Отчет по лабораторной работе №7

Управление журналами событий в системе

Сидорова Арина Валерьевна

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

## 2.1 Мониторинг журнала системных событий в реальном времени

Запустим три вкладки терминала и в каждом из них получим полномочия администратора.

На второй вкладке терминала запустим мониторинг системных событий в реальном времени. (рис. 1)

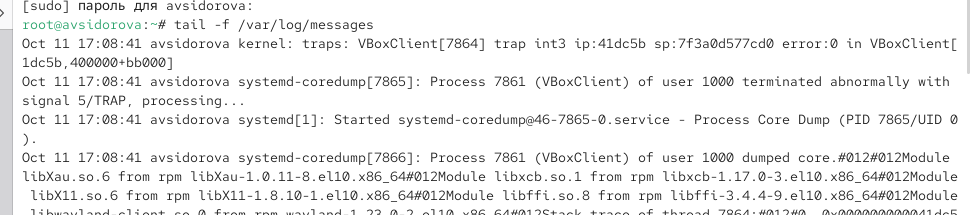


Рис. 1: мониторинг

В третьей вкладке терминала вернемся к учётной записи своего пользователя (достаточно нажать Ctrl + d ) и попробуем получить полномочия администратора, но введем неправильный пароль. Обратим внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username …». Отображаемые на экране сообщения также фиксируются в файле /var/log/messages.

В третьей вкладке терминала из оболочки пользователя введем logger hello (рис. 2)

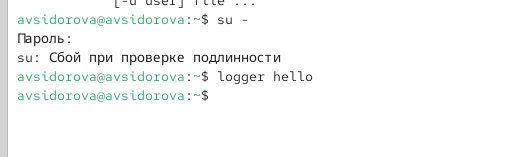


Рис. 2: logger hello

Во второй вкладке терминала с мониторингом остановим трассировку файла сообщений мониторинга реального времени, используя Ctrl + c . Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов). Мы увидите сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды su. (рис. 3)

