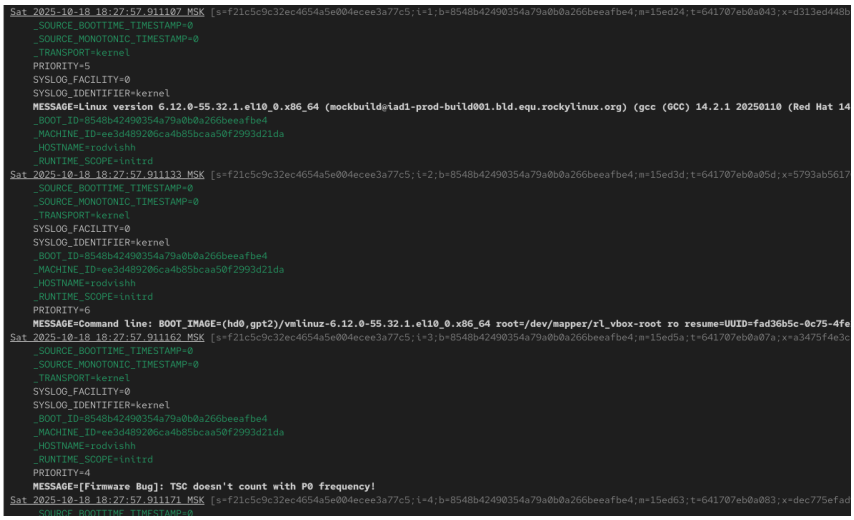

Рис. 2.24: Содержимое журнала

Просматриваю дополнительную информацию о модуле sshd

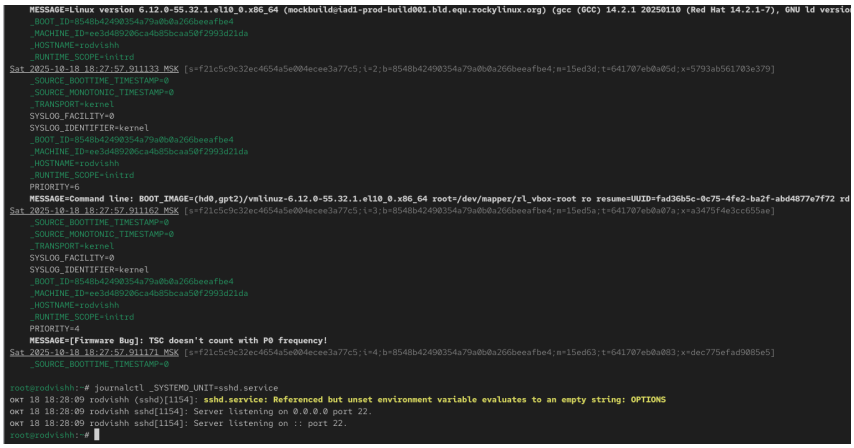

Рис. 2.25: Содержимое журнала

Создаю каталог для хранения записей журнала

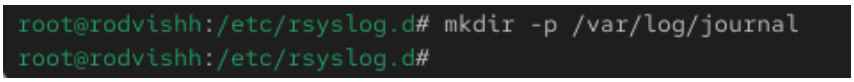

Рис. 2.26: Создание каталога

Корректирую права доступа

```
root@rodvishh:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal
root@rodvishh:/etc/rsyslog.d# chmod 2755 /var/log/journal
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.27: Права доступа

Для принятия изменений ввожу следующую команду

```
root@rodvishh:/etc/rsyslog.d# killall -USR1 systemd-journald
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.28: Принятие изменений

3 Вывод

Мы получили навыки работы с журналами мониторинга различных событий в системе.

4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd? `/etc/rsyslog.conf`
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? `/var/log/auth.log` (в Red Hat-системах — `/var/log/secure`)
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов? Еженедельно
4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info? `*.info /var/log/messages.info`
5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени? `tail -f` для файлов журналов или `journalctl -f` для systemd
6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00? `journalctl _PID=1 --since="09:00" --until="15:00"`
7. Какая команда позволяет вас видеть сообщения journald после последней перезагрузки системы? `journalctl -b`
8. Какая процедура позволяет сделать журнал journald постоянным? Создать директорию `/var/log/journal` и перезапустить systemd-journald