Лабораторная работа №7

Управление журналами событий в системе

Комягин Андрей Николаевич

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

## 2.1 Мониторинг журнала системных событий в реальном времени

Запустим мониторинг системных событий в реальном времени:(рис. 1).

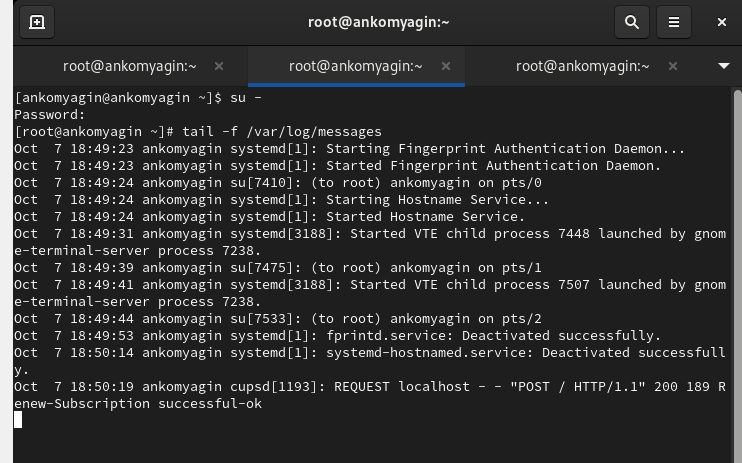


Рис. 1: Запустим мониторинг событий

Попробуем получить полномочия администратора, но введём неправильный пароль. Обратим внимание, что во второй вкладке терминала с мониторингом событий появится сообщение **«FAILED SU (to root)** (рис. 2).

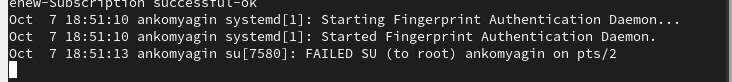


Рис. 2: отображение ошибки в мониторинге

В третьей вкладке терминала из оболочки пользователя введём **logger hello** Во второй вкладке терминала с мониторингом событий мы увидим сообщение(рис. 3).

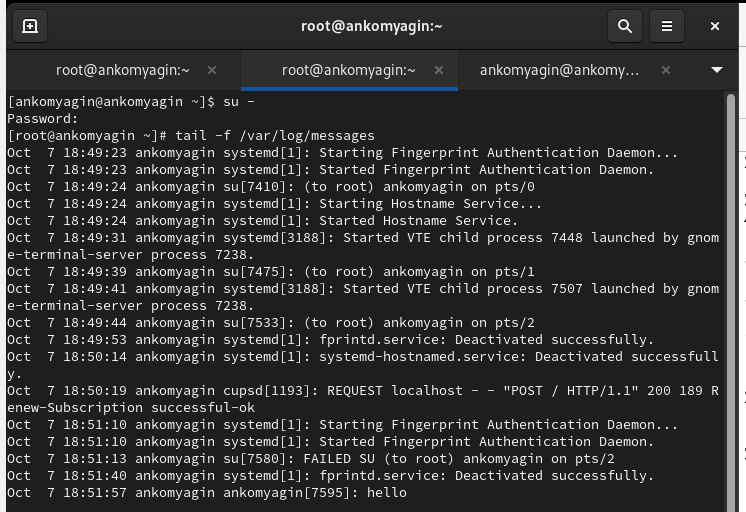


Рис. 3: logger hello

Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов(рис. 4).

