Лабораторная работа №7

Управление журналами событий в системе

Юсупова Ксения Равилевна

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с journalctl (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с journald (см. раздел 7.4.4).

# 3 Выполнение лабораторной работы

Запустили три вкладки терминала и в каждом из них получите полномочия администратора. На второй вкладке терминала запустили мониторинг системных событий в реальном времени, позже также во второй вкладке терминала с мониторингом остановили трассировку файла сообщений мониторинга реального времени, используя Ctrl + c . Затем запустили мониторинг сообщений безопасности (последние 20 строк соответствующего файла)(рис. 1).

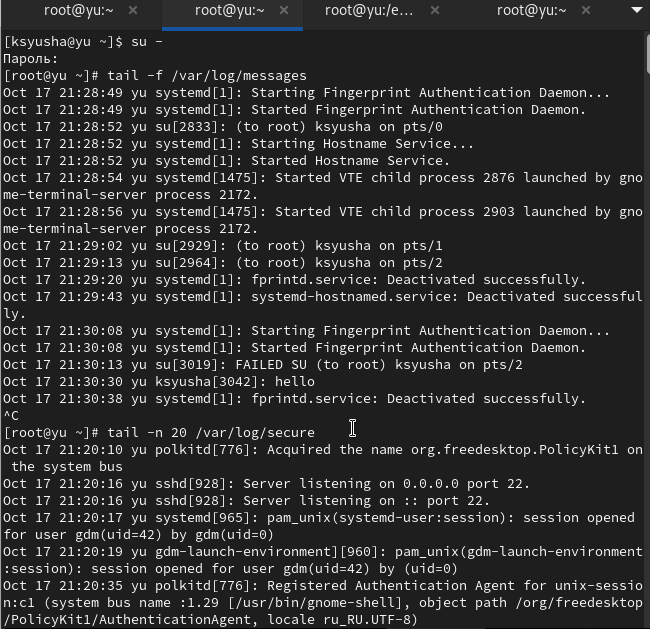


Рис. 1: Выполнили пункты 1, 2 и 5 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени)

В третьей вкладке терминала вернулись к учётной записи своего пользователя (достаточно нажать Ctrl + d ) и попробовали получить полномочия администратора, но ввели неправильный пароль. Обратили внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение “FAILED SU (to root) username …”, затем ввели logger hello (рис. 2).

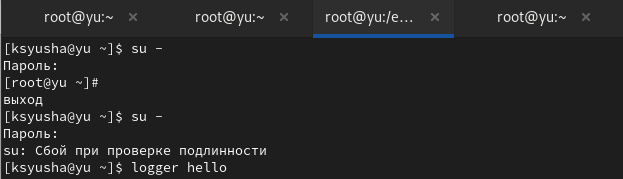


Рис. 2: Выполнили пункты 3 и 4 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени)

В первой вкладке терминала установили Apache, после окончания процесса установки запустили веб-службу(рис. 3).

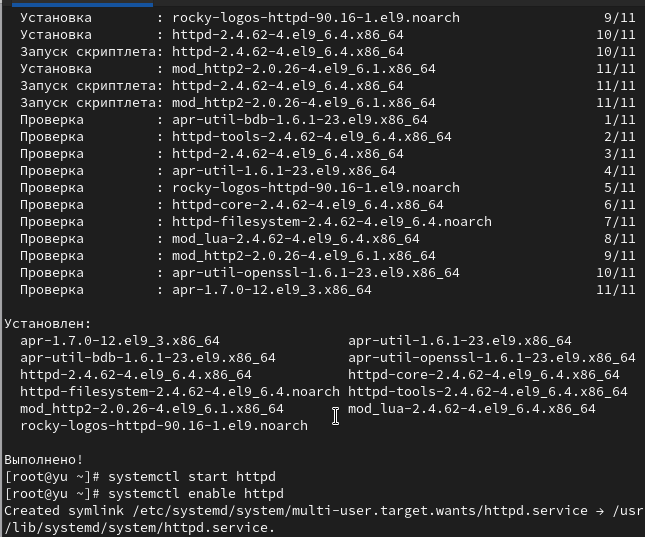


Рис. 3: Выполнили пункты 1 и 2 из раздела 7.4.2 (Изменение правил rsyslog.conf)

о второй вкладке терминала посмотрели журнал сообщений об ошибках веб-службы(рис. 4).

