Лабораторная работа № 7. Управление журналами событий в системе

Отчёт

Сергеев Даниил Олегович

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе. [1]

# 2 Задание

* Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени.
* Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
* Продемонстрируйте навыки работы с journalctl.
* Продемонстрируйте навыки работы с journald.

# 3 Ход выполнения лабораторной работы

## 3.1 Мониторинг журнала системных событий в реальном времени

Откроем три вкладки терминала и в каждом из них войдем под учетную запись root. На втором из них запустим мониторинг сисемных событий в реальном времени (tail -f /var/log/messages), а на третьем вернемся к своей стандартной учетной записи и попробуем снова получить полномочия администратора (Предварительно выйдем из нее, нажав сочетание Ctrl+d). На этот раз специально введем неправильный пароль, чтобы сообщение об ошибке передалось в лог системных событий. Чтобы зафиксировать сообщение “hello” пропишем команду logger hello. Оно отобразиться в выводе второго терминала.

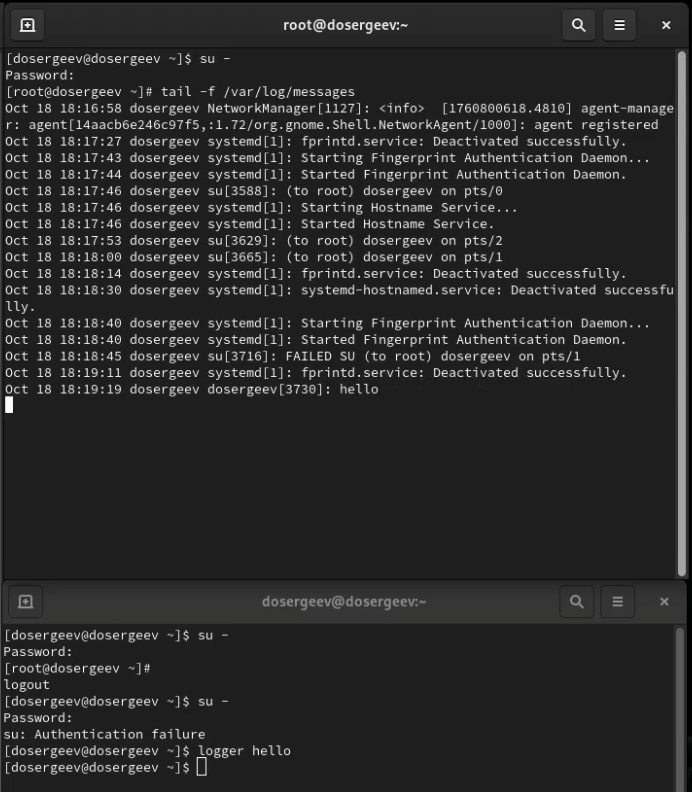


Рис. 1: Мониторинг системных событий в реальном времени

Во второй вкладке терминала с мониторингом остановим вывод логов в реальном времени (Ctrl+c) и выведем последние 20 строк файла сообщений безопасности командой tail -n 20 /var/log/secure

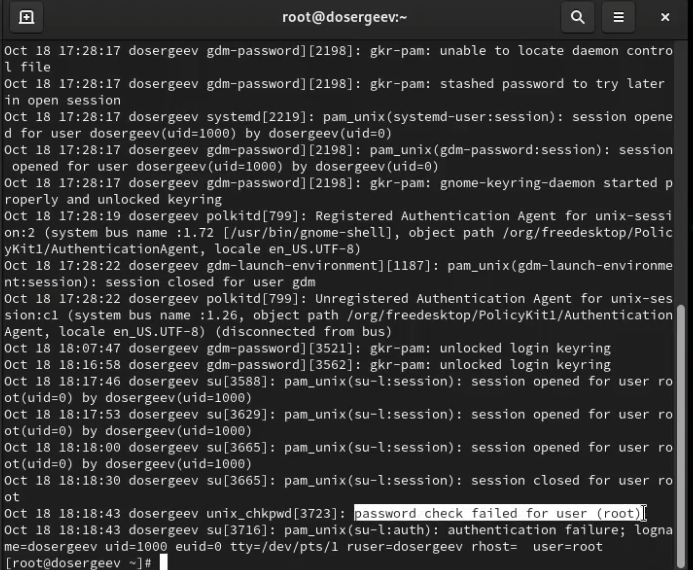


Рис. 2: Вывод логов /var/log/secure

## 3.2 Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache (пакет httpd). После окончания процесса установки запустим службу командами systemctl start httpd и systemctl enable httpd

