Отчет о лабораторной работе

Лабораторная работа №7

Казначеев Сергей Ильич

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

Для начала откроем три вклдки терминала и в каждом из них получим полномочия администратора рис. 1).

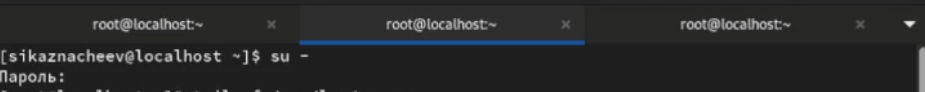


Рис. 1: 1

Теперь во второй вкладке пропишем команду tail -f /var/log/messages чтобы вывести события в реальном времени.После чего перейдем в 3 терминал и попробуем зайти в супер пользователя введя неправильный пароль и у нас во 2 терминале появится сообщение «FAILED SU (to root) username …». (рис. 2).

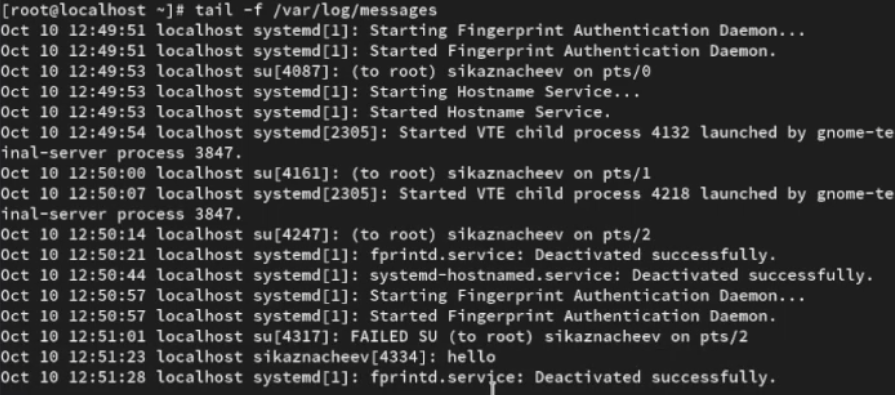


Рис. 2: 2

После в 3 терминале введем из оболочки пользователя logger hello (рис.3).

3

Рис. 3: 3

Далее открываем второй терминал и проверям то что hello записалось (рис. 4).

4

Рис. 4: 4

Затем введем команду tail -n 20 /var/log/secure чтобы увидить сообщения, которые ранее были зафиксированы во время ошибки (рис. 5).

5

Рис. 5: 5

В первой вкладке установим httpd (рис. 6).

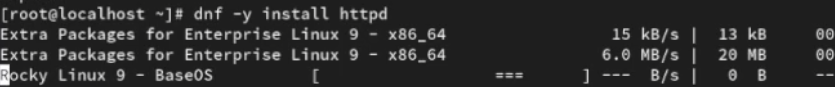


Рис. 6: 6

После окончания процесса установки запустим веб-службу (рис. 7).

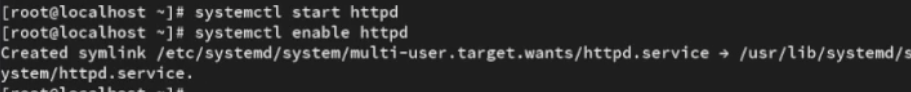


Рис. 7: 7

После во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-служб командой tail -f /var/log/httpd/error\_log (рис. 8).



Рис. 8: 8

Далее в 3 терминале запишем в файл конфигурации /etc/httpd/conf/httpd.conf в конце добавим ErrorLog syslog:local1 (рис. 9).

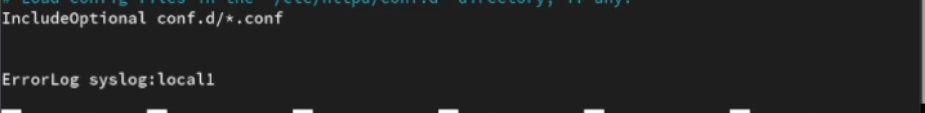


Рис. 9: 9

После чего переходим в каталог /etc/rsyslog.d и создаем файл мониторинга событий веб-службы (рис. 10).