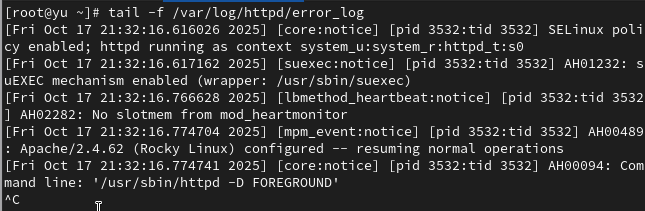


Рис. 4: Выполнили пункт 3 из раздела 7.4.2 (Изменение правил rsyslog.conf)

В третьей вкладке терминала получили полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавьте следующую строку: ErrorLog syslog:local1. Здесь local0 — local7 — это «настраиваемые» средства (объекты), которые syslog предоставляет пользователю для регистрации событий приложения в системном журнале. В каталоге /etc/rsyslog.d создали файл мониторинга событий веб-службы. Открыв его на редактирование, прописали в нём local1.\* -/var/log/httpd-error.log . Эта строка позволит отправлять все сообщения, получаемые для объекта local1. Позже создали отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале ввели echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf и logger -p daemon.debug “Daemon Debug Message(рис. 5).

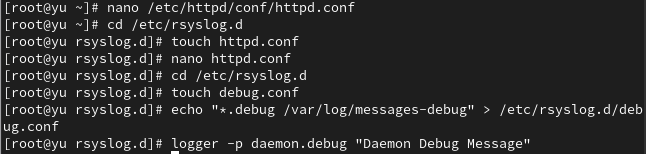


Рис. 5: Выполнили пункты 4, 5, 7, 10 из раздела 7.4.2 (Изменение правил rsyslog.conf)

Перешли в первую вкладку терминала и перезагрузили конфигурацию rsyslogd и веб-службу, позже снова перезапустили rsyslogd(рис. 6).

Выполнили пункты 6 и 8 з раздела 7.4.2 (Изменение правил rsyslog.conf)

Рис. 6: Выполнили пункты 6 и 8 з раздела 7.4.2 (Изменение правил rsyslog.conf)

Во второй вкладке терминала запустили мониторинг отладочной информации, позже посмотрели сообщение отладки.(рис. 7).

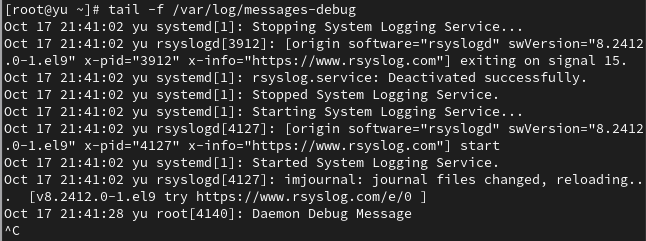


Рис. 7: Выполнили пункт 9 и 11 из раздела 6.5 (Самостоятельная работа) и 6.5.2 (Задание 2)

Во второй вкладке терминала посмотрели содержимое журнала с событиями с момента последнего запуска системы и содержимого журнала без использования пейджера(рис. 8).

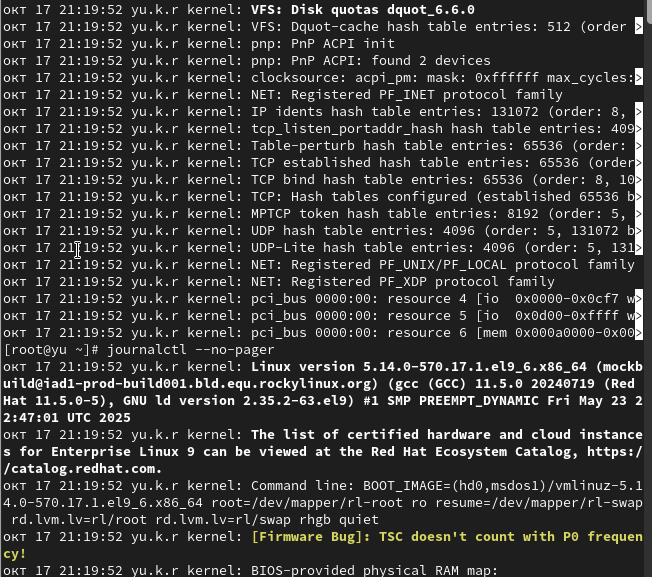


Рис. 8: Выполнили пункты 1 и 2 из раздела 7.4.3. (Использование journalctl)

Посмотрели режим просмотра журнала в реальном времени. Для использования фильтрации просмотра конкретных параметров журнала ввели journalctl и дважды нажмите клавишу Tab(рис. 9).