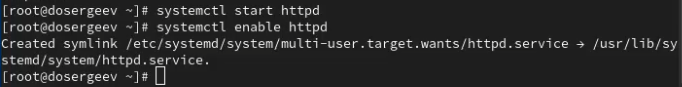


Рис. 3: Запуск службы httpd

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы. Закроем его сочетанием Ctrl+c.

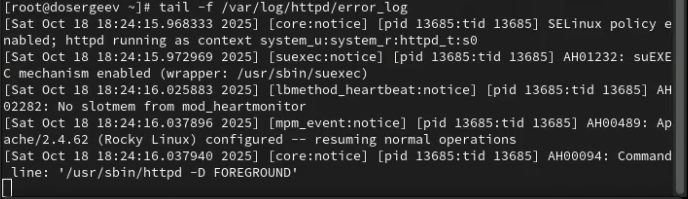


Рис. 4: Журнал ошибок httpd

В третьем терминале перейдем в каталог /etc/httpd/conf и отредактируем конфиг службы httpd.conf, добавив в конце строку ErrorLog syslog:local1.

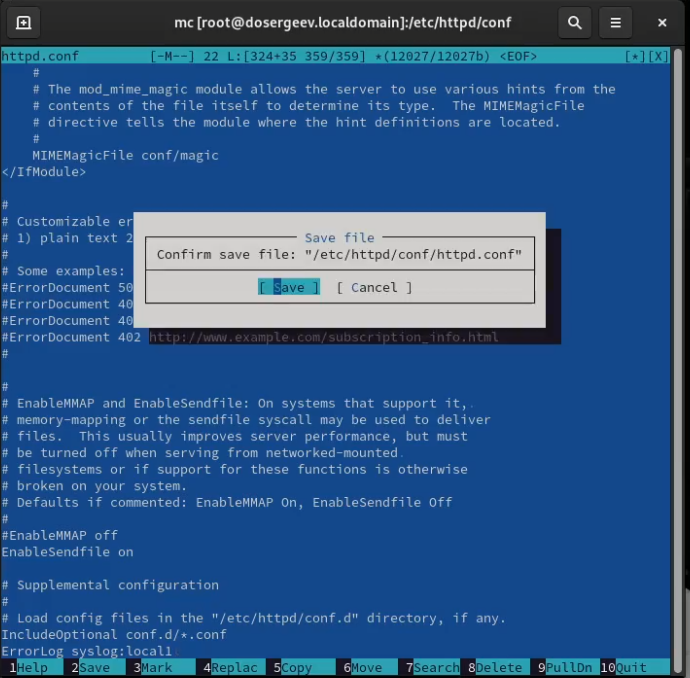


Рис. 5: Редактирование httpd.conf

Теперь перейдем в каталог /etc/rsyslog.d и создадим файл мониторинга событий веб-службы.

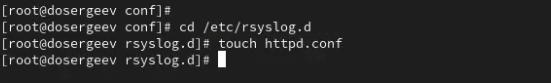


Рис. 6: Создание httpd.conf в /etc/rsyslog.d

Пропишем в нем строку, которая позволит нам отправлять все сообщения, получаемые для local1, в файл /var/log/httpd-error.log

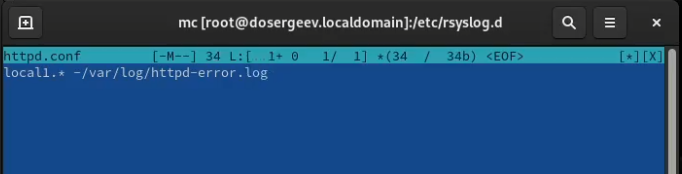


Рис. 7: Модификация файла мониторинга httpd.conf

Перейдем обратно в первый терминал и перезагрузим rsyslogd и httpd:

* systemctl restart rsyslog.service
* systemctl restart httpd

В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации.

