Лабораторная работа № 7

Отчёт

Ермишина Мария Кирилловна

Содержание

# 1 Цель работы

Целью данной лабораторной работы является получение навыков работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

1. Мониторинг журнала системных событий в реальном времени Запустите три вкладки терминала и в каждом из них получите полномочия админи- стратора. На второй вкладке терминала запустите мониторинг системных событий в реальном времени: (рис. 1)

* tail -f /var/log/messages В третьей вкладке терминала вернитесь к учётной записи своего пользователя и попробуйте получить полномочия администратора, но введите неправильный пароль. Обратите внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username …». (рис. 1) В третьей вкладке терминала из оболочки пользователя введите logger hello - во второй вкладке терминала с мониторингом событий вы увидите сообщение. (рис. 1)

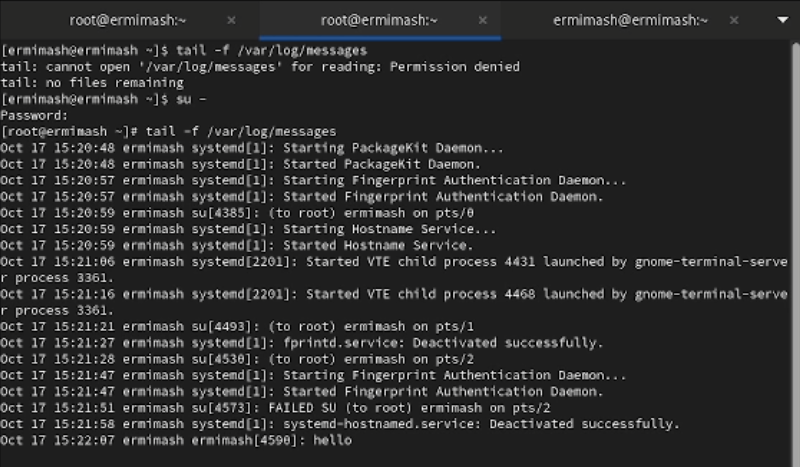


Рис. 1: Изменения на второй вкладке

Во второй вкладке терминала с мониторингом остановите трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем запустите мониторинг сообщений безопасности: (рис. 2) - tail -n 20 /var/log/secure

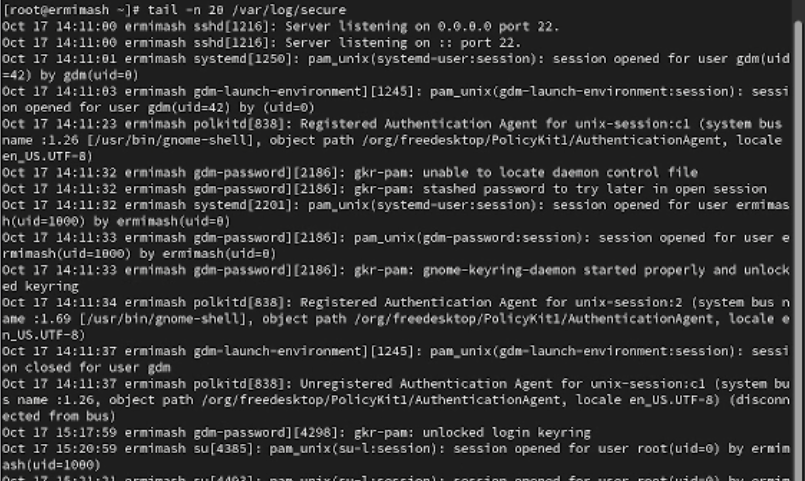


Рис. 2: Мониторинг сообщений безопасности

1. Изменение правил rsyslog.conf В первой вкладке терминала установите Apache, если он не был ранее инсталлирован: (рис. 3)

* dnf -y install httpd После окончания процесса установки запустите веб-службу: (рис. 3)
* systemctl start httpd
* systemctl enable httpd

