Отчёт по лабораторной работе №7

Управление журналами событий в системе

Тукаев Тимур

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение

2.1 Мониторинг журнала системных событий в реальном времени

1. Запущено три окна терминала.
   В каждом окне получены права администратора с использованием команды `su -`.

2. Во втором окне терминала запущен мониторинг системных событий в реальном времени.
   Команда позволяет отслеживать поступающие сообщения ядра и системных служб.

3. В третьем окне выполнен выход из режима суперпользователя с помощью `Ctrl + D`.
   Затем произведена попытка повторного входа с неверным паролем.
   В результате во втором окне отобразилось сообщение об ошибке аутентификации `FAILED SU (to root) titukaev on pts/1`, которое также зафиксировано в журнале `/var/log/messages`.

Рис. 2.1: Ошибка при вводе пароля root

4. В третьем окне введена команда `logger hello`.

   Во втором окне с активным мониторингом отобразилось сообщение, подтверждающее регистрацию записи в журнале `/var/log/messages`.

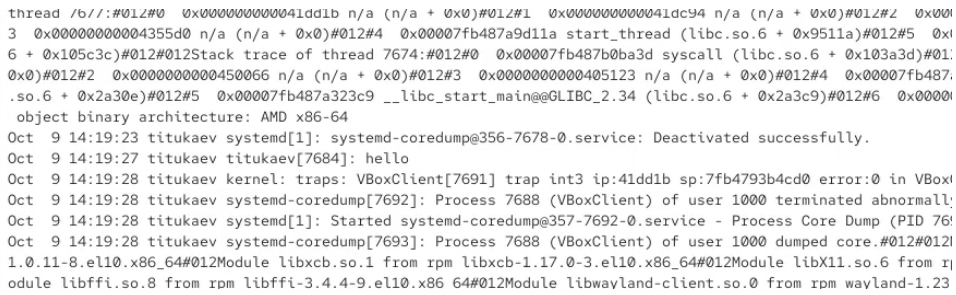

Рис. 2.2: Регистрация пользовательского сообщения в журнале

5. Мониторинг системных сообщений остановлен сочетанием клавиш `Ctrl + C`.

   Затем выполнен просмотр последних 20 строк журнала безопасности.

   В выводе зафиксированы события успешных и неуспешных попыток получения прав суперпользователя, а также операции открытия и закрытия сессий.

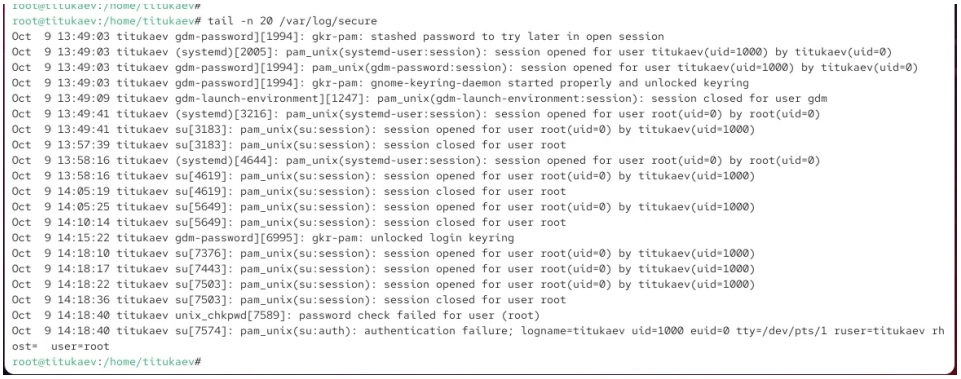

Рис. 2.3: Анализ лога безопасности /var/log/secure

2.2 Изменение правил rsyslog.conf

1. Установлен веб-сервер Apache.

   После завершения установки служба была запущена и добавлена в автозагрузку.

Рис. 2.4: Установка и запуск службы Apache

2. Выполнен просмотр журнала ошибок веб-службы для проверки её работы. В логе отображены уведомления о запуске и настройке Apache, а также о корректном применении контекста SELinux.