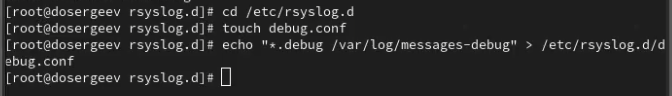


Рис. 8: Файл мониторинга отладочной информации

Во втором терминале запустим мониторинг файла /var/log/messages-debug в реальном времени, а на третьей вкладке отправим пробное сообщение с помощью команды logger:

* logger -p daemon.debug “Daemon Debug Message”

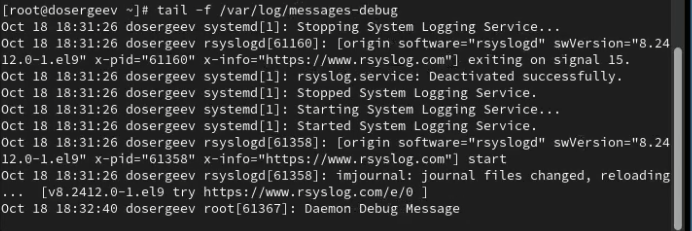


Рис. 9: Проверка мониторинга отладки rsyslog

## 3.3 Использование journalctl

Проведем ряд операций journalctl. А именно:

* Посмотрим содержимое журнала с событиями с момента последнего запуска системы: journalctl