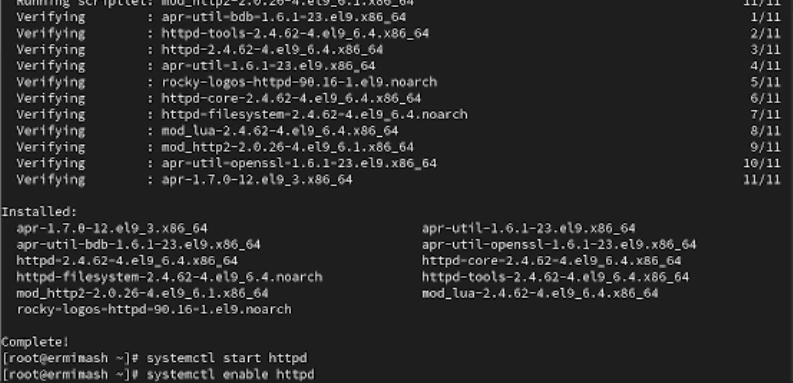


Рис. 3: Установка Apache

Во второй вкладке терминала посмотрите журнал сообщений об ошибках веб-службы: (рис. 4) - tail -f /var/log/httpd/error\_log



Рис. 4: Журнал соо. об ошибках

В каталоге /etc/rsyslog.d создайте файл мониторинга событий веб-службы: - cd /etc/rsyslog.d - touch httpd.conf Открыв его на редактирование, пропишите в нём: (рис. 5) - local1.\* -/var/log/httpd-error.log

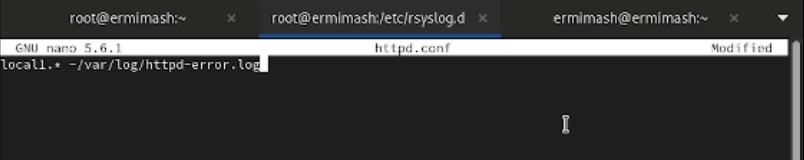


Рис. 5: Редактирование файла

Перейдите в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу: - systemctl restart rsyslog.service - systemctl restart httpd

В третьей вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации: (рис. 6) - cd /etc/rsyslog.d - touch debug.conf

В этом же терминале введите: (рис. 6) - echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf

В первой вкладке терминала снова перезапустите rsyslogd: - systemctl restart rsyslog.service

Во второй вкладке терминала запустите мониторинг отладочной информации: - tail -f /var/log/messages-debug

В третьей вкладке терминала введите: (рис. 6) - logger -p daemon.debug “Daemon Debug Message”

В терминале с мониторингом посмотрите сообщение отладки.

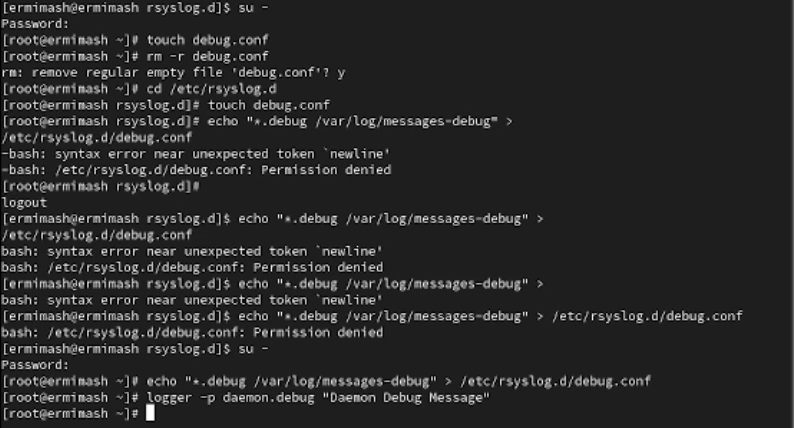


Рис. 6: Работа с третьим окном

1. Использование journalctl Во второй вкладке терминала посмотрите содержимое журнала с событиями с момента последнего запуска системы: (рис. 7)