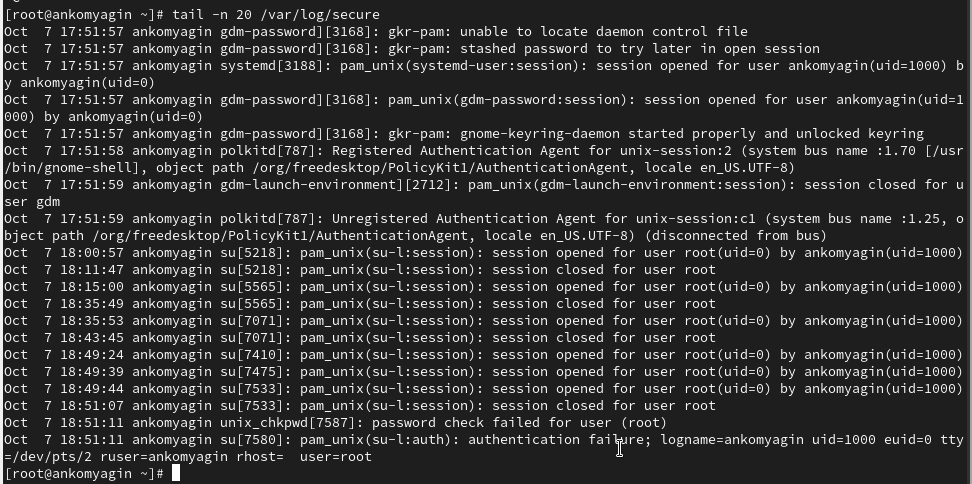


Рис. 4: мониторинг сообщений безопасности

## 2.2 Изменение правил rsyslog.conf

Установим Apache, запустим веб-службу (рис. 5).

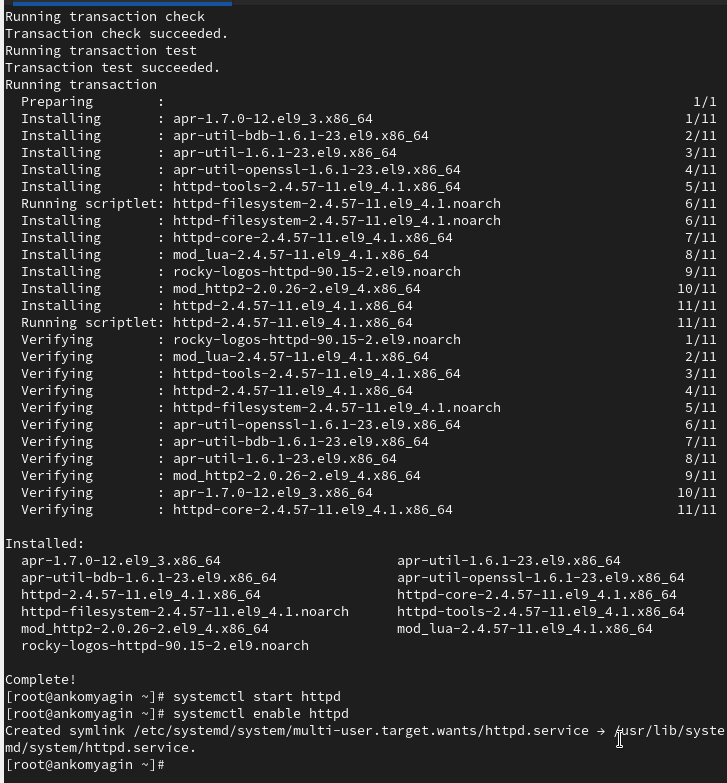


Рис. 5: Установка Apache и запуск веб-службы

Посмотрим журнал сообщений об ошибках веб-службы(рис. 6)

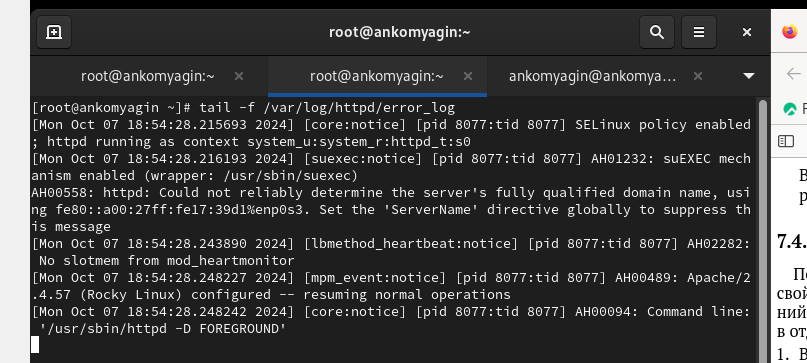


Рис. 6: журнал ошибок веб-службы

В файле конфигурации /etc/httpd/conf/httpd.conf в конце добавим строку(рис. 7)

