Отчёт по лабораторной работе №7

Управление журналами событий в системе

Агджабекова Эся Рустамовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Ход выполнения работы

2.1 Мониторинг журнала системных событий в реальном времени

1. В трёх вкладках терминала получены полномочия администратора командой `su -`.

2. Во второй вкладке запущен мониторинг системных событий в реальном времени:
   tail -f /var/log/messages
   (см. рис. fig. 2.1).

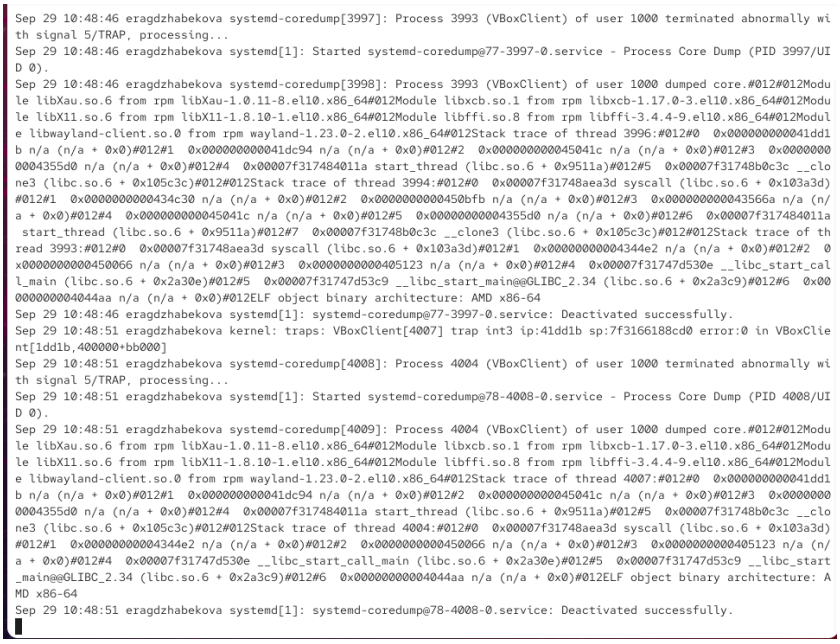

Рис. 2.1: Мониторинг системных событий в реальном времени

3. В третьей вкладке выполнена попытка получить права администратора с неверным паролем. В результате в журнале зафиксирована ошибка авторизации `FAILED su (to root)` (см. рис. fig. 2.2).

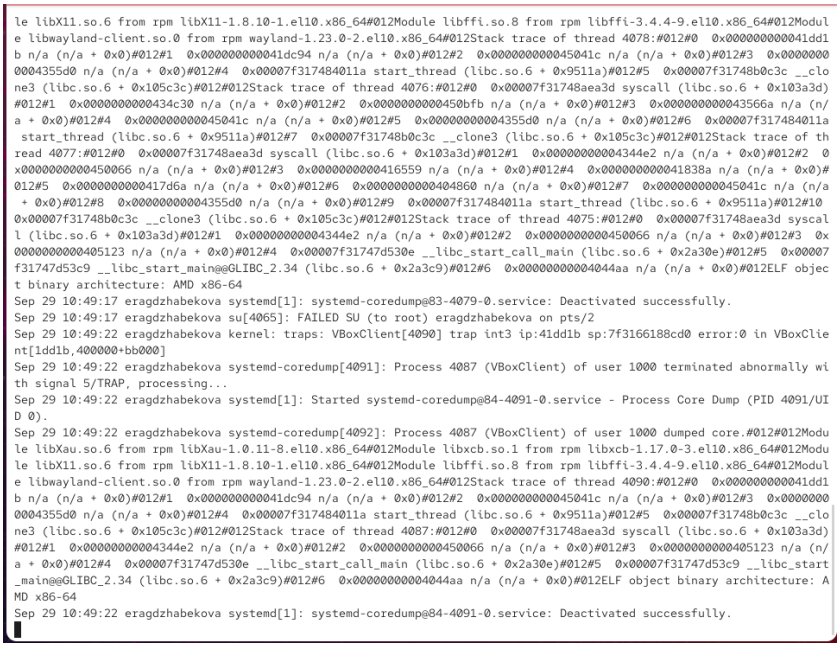

Рис. 2.2: Ошибка при вводе неправильного пароля

4. В оболочке пользователя выполнена команда:

   logger hello

   Сообщение появилось в окне мониторинга и было сохранено в журнале `/var/log/messages` (см. рис. fig. 2.3).