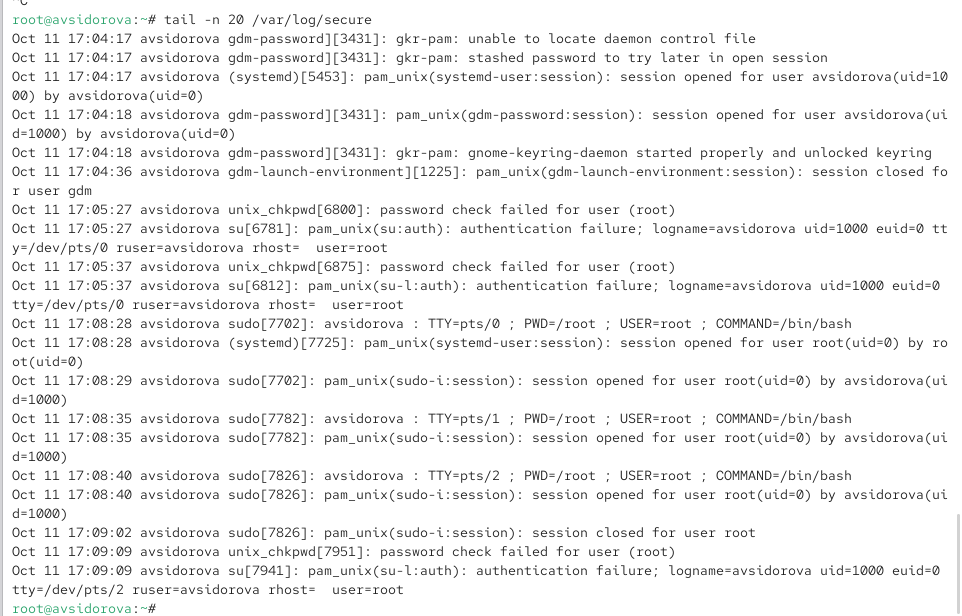


Рис. 3: tail -n 20 /var/log/secure

## 2.2 Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache (рис. 4)

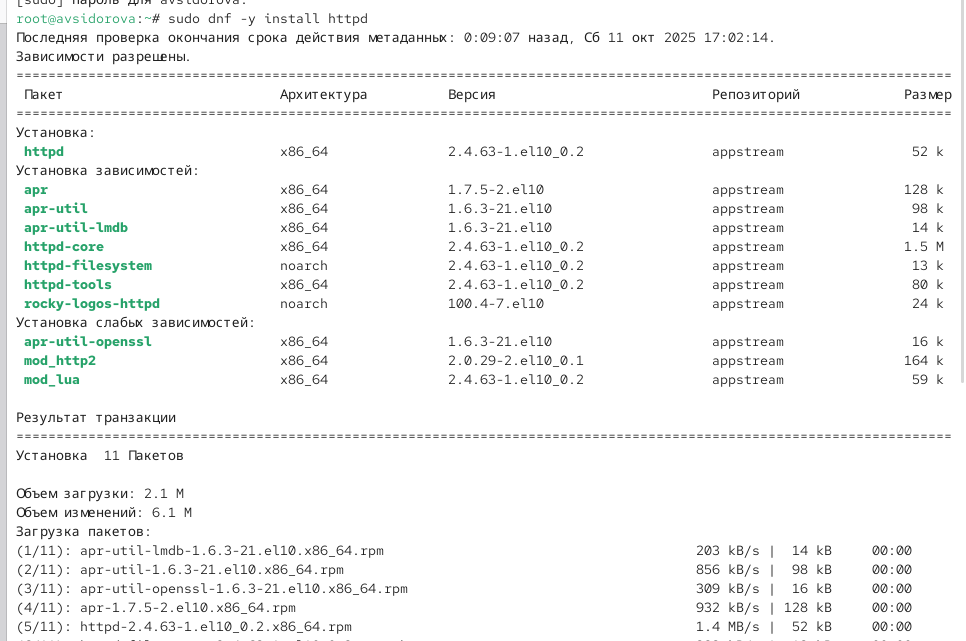


Рис. 4: Apache

После окончания процесса установки запустим веб-службу (рис. 5)

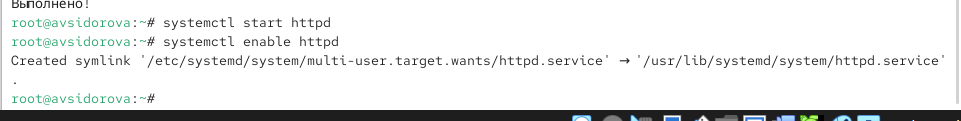


Рис. 5: system start, enable

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы (рис. 6)

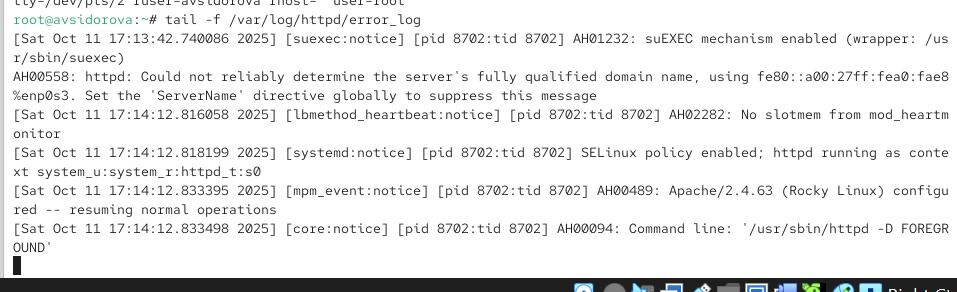


Рис. 6: error\_log

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавим строку (рис. 7)

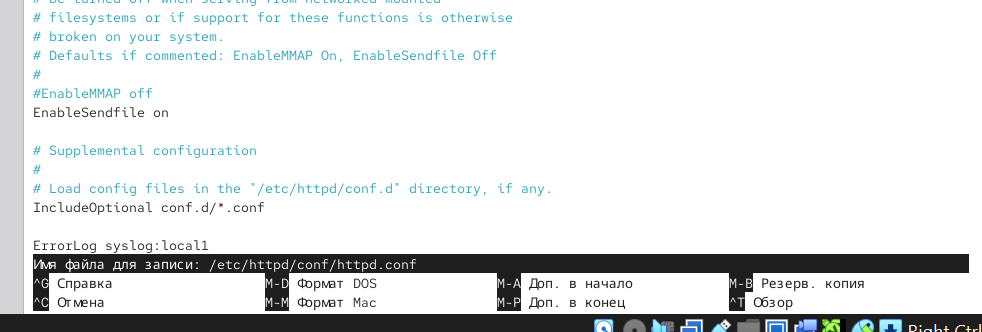


Рис. 7: errorlog syslog:local1

Здесь local0 — local7 — это «настраиваемые» средства (объекты), которые syslog предоставляет пользователю для регистрации событий приложения в системном журнале.