10

Рис. 10: 10

Далее открыв его на редактировании запишем local1.\* -/var/log/httpd-error.log (рис. 11).



Рис. 11: 11

После чего переходим в первую вкладку терминала и перезагружаем концигурацию rsyslogd и веб-службу (рис. 12).

12

Рис. 12: 12

После в третьей вкладке терминала создайем отдельный файл концигурации для мониторинга отладочной информации и в том же терминале вводим echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf

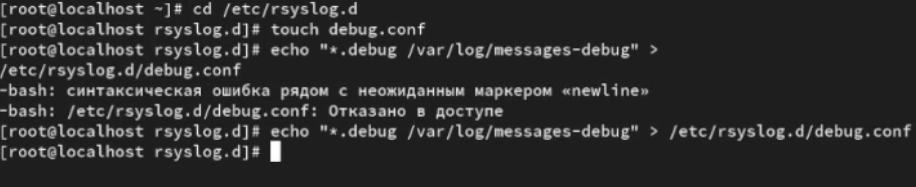


Рис. 13: 13

Затем в первой вкладке терминала снова перезапускаем rsyslogd (рис. 14).

14

Рис. 14: 14

Далее переходим во вторую вкладку терминала запускаем мониторинг отладочной информации tail -f /var/log/messages-debug (рис. 15).

15

Рис. 15: 15

Далее в третьей вкладке терминала введем logger -p daemon.debug “Daemon Debug Message”

16

Рис. 16: 16

Проверим это (рис. 17).

17

Рис. 17: 17

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы (рис. 18).