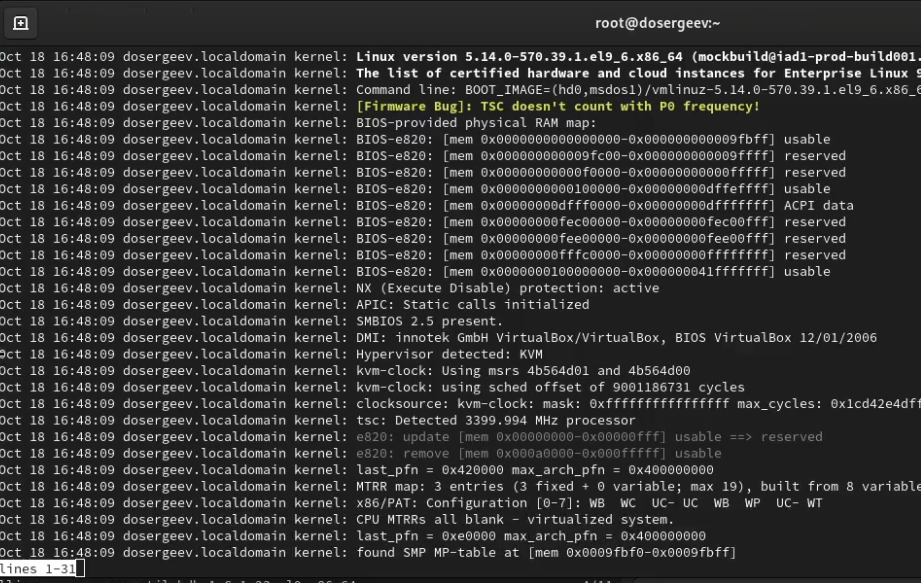


Рис. 10: Вывод journalctl

* Посмотрим содержимое журнала без использования пейджера: journalctl –no-pager

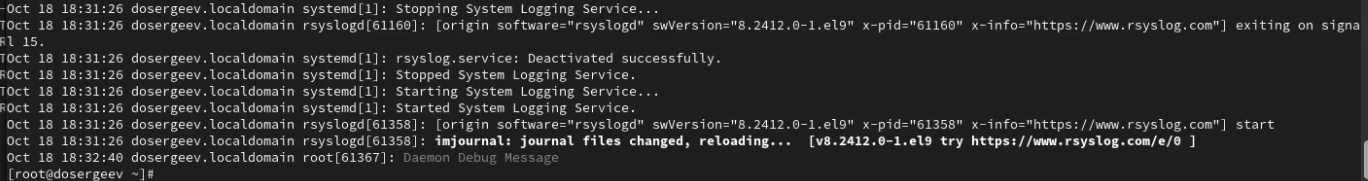


Рис. 11: Вывод journalctl –no-pager

* Включим режим просмотра в реальном времени: journalctl -f

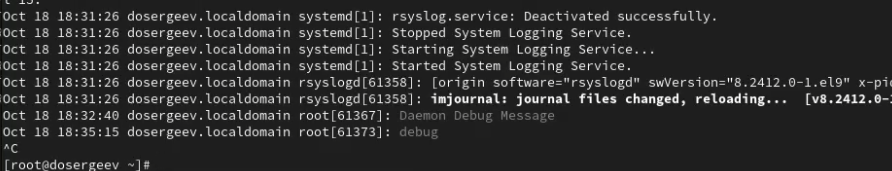


Рис. 12: Вывод journalctl -f

* Просмотрим события для UID0: journalctl \_UID=0

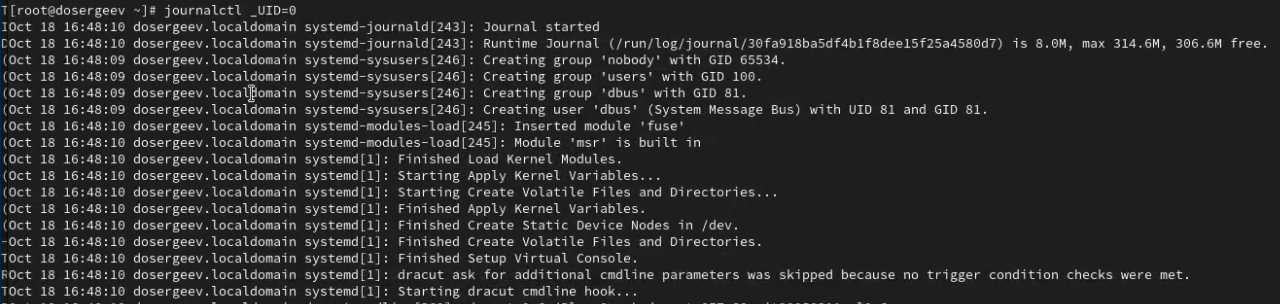


Рис. 13: Вывод journalctl \_UID=0

* Отобразим последние 20 строк журнала: journalctl -n 20

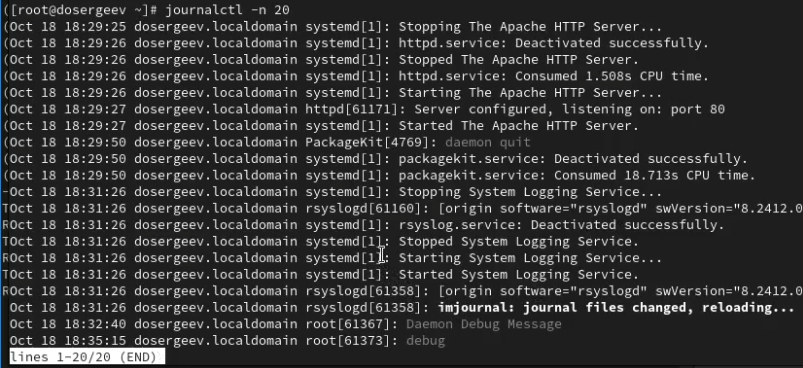


Рис. 14: Вывод journalctl -n 20

* Просмотрим только сообщения об ошибках: journalctl -p err

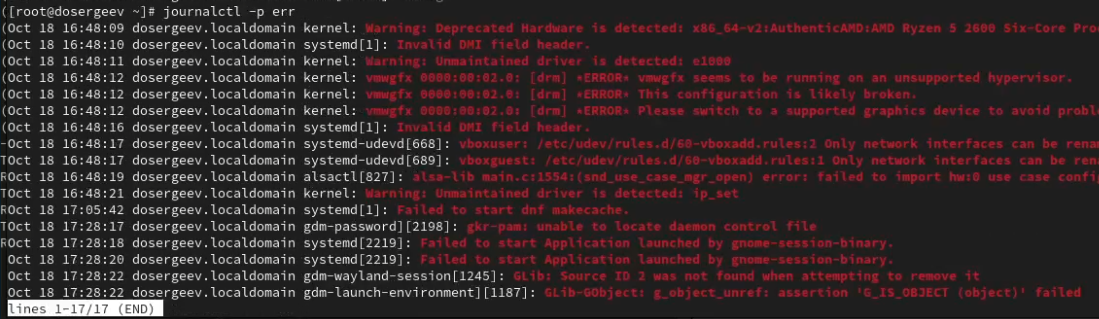


Рис. 15: Вывод journalctl -p err

* Отфильтруем вывод журнала по точному времени: journalctl –since “2025-10-18 18:28:00”

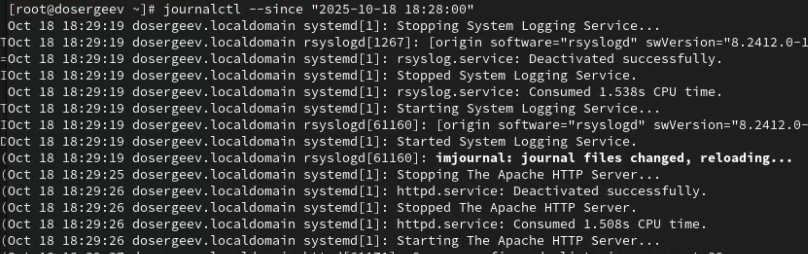


Рис. 16: Вывод journalctl –since “2025-10-18 18:28:00”