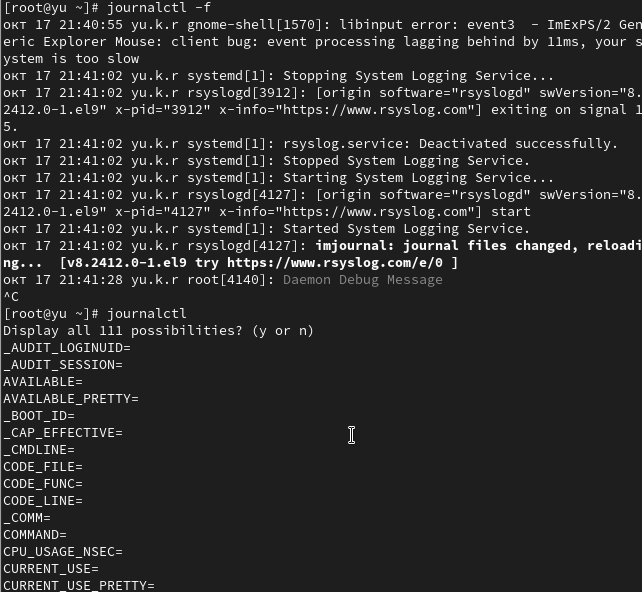


Рис. 9: Выполнили пункты 3 и 4 из раздела 7.4.3. (Использование journalctl)

Просмотрели события для UID0. Для отображения последних 20 строк журнала ввели journalctl -n 20 и для просмотра только сообщений об ошибках journalctl -p err(рис. 10).

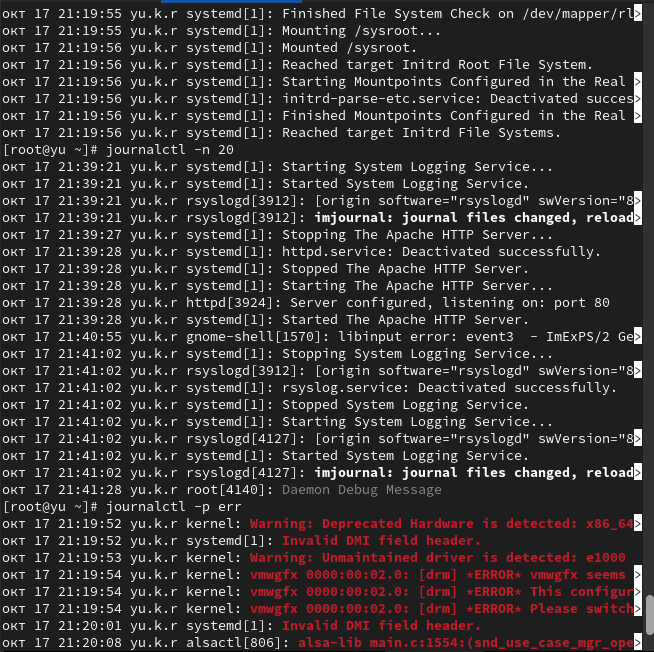


Рис. 10: Выполнили пункты 4-5 из раздела 7.4.3. (Использование journalctl)

Для просмотра всех сообщений со вчерашнего дня ввели journalctl –since yesterday, чтобы показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то использовали journalctl –since yesterday -p err, для детальной информации ввели journalctl -o verbose, для просмотра дополнительной информации о модуле sshd ввели journalctl \_SYSTEMD\_UNIT=sshd.service(рис. 11).