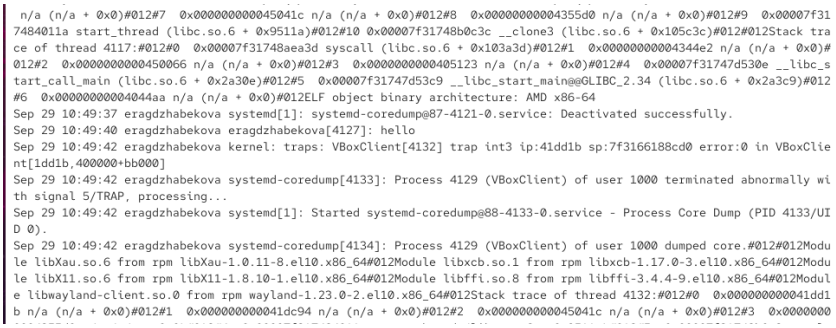

Рис. 2.3: Сообщение, записанное с помощью logger

5. Мониторинг системных сообщений во второй вкладке остановлен комбинацией `Ctrl + C`. Затем просмотрены последние 20 строк файла журнала безопасности командой:

   tail -n 20 /var/log/secure

   В нём отобразились записи о неудачной попытке авторизации (см. рис. fig. 2.4).

Рис. 2.4: Просмотр сообщений безопасности

2.2 Изменение правил rsyslog.conf

1. Установлен Apache (если ранее не был установлен) и запущена веб-служба:
   dnf -y install httpd
   systemctl start httpd
   systemctl enable httpd
   (см. рис. fig. 2.5).

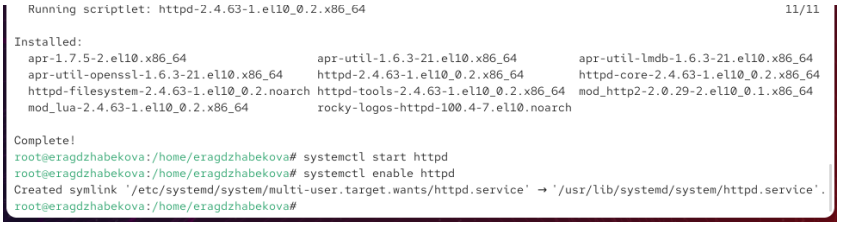

Рис. 2.5: Установка и запуск Apache

2. Во второй вкладке терминала просмотрен журнал ошибок веб-службы командой

tail -f /var/log/httpd/error_log

(см. рис. fig. 2.6).

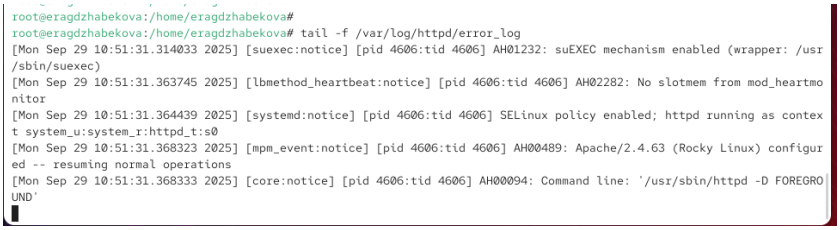

Рис. 2.6: Просмотр журнала ошибок Apache

3. В файле `/etc/httpd/conf/httpd.conf` добавлена строка перенаправления ошибок в syslog:

   ErrorLog syslog:local1

   (см. рис. fig. 2.7).

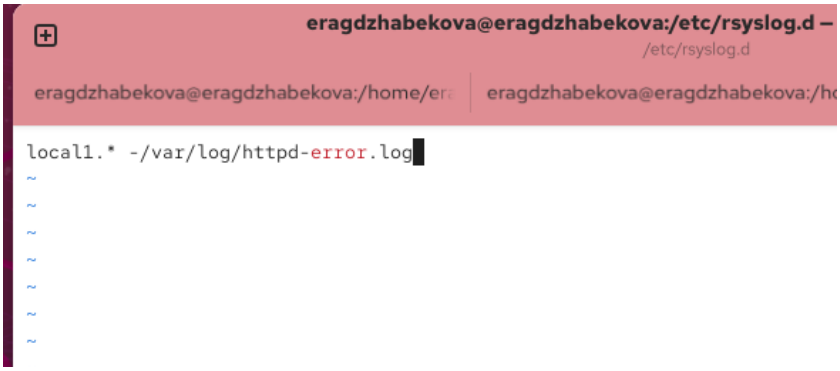

Рис. 2.7: Добавление правила ErrorLog в httpd.conf

4. В каталоге `/etc/rsyslog.d` создан файл `httpd.conf` со строкой:

   local1.* -/var/log/httpd-error.log

   (см. рис. fig. 2.8).