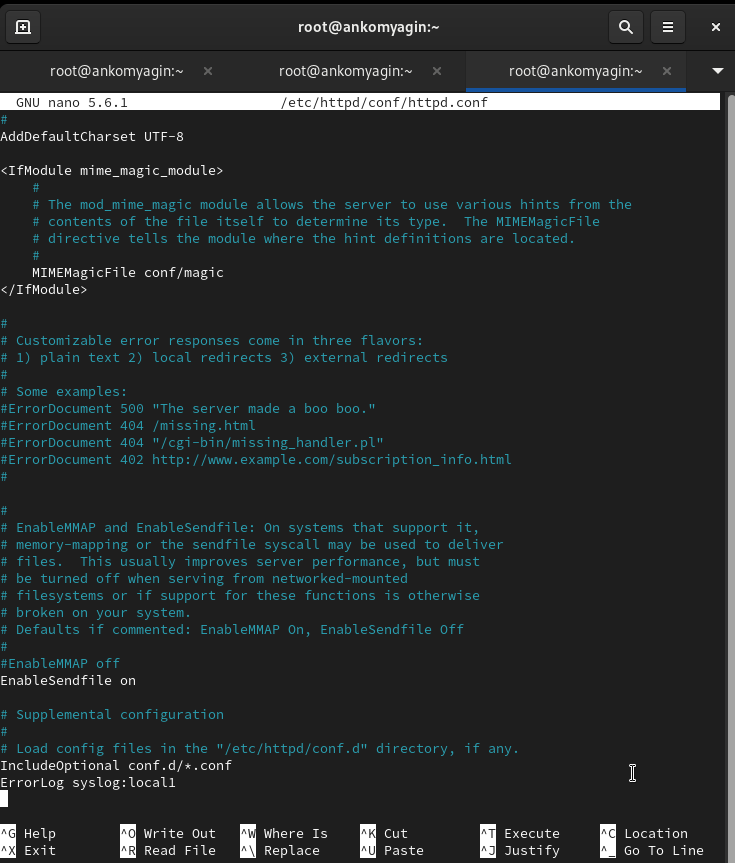


Рис. 7: /etc/httpd/conf/httpd.conf

В каталоге /etc/rsyslog.d создадим файл мониторинга событий веб-службы, открыв его на редактирование, пропишем в нём local1.\* -/var/log/httpd-error.log (рис. 8).

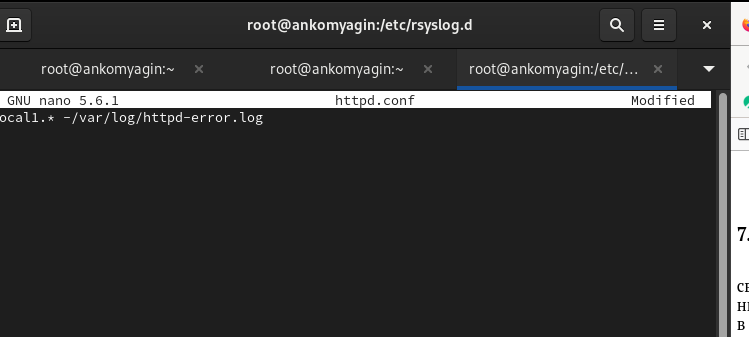


Рис. 8: файл мониторинга

перезагрузим конфигурацию rsyslogd и веб-службу (рис. 9)

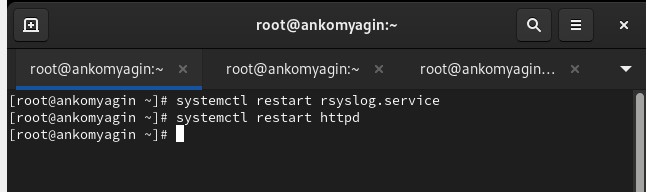


Рис. 9: перезагрузка конфигураций

Создадим отдельный файл конфигурации для мониторинга отладочной информации(рис. 10)

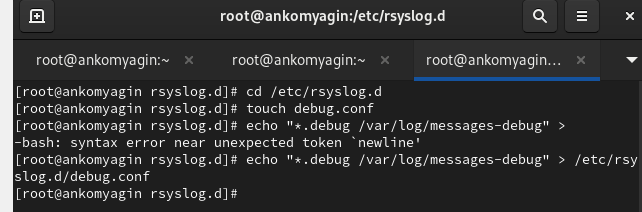


Рис. 10: Мониторинг отладки

Запустим мониторинг отладочной информации(рис. 11)

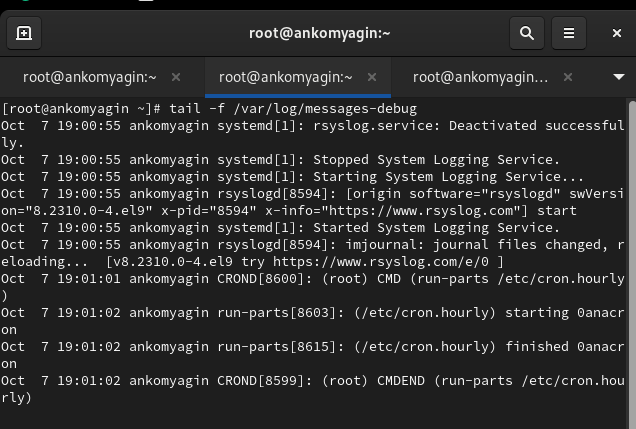


Рис. 11: мониторинг

## 2.3 Использование journalctl

Посмотрим содержимое журнала с событиями с момента последнего запуска системы (рис. 12)