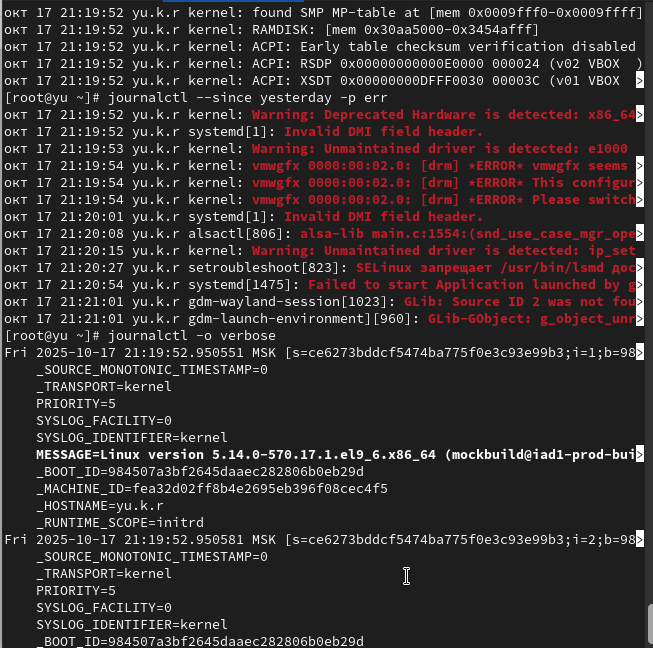


Рис. 11: Выполнили пункты 8-11 из раздела 7.4.3. (Использование journalctl)

Запустили терминал и получили полномочия администратора. Создали каталог для хранения записей журнала, скорректировали права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: killall -USR1 systemd-journald. Журнал systemd теперь постоянный, чтобы видеть сообщения журнала с момента последней перезагрузки journalctl -b(рис. 12).

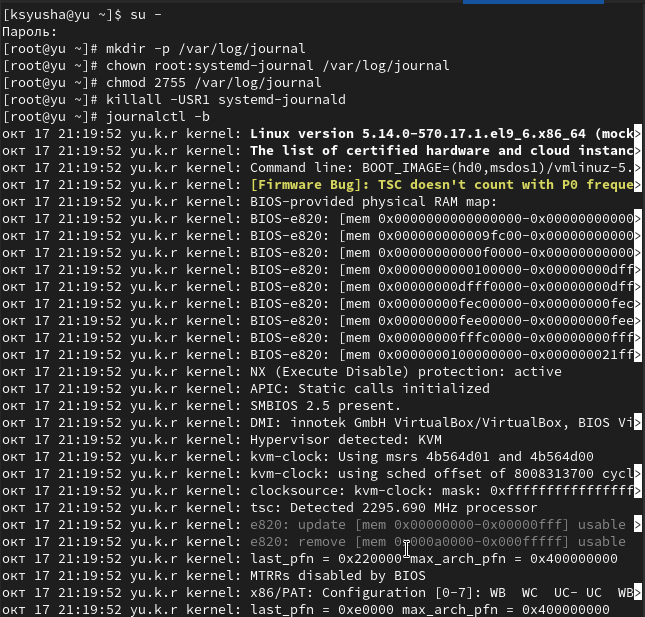


Рис. 12: Выполнили пункты 1-5 из раздела 7.4.4. (Постоянный журнал journald)

# 4 Ответы на контрольные вопросы

1. Для настройки rsyslogd используется файл /etc/rsyslog.conf.
2. Сообщения, связанные с аутентификацией, содержатся в файле /var/log/secure.
3. Без дополнительной настройки ротация файлов журналов выполняется еженедельно.
4. Для записи сообщений с приоритетом info в файл /var/log/messages.info следует добавить строку: \*.info /var/log/messages.info
5. Команда tail -f /var/log/messages позволяет просматривать сообщения журнала в реальном времени.
6. Команда journalctl \_PID=1 –since “09:00” –until “15:00” показывает сообщения для PID 1 за указанный период.
7. Команда journalctl -b отображает сообщения journald с последней перезагрузки системы.
8. Для создания постоянного журнала journald необходимо создать директорию /var/log/journal и перезапустить службу systemd-journald.

# 5 Выводы

В ходе лабораторной работы мы получили навыки работы с журналами мониторинга различных событий в системе.