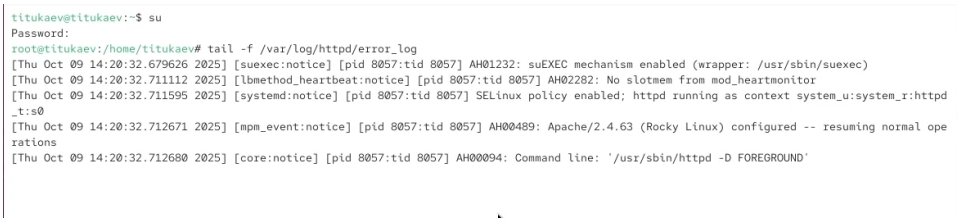

Рис. 2.5: Проверка журнала ошибок Apache

3. В конфигурационном файле `/etc/httpd/conf/httpd.conf` добавлена строка `ErrorLog syslog:local1`,
   обеспечивающая передачу сообщений об ошибках веб-службы через систему журналирования rsyslog.

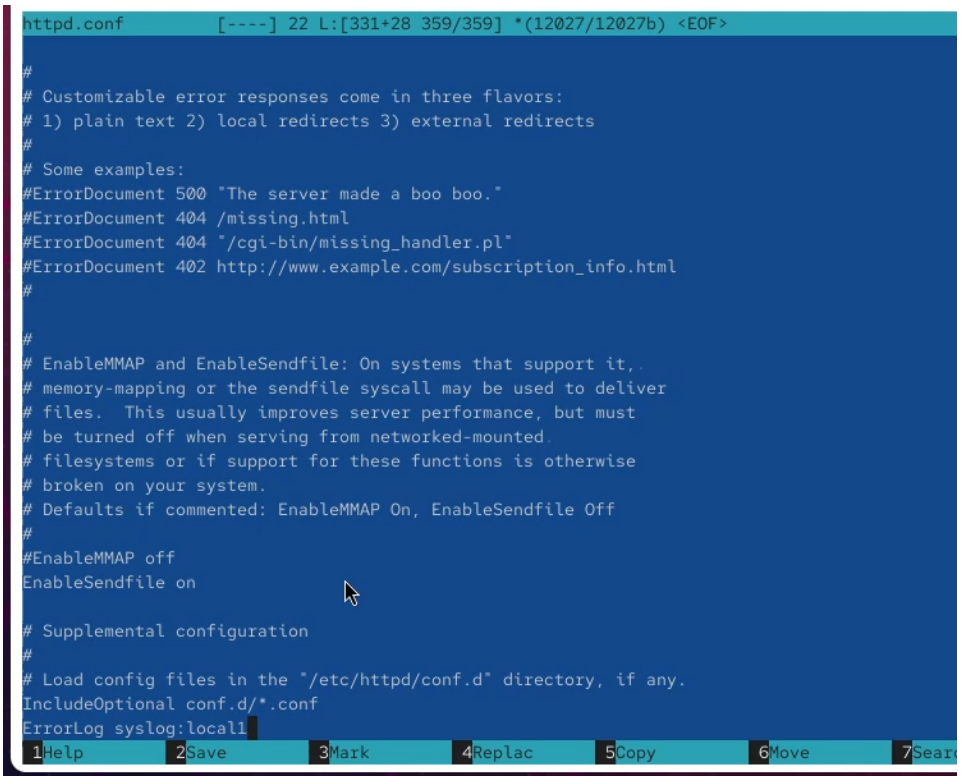

Рис. 2.6: Редактирование конфигурационного файла httpd.conf

4. В каталоге `/etc/rsyslog.d` создан файл `httpd.conf`,
   в котором прописано правило `local1.* -/var/log/httpd-error.log`,
   направляющее сообщения категории `local1` в отдельный файл журнала `/var/log/httpd-error.log`.