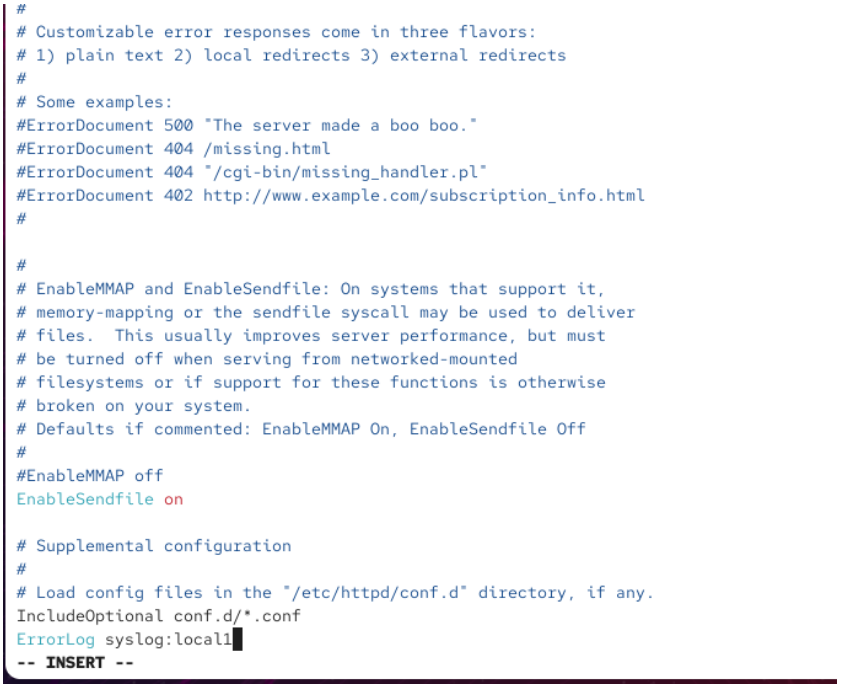

Рис. 2.8: Создание файла конфигурации для ошибок Apache

5. Перезагружены службы `rsyslog` и `httpd`. Сообщения об ошибках веб-сервера начали записываться в `/var/log/httpd-error.log`.

6. Создан файл `/etc/rsyslog.d/debug.conf` с правилом:
   *.debug /var/log/messages-debug
   (см. рис. fig. 2.9).

Рис. 2.9: Создание конфигурации для отладочных сообщений

7. После перезапуска `rsyslog` запущен мониторинг нового файла:
   tail -f /var/log/messages-debug

8. С помощью команды
   logger -p daemon.debug “Daemon Debug Message”
   в журнал отправлено тестовое сообщение, которое успешно отобразилось в логе (см. рис. fig. 2.10).

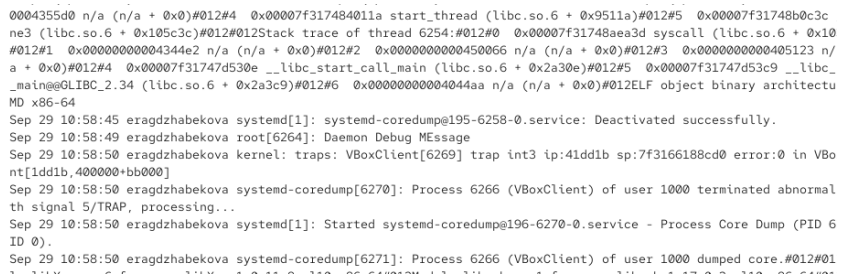

Рис. 2.10: Вывод отладочного сообщения через logger

2.3 Использование journalctl

1. Просмотрен журнал событий с момента последнего запуска системы командой
   journalctl
   (см. рис. fig. 2.11).

Рис. 2.11: Просмотр журнала с момента запуска

2. Выведено содержимое журнала без использования пейджера:
   journalctl –no-pager
   (см. рис. fig. 2.12).