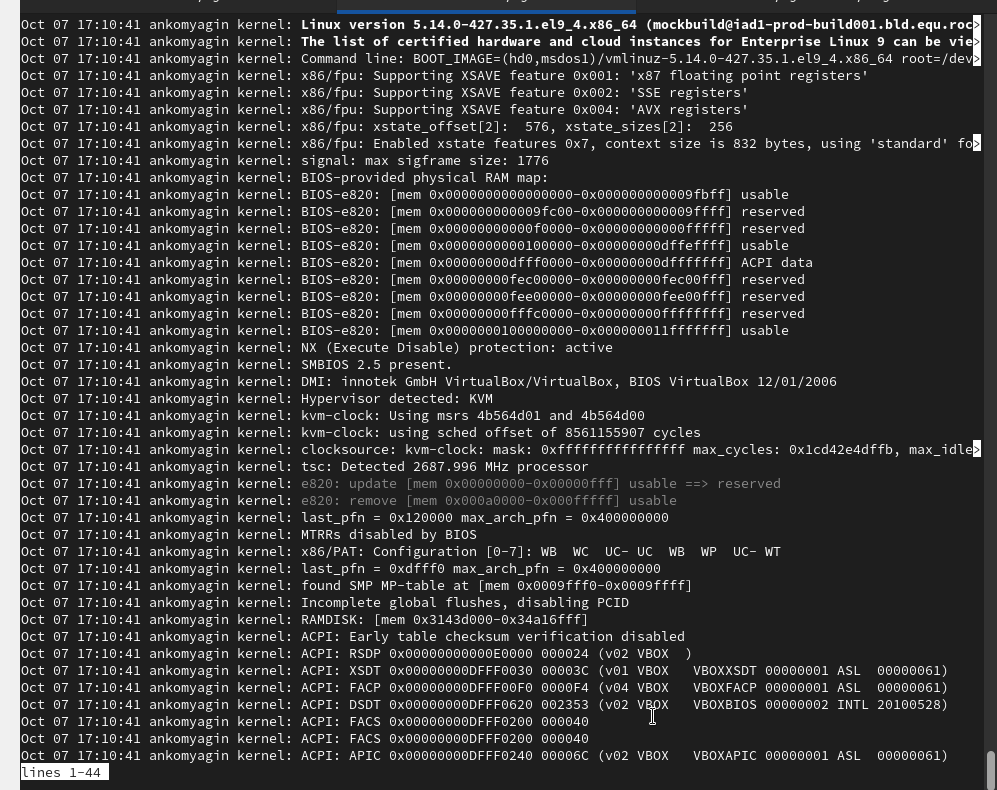


Рис. 12: содержимое журнала событий

Режим просмотра журнала в реальном времени(рис. 13)

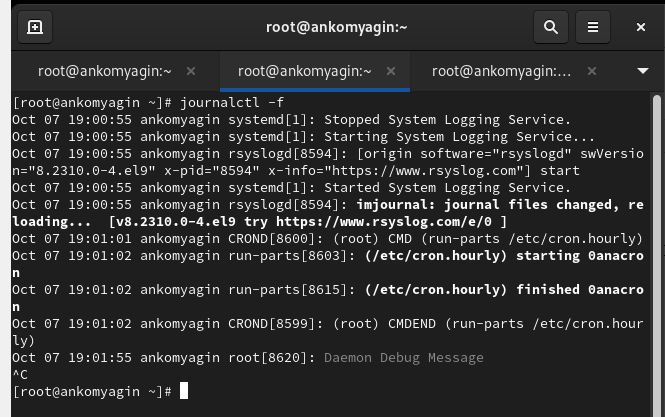


Рис. 13: реальное время

Отобрахим последние 20 строк журнала(рис. 14)