В каталоге /etc/rsyslog.d создадим файл мониторинга событий веб-службы: (рис. 8)



Рис. 8: touch httpd.conf

Открыв его на редактирование, пропишем в нём (рис. 9)

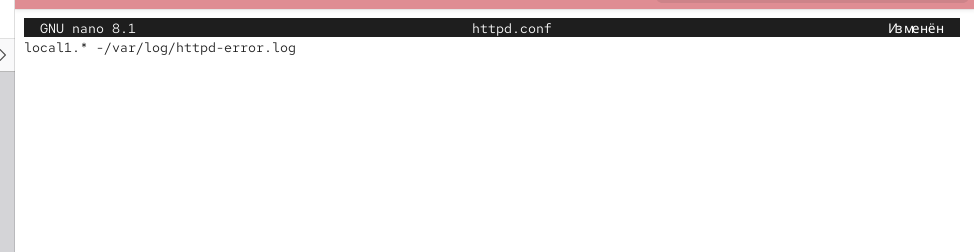


Рис. 9: local1. \* -/var/log/httpd-error.log

Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log.

Перейдем в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу: (рис. 10)

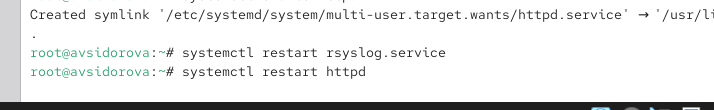


Рис. 10: restart

Все сообщения об ошибках веб-службы теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени, используя команду tail с соответствующими параметрами, или непосредственно просматривая указанный файл.

В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации: (рис. 11)



Рис. 11: touch debug.conf

В первой вкладке терминала снова перезапустим rsyslogd: (рис. 12)

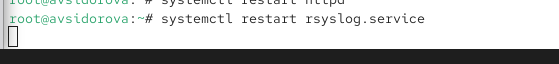


Рис. 12: restart

Во второй вкладке терминала запустим мониторинг отладочной информации: (рис. 13)

tail -f /var/log/messages-debug

Рис. 13: tail -f /var/log/messages-debug

В третьей вкладке терминала введем: (рис. 14)

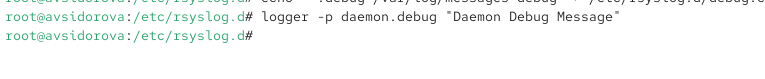


Рис. 14: logger -p

В терминале с мониторингом посмотрим сообщение отладки.

## 2.3 Использование journalctl

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: journalctl (рис. 15)