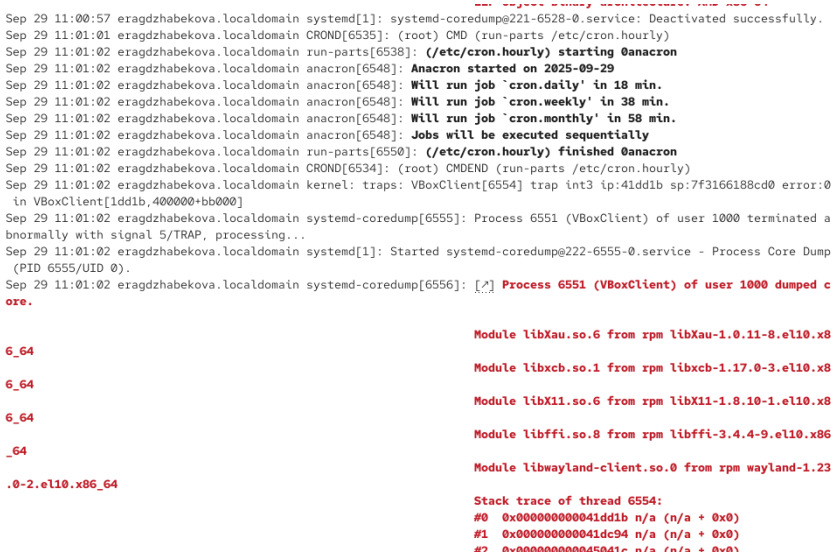

Рис. 2.12: Вывод журнала без пейджера

3. Включён режим просмотра журнала в реальном времени:

   journalctl -f

   Для выхода использована комбинация `Ctrl + C` (см. рис. fig. 2.13).

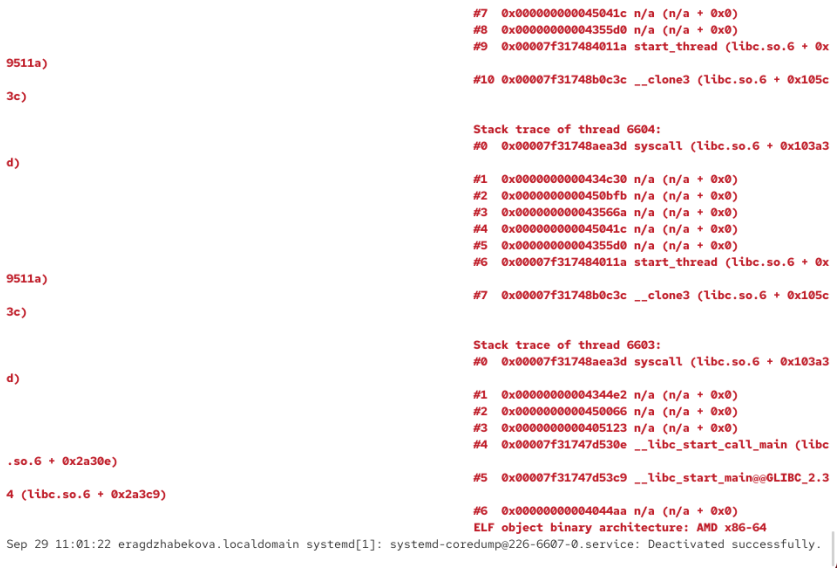

Рис. 2.13: Просмотр журнала в реальном времени

4. Для изучения доступных параметров фильтрации к команде journalctl была добавлена двойная клавиша Tab. Отобразился список поддерживаемых ключей (см. рис. fig. 2.14).

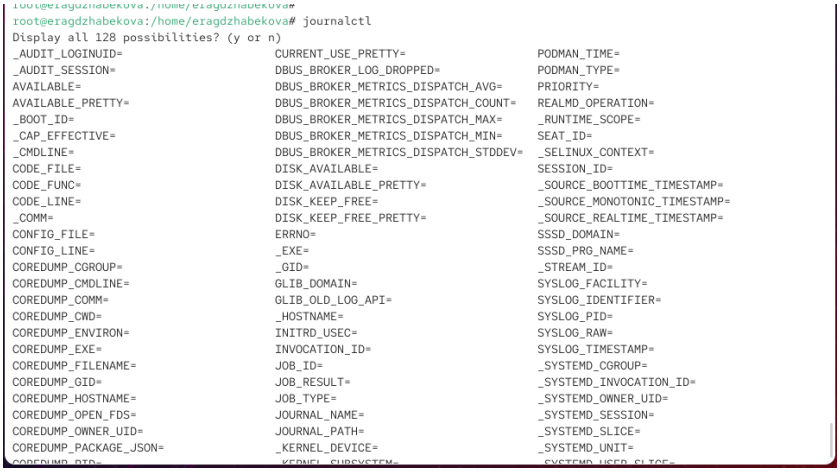

Рис. 2.14: Параметры фильтрации journalctl

5. Отображены события, связанные с пользователем UID 0:

   journalctl _UID=0

   (см. рис. fig. 2.15).