* Отфильтруем вывод журнала по относительному времени с выводом сообщений с ошибкой приоритета: journalctl –since yesterday -p err

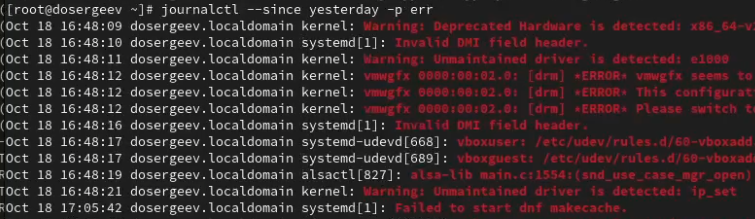


Рис. 17: Вывод journalctl –since yesterday -p err

* Выведем детальную информацию: journalctl -o verbose

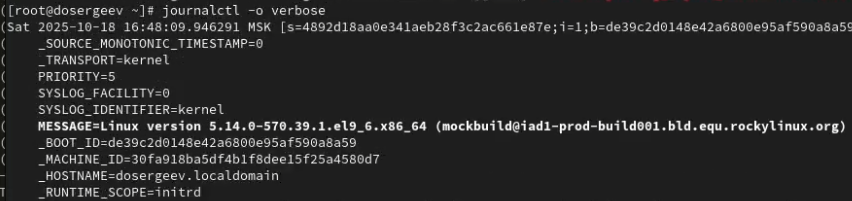


Рис. 18: Вывод journalctl -o verbose

* Просмотрим дополнительную информацию о службе, напрмер о sshd: journalctl \_SYSTEMD\_UNIT=sshd.service

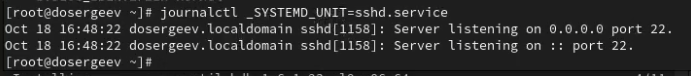


Рис. 19: Вывод journalctl \_SYSTEMD\_UNIT=sshd.service

## 3.4 Постоянный журнал journald

Запустим терминал и получим полномочия администратора. Создадим каталог для хранения записей журнала и настроим права доступа так, чтобы journald смог записывать информацию в журнал /var/log/journal. Для принятия изменений используем команду killall -USR1 systemd-journald

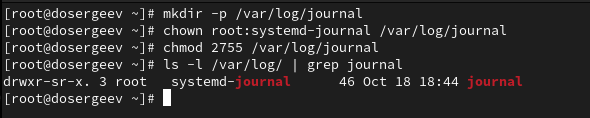


Рис. 20: Настройка прав для /var/log/journal

Журнал systemd теперь стал постоянным. Посмотрим сообщения журнала с момента загрузки: journalctl -b.