* journalctl Просмотр содержимого журнала без использования пейджера: (рис. 8)
* journalctl –no-pager Режим просмотра журнала в реальном времени: (рис. 8)
* journalctl -f

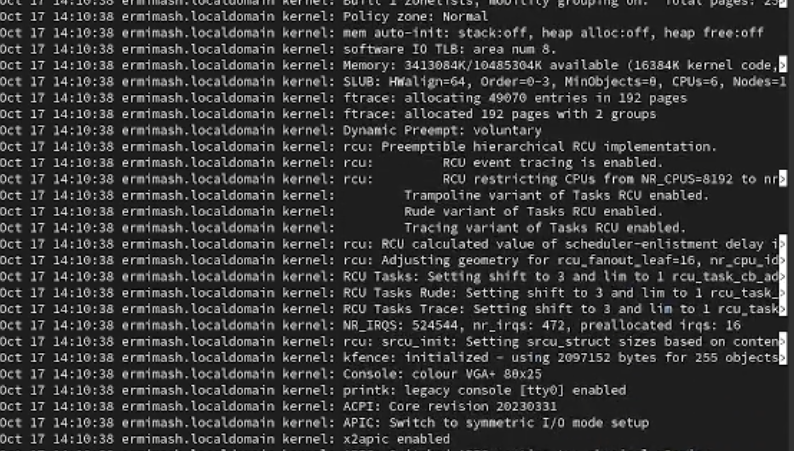


Рис. 7: Журнал с событиями с момента запуска

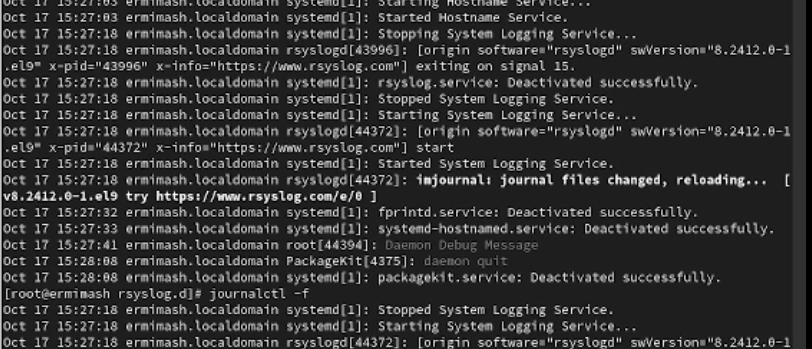


Рис. 8: Журналы без пейджера и в реальном времени

Для использования фильтрации просмотра конкретных параметров журнала введите - journalctl и дважды нажмите клавишу Tab (рис. 9)

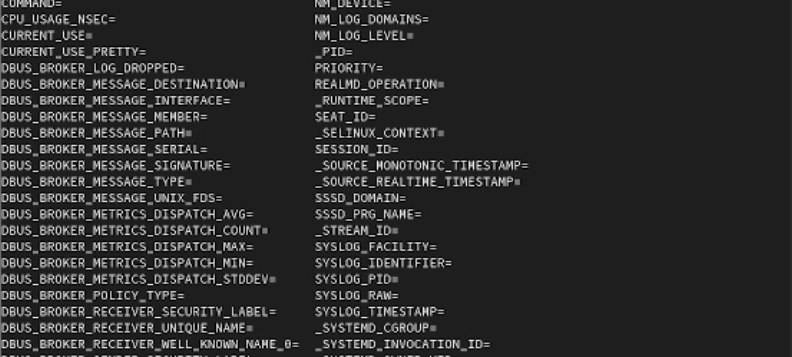


Рис. 9: Фильтрация

Просмотрите события для UID0: - journalctl \_UID=0 Для отображения последних 20 строк журнала введите: - journalctl -n 20 Для просмотра только сообщений об ошибках введите: (рис. 10) - journalctl -p err Для просмотра всех сообщений со вчерашнего дня введите: - journalctl –since yesterday