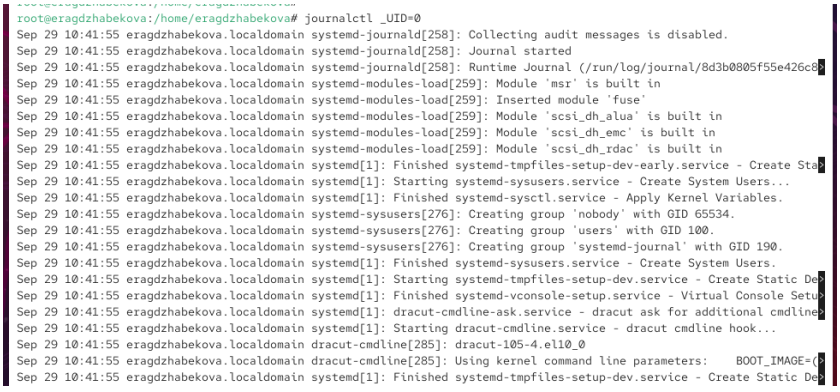

Рис. 2.15: Фильтрация по UID=0

6. Выведены последние 20 строк журнала:

   journalctl -n 20

   (см. рис. fig. 2.16).

Рис. 2.16: Просмотр последних 20 строк

7. Получены только сообщения с уровнем «ошибка»:

   journalctl -p err

   (см. рис. fig. 2.17).

Рис. 2.17: Фильтрация только ошибок

8. Просмотрены все события со вчерашнего дня:

   journalctl –since yesterday

   (см. рис. fig. 2.18).

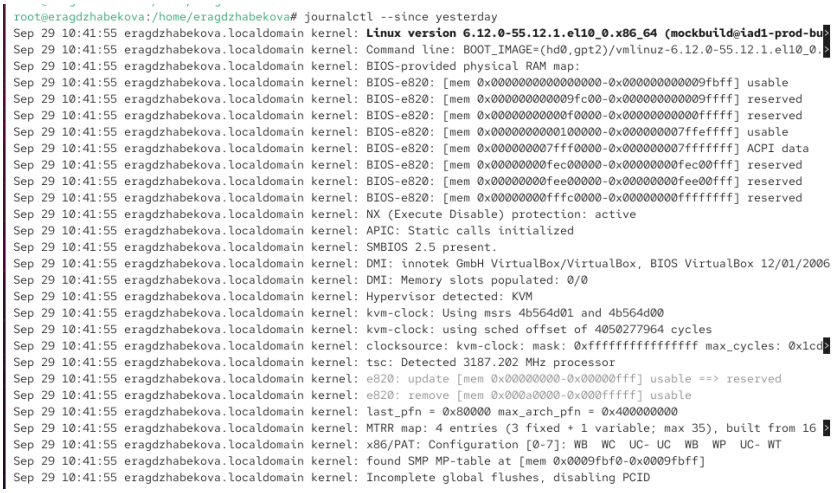

Рис. 2.18: Просмотр событий со вчерашнего дня

9. Отображены только ошибки со вчерашнего дня:

   journalctl –since yesterday -p err

   (см. рис. fig. 2.19).

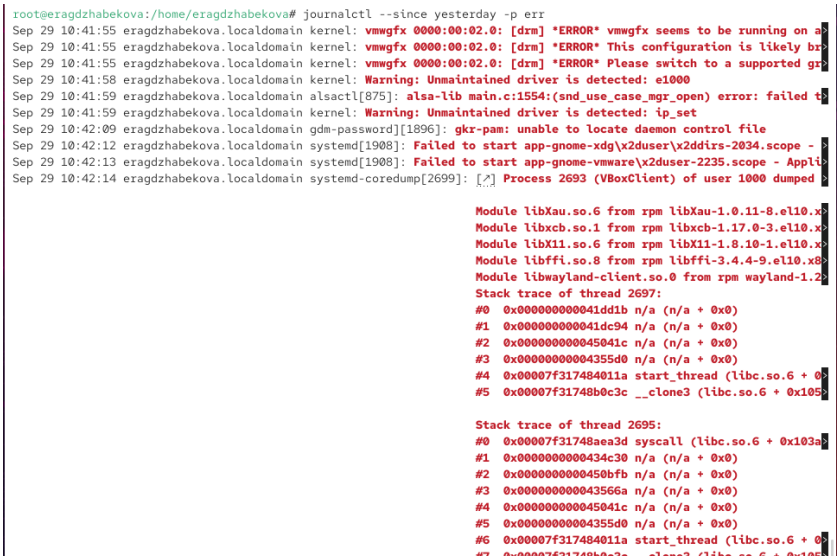

Рис. 2.19: Ошибки со вчерашнего дня

10. Использован режим детализированного вывода:

    journalctl -o verbose

    (см. рис. fig. 2.20).