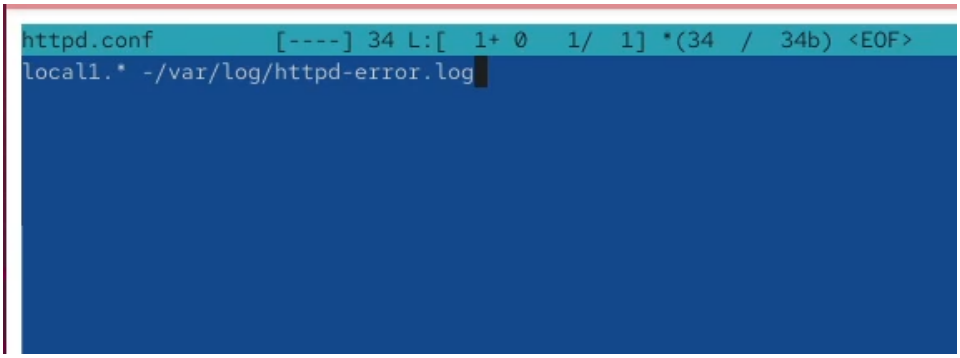

Рис. 2.7: Создание правила для регистрации сообщений Apache в rsyslog

5. Создан отдельный файл конфигурации `debug.conf` для регистрации отладочных сообщений.
   В него добавлено правило `*.debug /var/log/messages-debug`, позволяющее сохранять сообщения уровня отладки в отдельный лог-файл.

Рис. 2.8: Создание файла конфигурации для отладочных сообщений

6. После внесённых изменений службы `rsyslog` и `httpd` были перезапущены.
   При генерации отладочного сообщения с помощью `logger -p daemon.debug "Daemon Debug Message"`
   запись появилась в файле `/var/log/messages-debug`, что подтвердило корректность настроек.

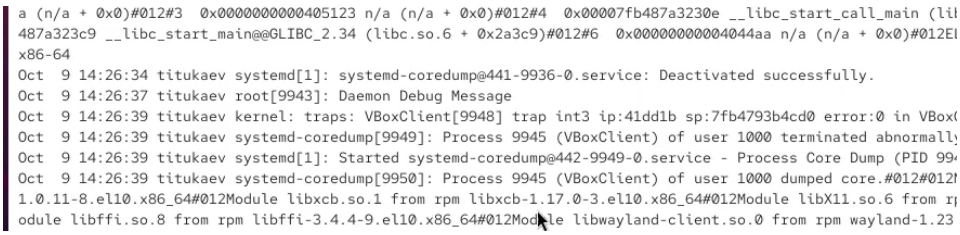

Рис. 2.9: Регистрация отладочного сообщения в системном журнале

2.3 Использование journalctl

1. Просмотрен системный журнал с момента последнего запуска системы. Отображены сообщения ядра, включая сведения о версии Linux, параметрах BIOS и аппаратной конфигурации.