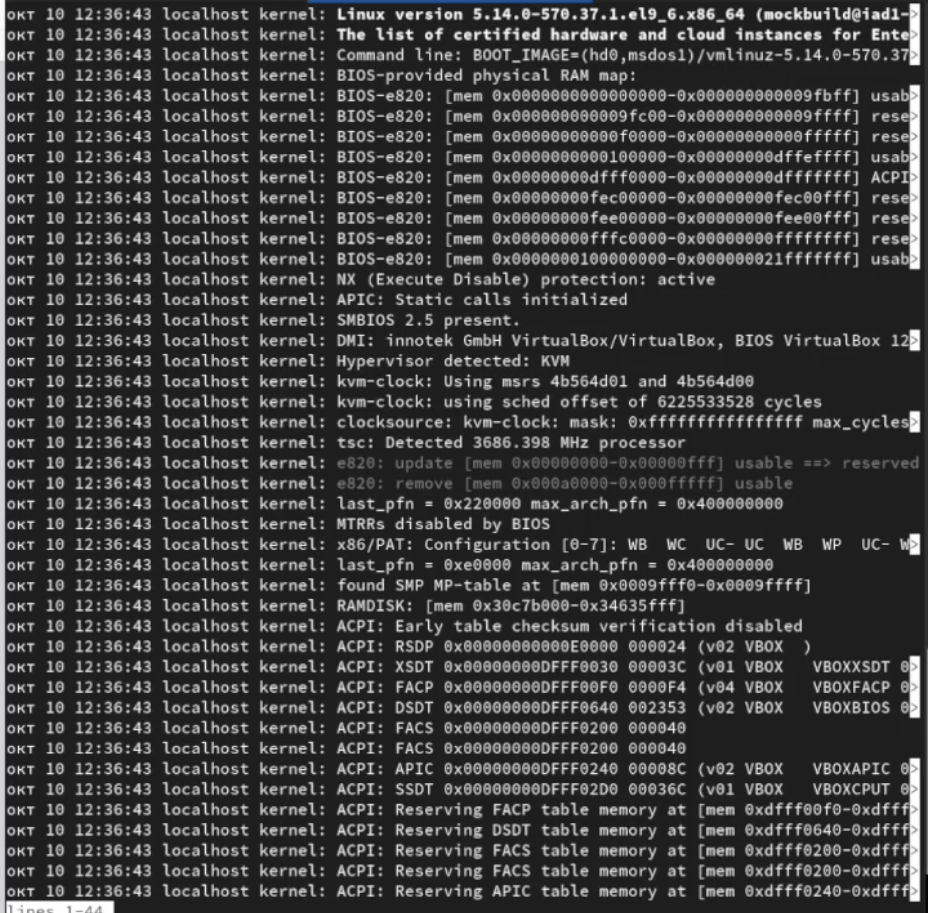


Рис. 18: 18

Затем просмотрим содержимое журнала без использования пейджера командой journalctl –no-pager и просмотрим журнал в реальном времени journalctl -f (рис. 19).

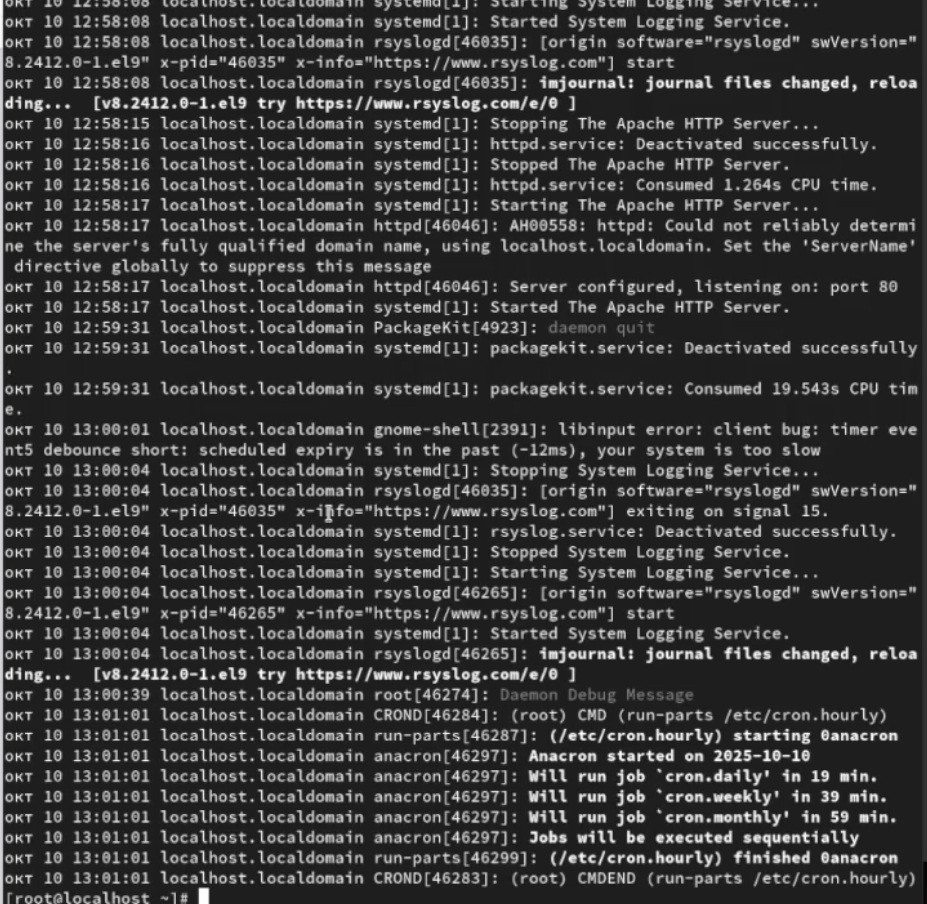


Рис. 19: 19

После чего используем фильтрацию просмотра конкретных параметров журнала введя команду journalctl и дважды нажав на tab

20

Рис. 20: 20

Пробуем просмотреть события для uid0

21

Рис. 21: 21

После чего запустим journalctl -n 20 для просмотра только сообщений об ошибке используем комаду journalctl -p err