Рис. 2.20: Детализированный вывод сообщений

11. Для просмотра дополнительной информации о модуле sshd использована команда:

    journalctl _SYSTEMD_UNIT=sshd.service

    В выводе отобразились записи о запуске службы (см. рис. fig. 2.21).

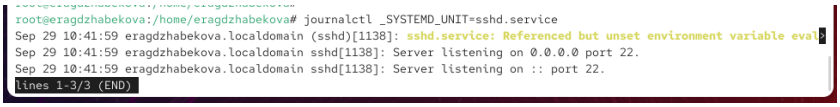

Рис. 2.21: Просмотр информации о модуле sshd

2.4 Постоянный журнал journald

1. Создан каталог для хранения постоянных записей журнала:

   mkdir -p /var/log/journal

2. Для каталога `/var/log/journal` скорректированы права доступа, чтобы служба `systemd-journald` могла вести туда запись:

   chown root:systemd-journal /var/log/journal

   chmod 2755 /var/log/journal

3. Чтобы принять изменения без перезагрузки системы, journald был принудительно перезапущен сигналом:

killall -USR1 systemd-journald

4. После этого просмотрен журнал с момента последней перезагрузки с помощью команды:
   journalctl -b
   (см. рис. fig. 2.22).

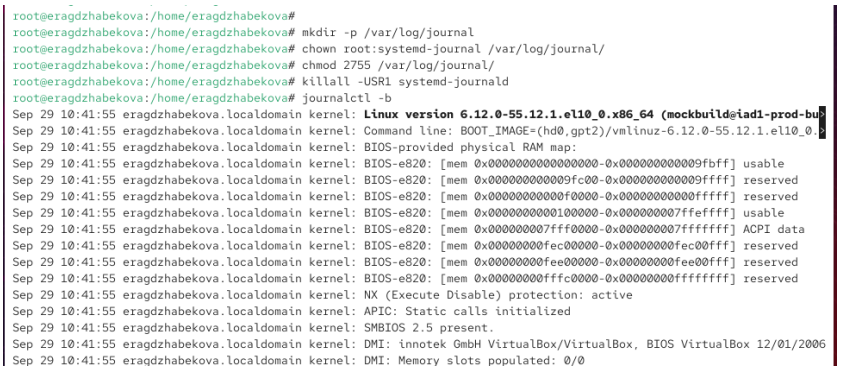

Рис. 2.22: Включение постоянного журнала journald

3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**
   Основной конфигурационный файл — `/etc/rsyslog.conf`. Дополнительные правила могут храниться в каталоге `/etc/rsyslog.d/`.

2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**
   Сообщения об аутентификации и авторизации записываются в файл `/var/log/secure`.

3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**
   По умолчанию лог-файлы ротируются **еженедельно**, настройки задаются в `/etc/logrotate.conf`.

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?**
   Используются команды:

- `tail -f /var/log/имя_журнала` — для файлов rsyslog.

- `journalctl -f` — для systemd-journald.

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 вам видеть сообщения journald после последней перезагрузки системы?**
   `journalctl -b`

8. **Какая процедура позволяет сделать журнал journald постоянным?**

- Создать каталог `/var/log/journal`.

- Назначить права доступа:
  `chown root:systemd-journal /var/log/journal`
  `chmod 2755 /var/log/journal`

- Перезапустить journald командой `killall -USR1 systemd-journald` или выполнить перезагрузку.

4 Заключение

В ходе лабораторной работы были изучены принципы работы с системными журналами в Linux. Рассмотрена настройка службы rsyslog, включая перенаправление сообщений веб-сервера Apache и регистрацию отладочной информации в отдельные файлы. Освоены приёмы мониторинга логов в реальном времени с помощью `tail` и `journalctl`, выполнена фильтрация событий по различным параметрам. Настроен постоянный журнал `journald`, что позволило сохранять сообщения после перезагрузки системы. Получены практические навыки администрирования, связанные с управлением логами и диагностикой работы служб.