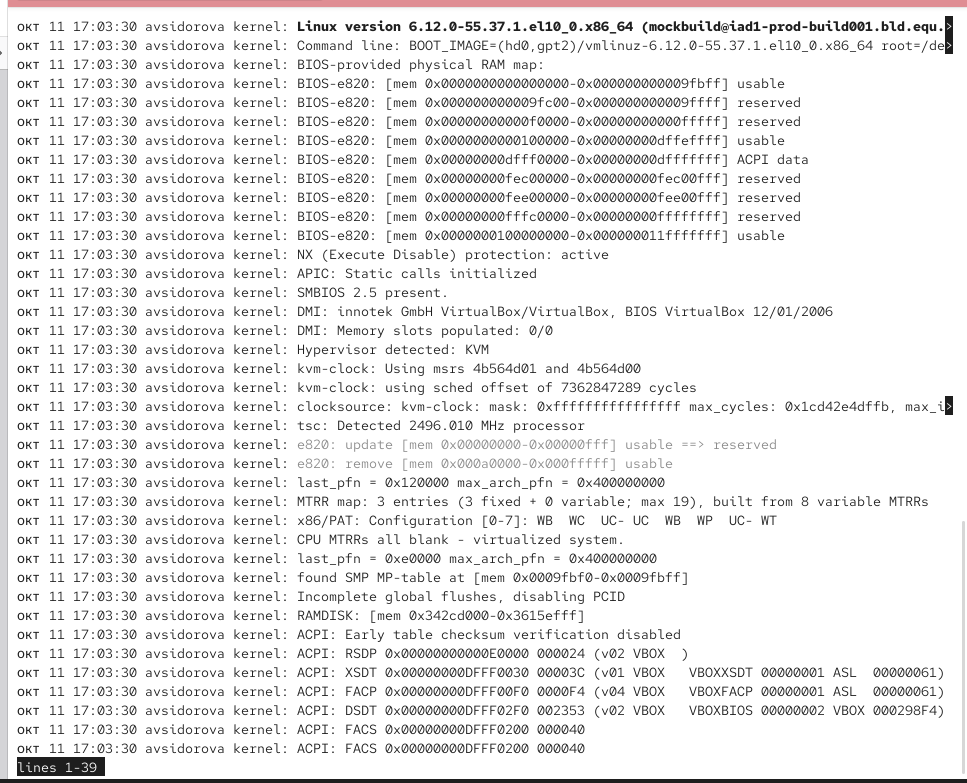


Рис. 15: journalctl

Просмотр содержимого журнала без использования пейджера: journalctl –no-pager (рис. 16)

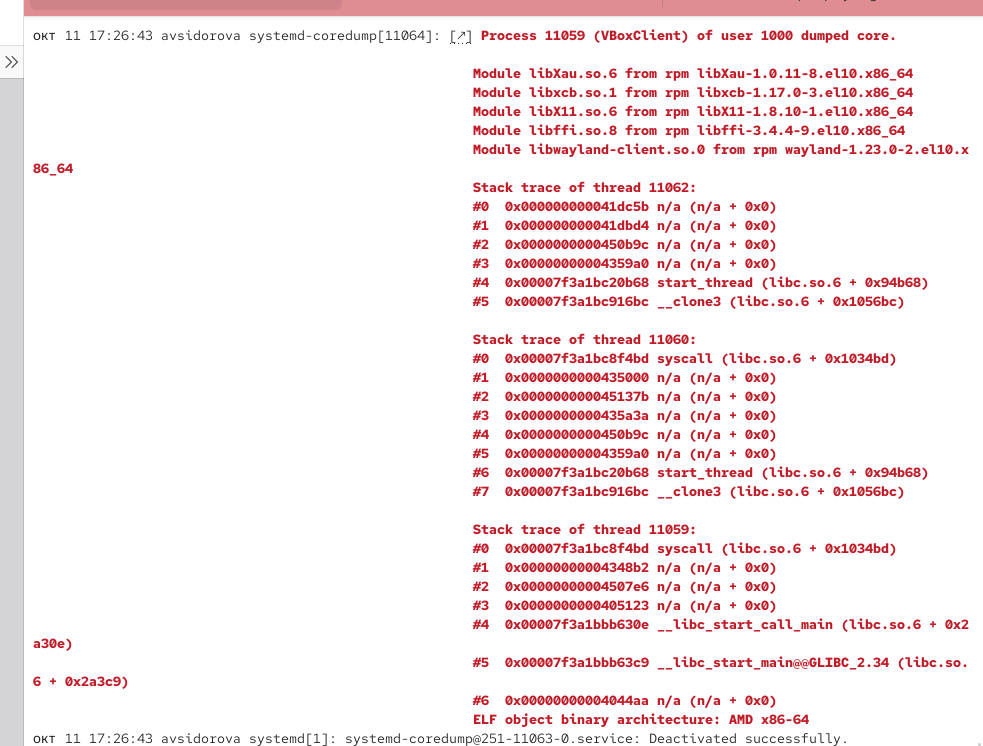


Рис. 16: journalctl –no-pager

Режим просмотра журнала в реальном времени: journalctl -f Используем Ctrl + c для прерывания просмотра. (рис. 17)

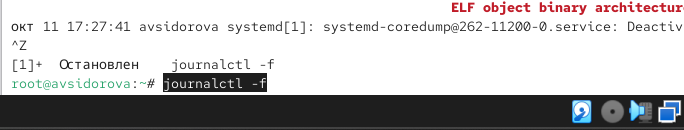


Рис. 17: journalctl -f

Для использования фильтрации просмотра конкретных параметров журнала введем journalctl и дважды нажмите клавишу Tab .