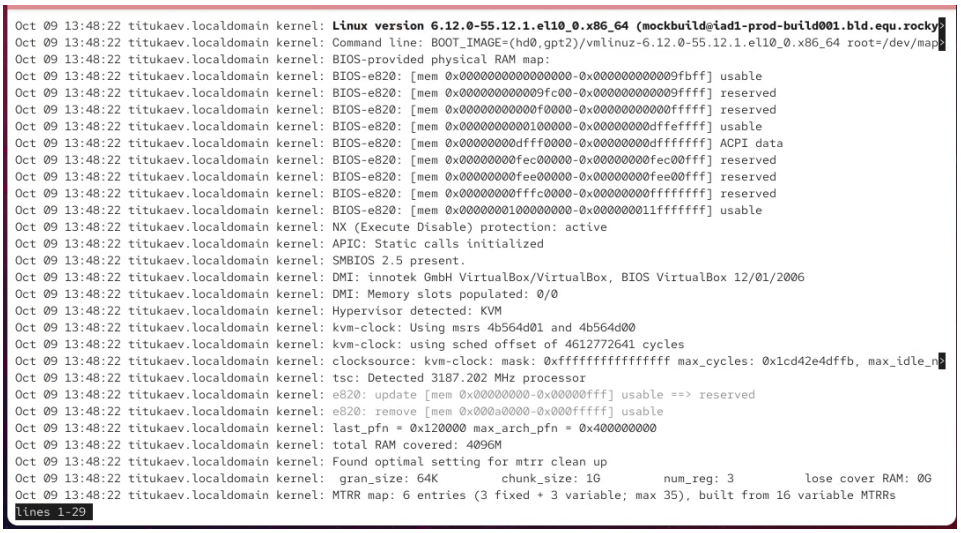

Рис. 2.10: Просмотр системного журнала после запуска системы

2. Произведён просмотр журнала без использования пейджера для вывода всех сообщений в непрерывном виде.
   Это позволяет анализировать логи без постраничной навигации.

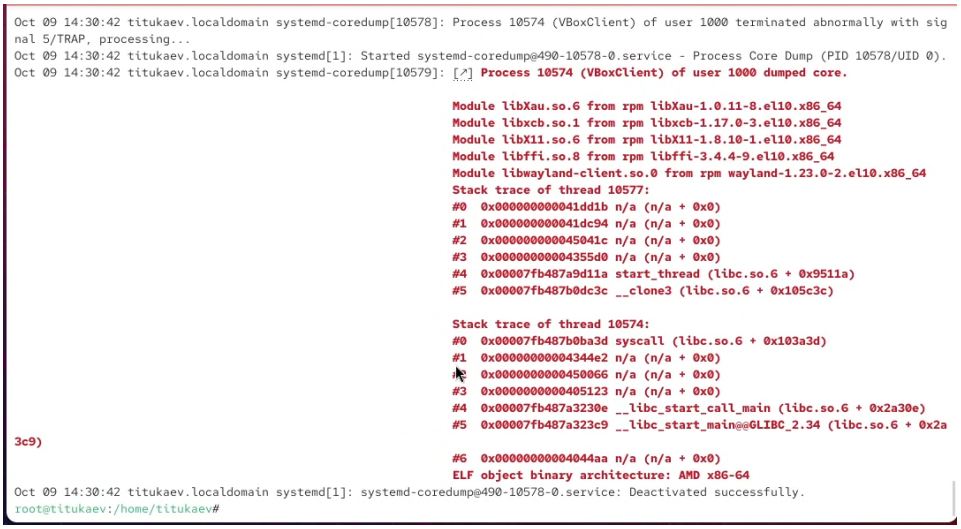

Рис. 2.11: Просмотр журнала без пейджера

3. Активирован режим мониторинга журнала в реальном времени.

   В ходе наблюдения зафиксированы ошибки, связанные с процессом `VBoxClient`, приведшие к созданию дампа ядра.

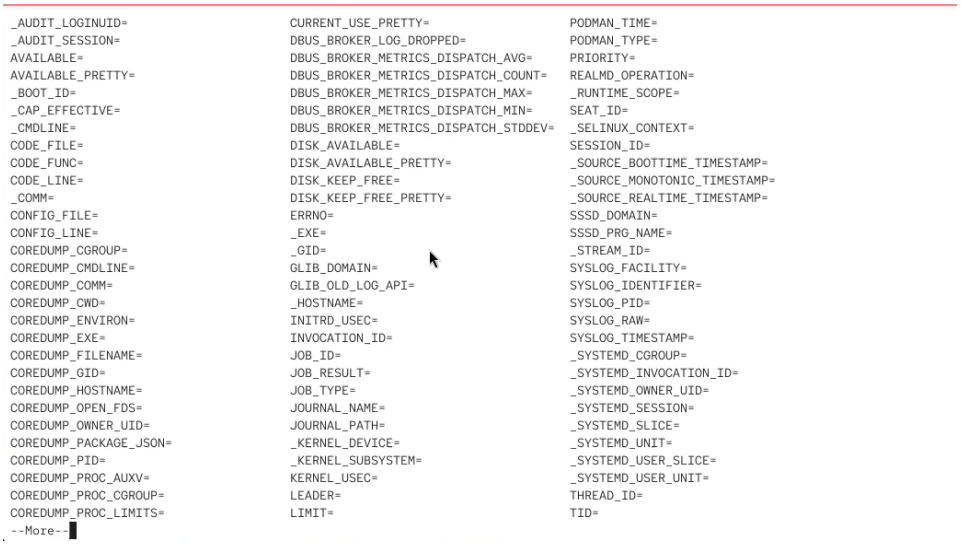

Рис. 2.12: Мониторинг журнала в реальном времени и фиксация ошибок VBoxClient

4. Выполнен просмотр всех доступных параметров фильтрации с помощью двойного нажатия клавиши Tab после ввода команды `journalctl`.