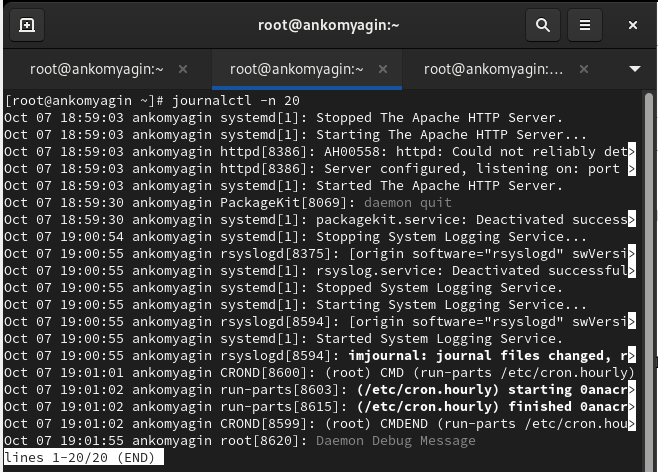


Рис. 14: последние строки журнала

Просмотрим только сообщения об ошибках(рис. 15)

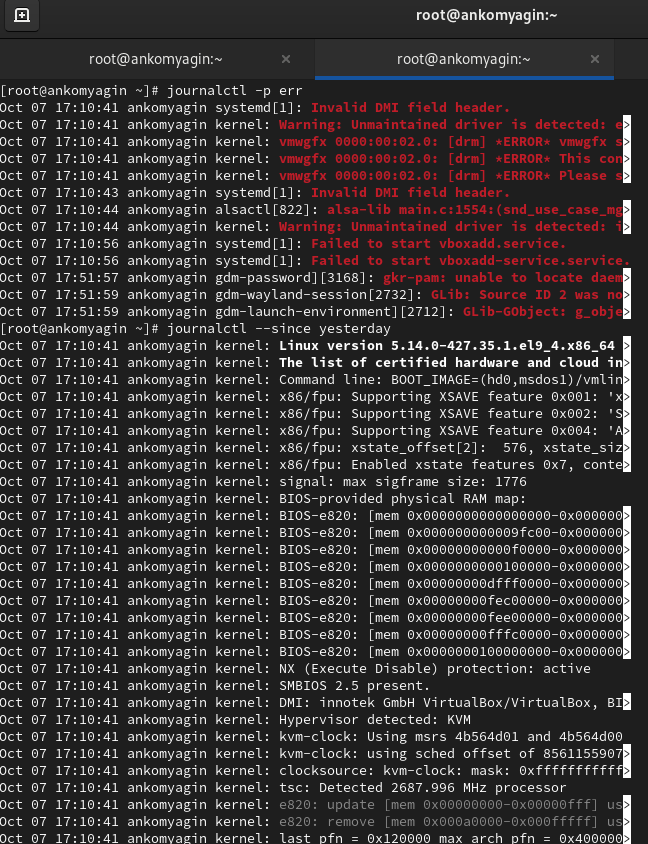


Рис. 15: сообщения об ошибках

Для просмотра всех сообщений со вчерашнего дня введём **journalctl –since yesterday**(рис. 16).