Просмотрим события для UID0: journalctl \_UID=0 (рис. 18)



Рис. 18: journalctl \_UID=0

Для отображения последних 20 строк журнала введем journalctl -n 20 (рис. 19)

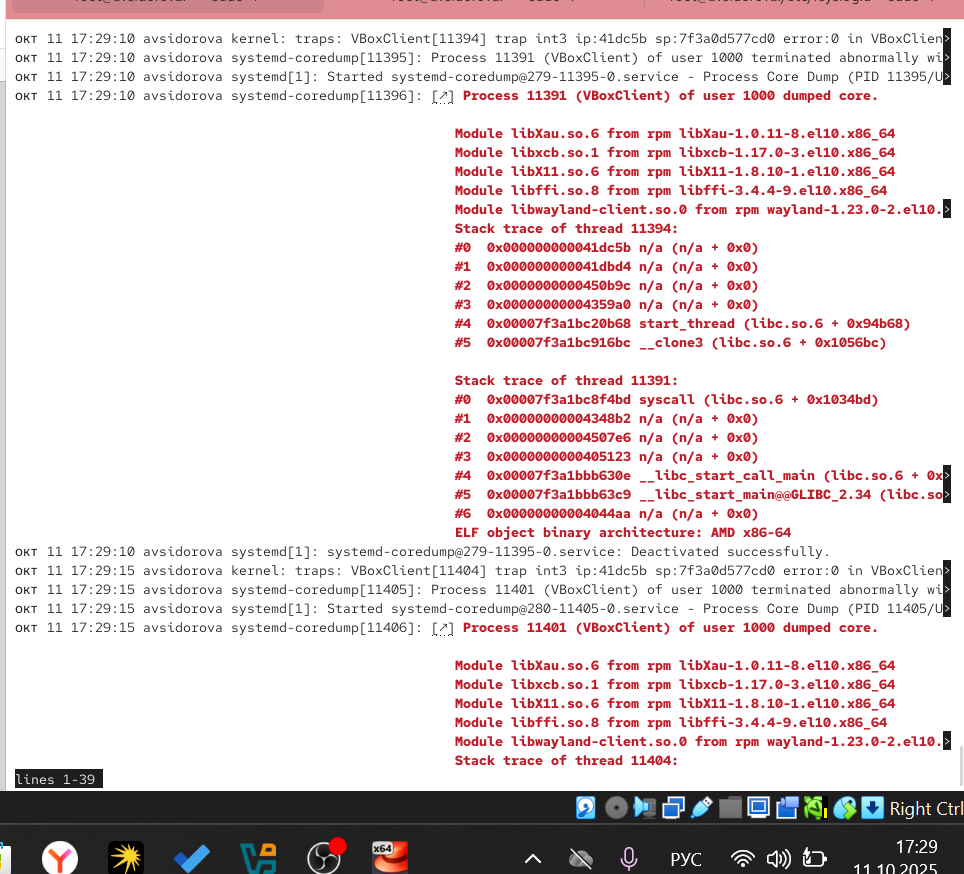


Рис. 19: journalctl -n 20

Для просмотра только сообщений об ошибках введем journalctl -p err (рис. 20)