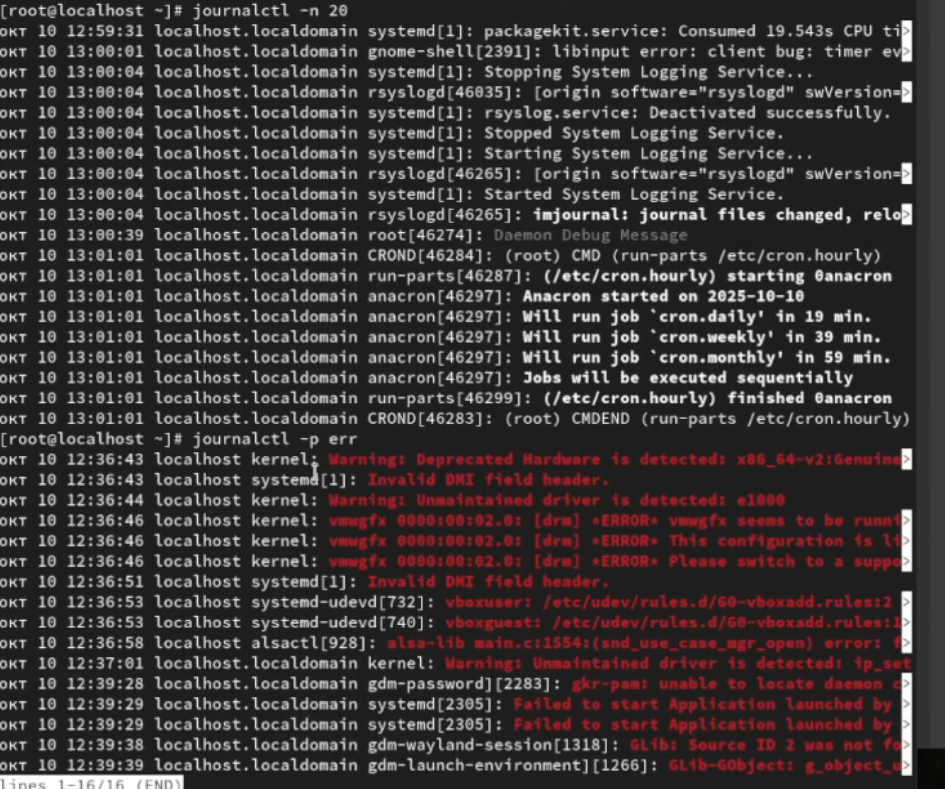


Рис. 22: 22

Теперь просмотрим сообщейния вчерашнего дня введя команду journalctl –since yesterday

23

Рис. 23: 23

Затем выведем все сообщения с ошибкой приоритета которые были зафиксированы со вчерашнего дня

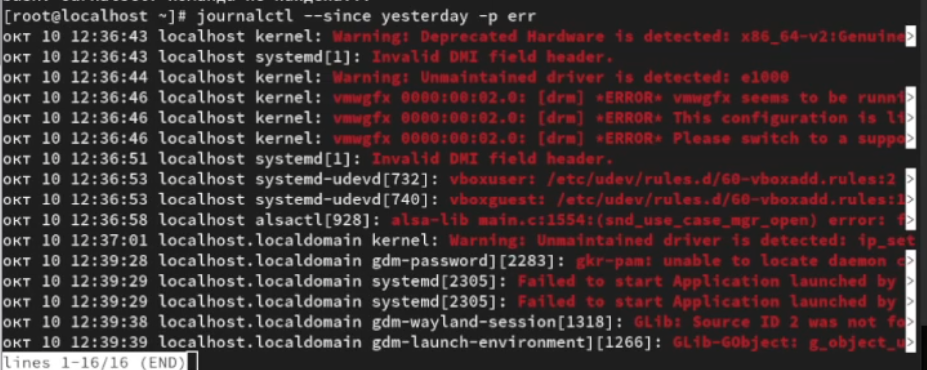


Рис. 24: 24

Затем выведем детальную информацию с помощью команды journalctl -o verbose

25

Рис. 25: 25

Далее просмотрим дополнительную информацию о модуле sshd введя команду journalctl \_SYSTEMD\_UNIT=sshd.service