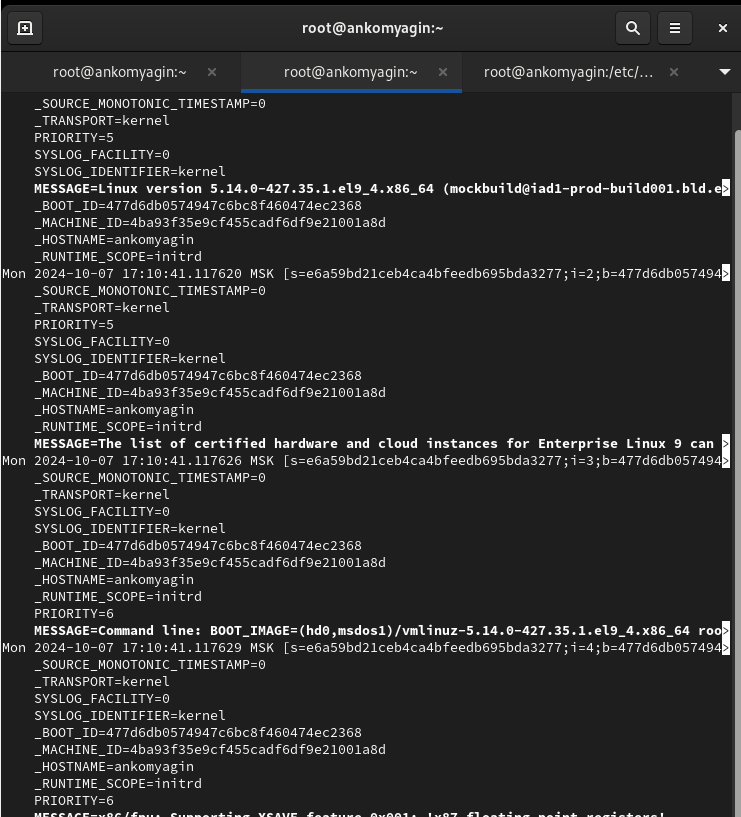


Рис. 16: сообщения со вчерашнего дня

Просмотрим дополнительную информацию о модуле sshd(рис. 17).

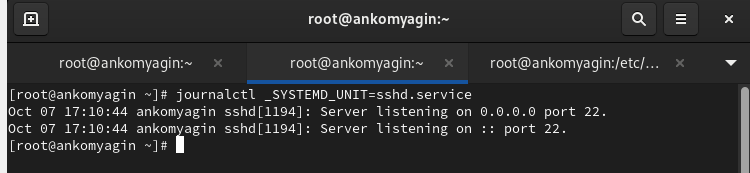


Рис. 17: доп информация о sshd

## 2.4 Постоянный журнал journald

Создадим каталог для хранения записей журнала. Скорректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Журнал systemd теперь постоянный (рис. 18).

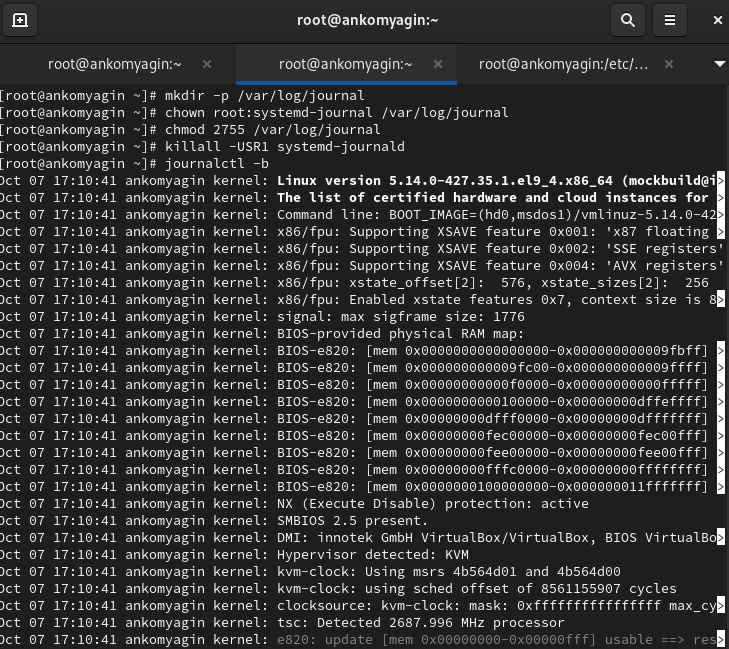


Рис. 18: доп информация о sshd

# 3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?
   * Основной файл конфигурации для rsyslogd — это /etc/rsyslog.conf.
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?
   * Сообщения, связанные с аутентификацией, обычно записываются в файл /var/log/auth.log (или /var/log/secure в некоторых дистрибутивах).
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?
   * По умолчанию ротация файлов журналов происходит раз в неделю (это может варьироваться в зависимости от конфигурации системы и используемого инструмента ротации, например, logrotate).
4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?
   * Добавим строку: \*.info /var/log/messages.info.
5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?
   * Команда tail -f /var/log/syslog (или другой соответствующий файл журнала).
6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?
   * Используем команду: journalctl \_PID=1 –since “YYYY-MM-DD 09:00” –until “YYYY-MM-DD 15:00” (замените YYYY-MM-DD на нужную дату).
7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?
   * Команда: journalctl -b.
8. Какая процедура позволяет сделать журнал journald постоянным?
   * Чтобы сделать журнал journald постоянным, нужно отредактировать файл конфигурации /etc/systemd/journald.conf и установить параметр Storage=persistent. Затем перезапустите службу journald с помощью команды systemctl restart systemd-journald.

# 4 Вывод

В ходе выполнения лабораторной работы я получил навыки работы с журналами мониторинга различных событий в системе.

# Список литературы

[Туис, курс Администрирование операционных систем](https://esystem.rudn.ru/course/view.php?id=5946)