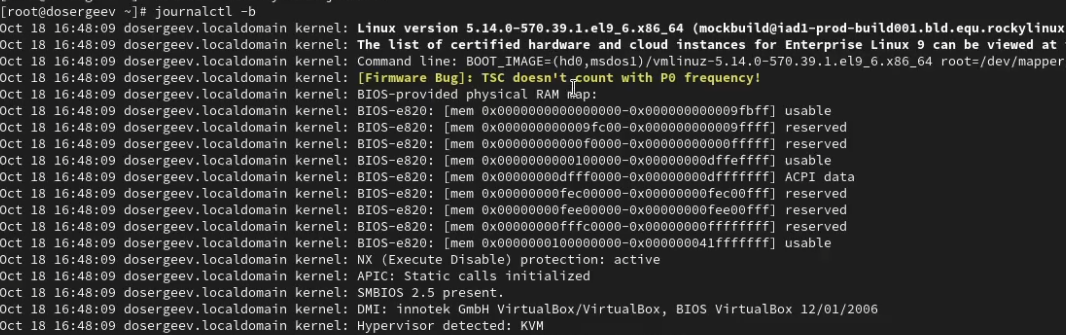


Рис. 21: Вывод сообщений журнала

# 4 Ответы на контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

* /etc/rsyslog.conf

1. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

* /var/log/secure

1. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

* По умолчанию в дистрибутиве Rocky Linux установлена утилита logrotate, которая автоматически ротирует журналы. Чтобы узнать период ротации, можно посмотреть файл /etc/logrotate.conf

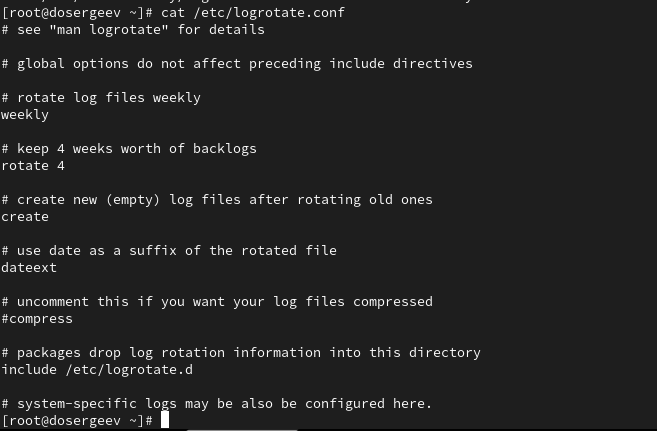


Рис. 22: Файл конфигурации logrotate

* Для ротации файлов журналов потребуется одна неделя (weekly)

1. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

* “\*.info /var/log/messages.info”

1. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

* tail -f <Журнал>

1. 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”

1. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

* journalctl -b(–boot)

1. Какая процедура позволяет сделать журнал journald постоянным?

* Создать директорию для хранения журналов: mkdir -p /var/log/journal
* Настроить права директории: chown root:systemd-journal /var/log/journal; chmod 2775 /var/log/journal.
* Перезапустить систему или службу: reboot или killall -USR1 systemd-journald

# 5 Вывод

В результате выполнения лабораторной работы я получил навыки работы с утилитой journalctl и мониторинга событий в системе Linux.

# Список литературы

1. Kulyabov, Korolykova. Лабораторная работа № 7. Управление журналами событий в системе. <https://esystem.rudn.ru/pluginfile.php/2843484/mod_resource/content/4/008-syslog.pdf>; RUDN.