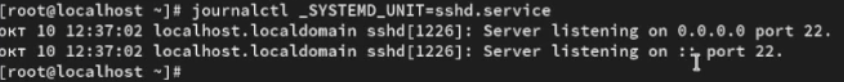


Рис. 26: 26

После чего откроем новый терминла и создадим новый каталог и скорректируем его права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию и для принятия изменений необходимо перезагрузить систему или использовать команду killall SR1 systemd-journald



Рис. 27: 27

Теперь журнал systemd теперь постоянный и можем проверить это командой journalctl -b

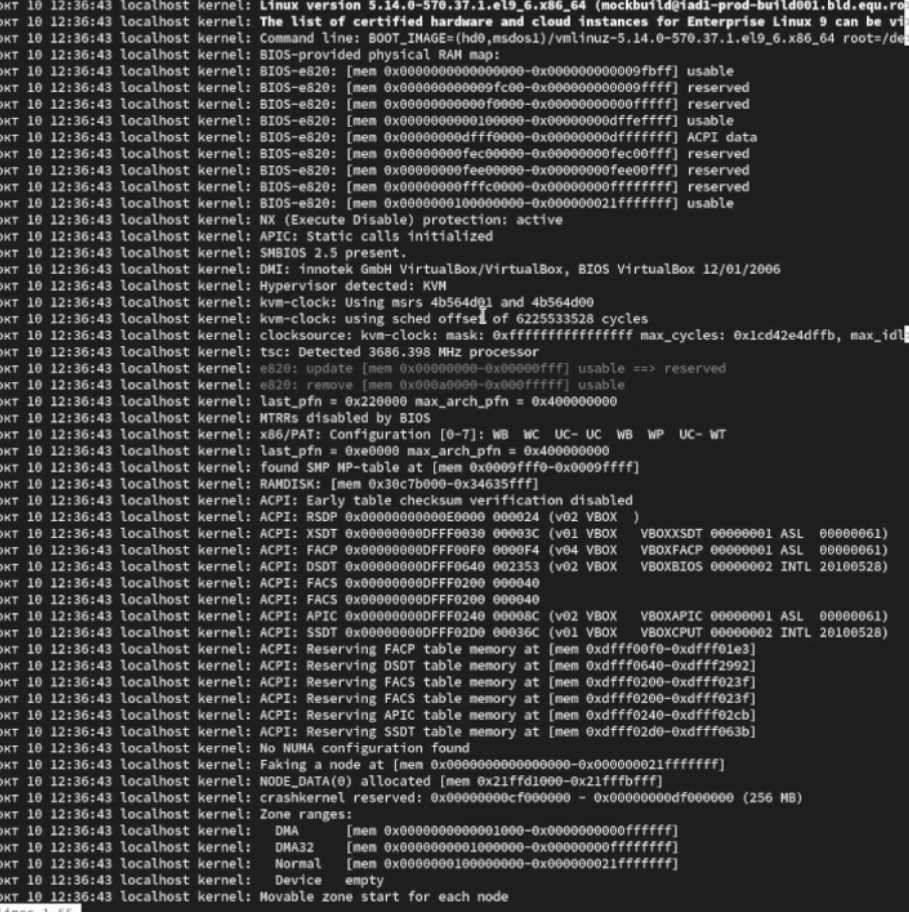


Рис. 28: 27

# 3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Ответ - файл /etc/rsyslog.conf

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

Ответ - файл журнала айнтефекации /var/log/auth.log

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

Ответ - период ротации журналов по умолчанию раз в неделю

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

Ответ - строку /var/log/message.info

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

Ответ - команда tail -f /var/log/syslog

1. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

Ответ - команада journalctl \_PID=1 –since “9:00” –until “15:00”

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

Ответ - команда journalctl -b

1. Какая процедура позволяет сделать журнал journald постоянным?

Ответ - команда создать каталог и перезапустить службу mkdir -p /var/log/journal systemctl restart systemd-journald

# 4 Выводы

В результате выполнения лабораторной работы я получил навыки работы с журналами мониторинга различных событий в системе