В списке представлены ключи, позволяющие выполнять выборку по полям системных сообщений.

Рис. 2.13: Просмотр параметров фильтрации журнала

5. Выполнен фильтр вывода по идентификатору пользователя с UID 0, чтобы отобразить все события, связанные с пользователем root.

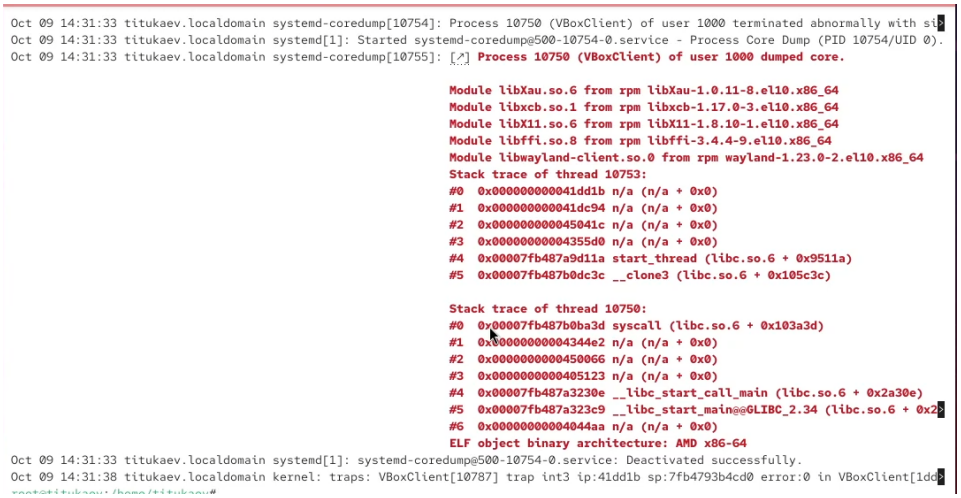

Рис. 2.14: Фильтрация сообщений журнала по UID 0

6. Произведён просмотр последних 20 строк системного журнала для анализа последних записей.

Зафиксированы записи об успешной инициализации служб и завершении процессов.