Если вы хотите показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используйте: - journalctl –since yesterday -p err Если вам нужна детальная информация, то используйте: - journalctl -o verbose Для просмотра дополнительной информации о модуле sshd введите: - journalctl \_SYSTEMD\_UNIT=sshd.service

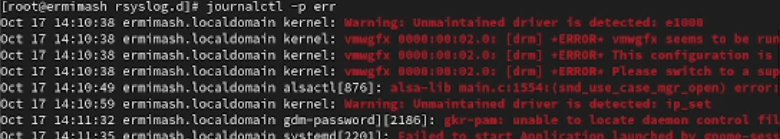


Рис. 10: Сообщения об ошибках

1. Постоянный журнал journald Запустите терминал и получите полномочия администратора. Создайте каталог для хранения записей журнала: (рис. 11)

* mkdir -p /var/log/journal Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию: (рис. **¿fig:0111?**)
* chown root:systemd-journal /var/log/journal
* chmod 2755 /var/log/journal Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: (рис. 11)
* killall -USR1 systemd-journald

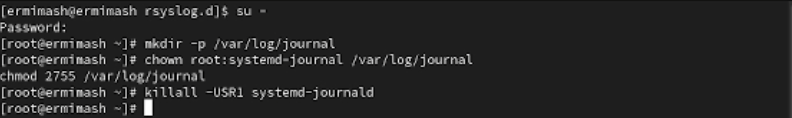


Рис. 11: Каталог для хранения записей журнала

Если вы хотите видеть сообщения журнала с момента последней перезагрузки, используйте: (рис. 12) - journalctl -b

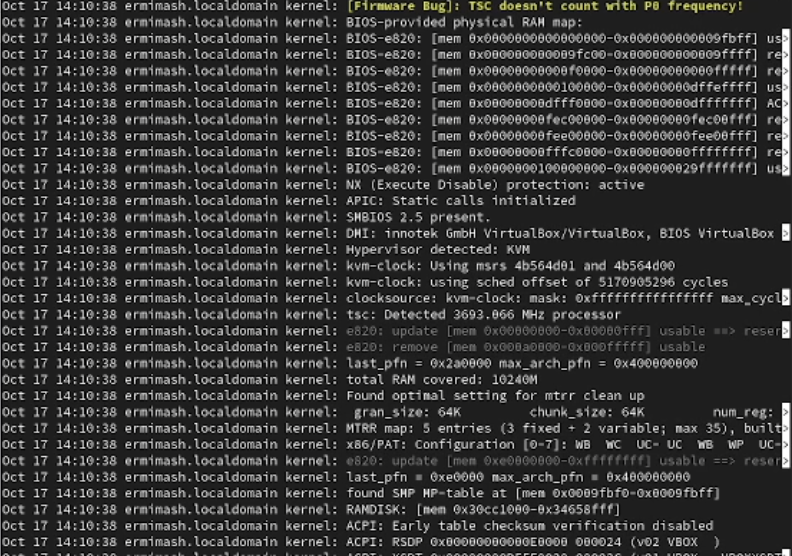


Рис. 12: Журнал с момента посл. перезагрузки

# 3 Контрольные вопросы

1. /etc/rsyslog.conf
2. /var/log/secure
3. Неделя
4. info.\* - /var/log/messages.info
5. tail -f /var/log/messages
6. journalctl \_PID=1 -since “2025-02-01 09:00:00” –until “2025-02-01 15:00:00”
7. journalctl - b
8. Запустите терминал и получите полномочия администратора: su – Создайте каталог для хранения записей журнала:

* mkdir -p /var/log/journal Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию:
* chown root:systemd-journal /var/log/journal
* chmod 2755 /var/log/journal Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду:
* killall -USR1 systemd-journald

# 4 Выводы

Получены навыки работы с журналами мониторинга различных событий в системе.