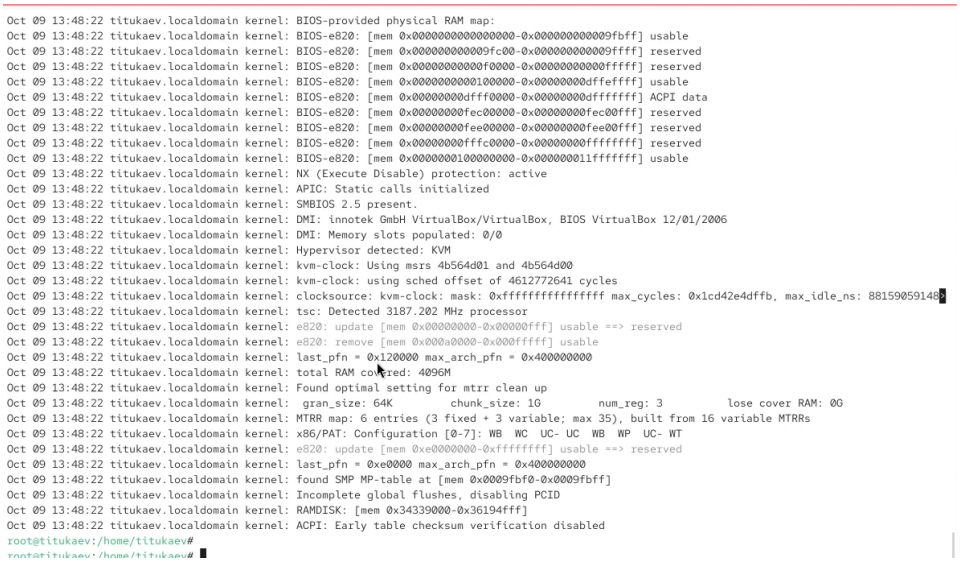

Рис. 2.15: Просмотр последних строк журнала

7. Выполнен фильтр по модулю `sshd.service` для получения сведений о работе SSH-сервера.

   В журнале отображены записи о запуске службы и активации прослушивания порта 22.

Рис. 2.16: Просмотр сообщений о работе службы SSHD

2.4 Постоянный журнал journald

1. Получены права администратора для внесения изменений в конфигурацию службы журналирования.

2. Создан каталог `/var/log/journal`, предназначенный для хранения постоянных записей системного журнала.
   Это позволяет сохранять логи между перезагрузками системы.

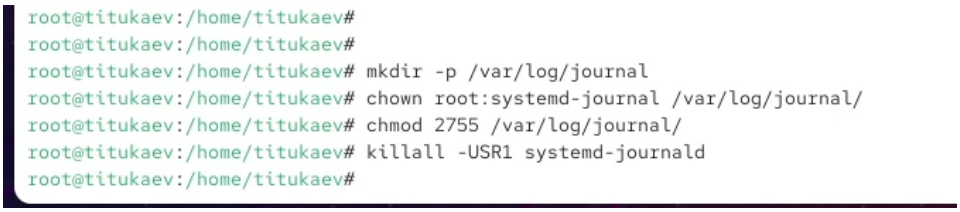

Рис. 2.17: Создание каталога для постоянного хранения журнала

3. Установлены необходимые права доступа к каталогу:
   владельцем назначена группа `systemd-journal`, а права доступа заданы как `2755`.
   Такая настройка обеспечивает возможность записи службы journald в данный каталог.

4. Для применения изменений выполнена команда `killall -USR1 systemd-journald`,
   сигнализирующая службе journald о необходимости перезапуска с учётом новой конфигурации.

5. После выполнения всех шагов система ведёт **постоянный журнал**,
   записи которого сохраняются в каталоге `/var/log/journal` и доступны после перезагрузки.

3 Контрольные вопросы

1. Для настройки службы системного журналирования используется файл конфигурации `/etc/rsyslog.conf`.
2. Сообщения, связанные с аутентификацией пользователей и доступом, сохраняются в файле `/var/log/secure`.
3. Если не изменять стандартную конфигурацию, ротация файлов журналов выполняется еженедельно.
4. Для записи всех сообщений с приоритетом `info` в отдельный файл необходимо добавить строку:
   `*.info /var/log/messages.info`
5. Для просмотра сообщений журнала в режиме реального времени используется команда `tail -f /var/log/messages`
   или её системная альтернатива `journalctl -f`.
6. Чтобы вывести все сообщения, записанные для процесса с PID 1 между 9:00 и 15:00, применяют команду:
   `journalctl _PID=1 --since "09:00" --until "15:00"`.
7. Для просмотра всех сообщений journald, зафиксированных после последней перезагрузки системы, используется команда:
   `journalctl -b`.
8. Чтобы сделать журнал journald постоянным, необходимо создать каталог `/var/log/journal`,

назначить ему владельца `root:systemd-journal`, установить права доступа `chmod 2755`,
а затем перезапустить службу journald с помощью команды
`killall -USR1 systemd-journald` или перезагрузить систему.

4 Заключение

В ходе лабораторной работы были изучены механизмы системного журналирования в Linux.
Рассмотрены принципы работы служб `rsyslogd` и `journald`, методы фильтрации и анализа сообщений,
а также способы настройки постоянного хранения логов.
Полученные навыки позволяют эффективно контролировать состояние системы и выявлять источники ошибок.