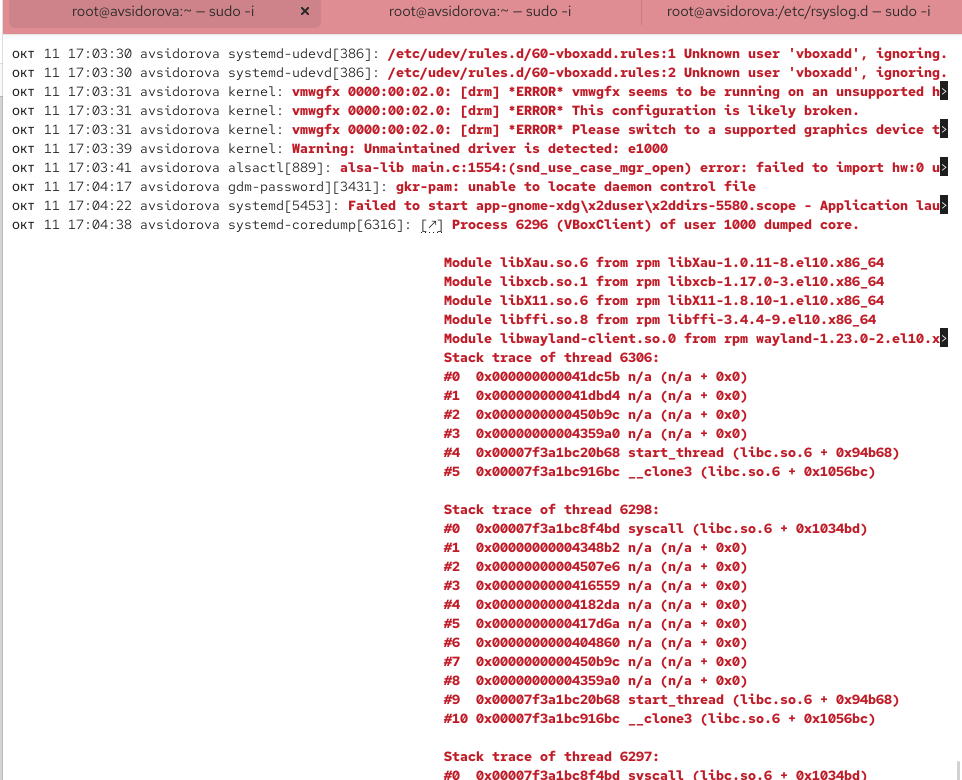


Рис. 20: journalctl -p err

Для просмотра всех сообщений со вчерашнего дня введем journalctl –since yesterday (рис. 21)

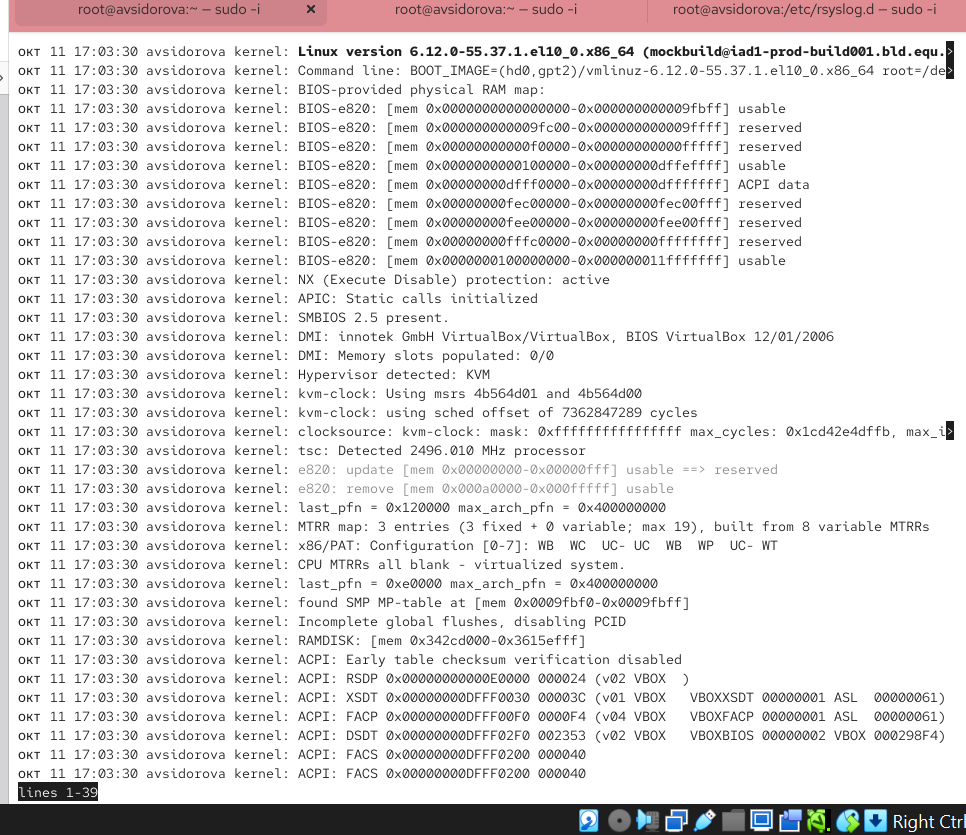


Рис. 21: journalctl –since yesterday

Используем journalctl –since yesterday -p err (рис. 22)

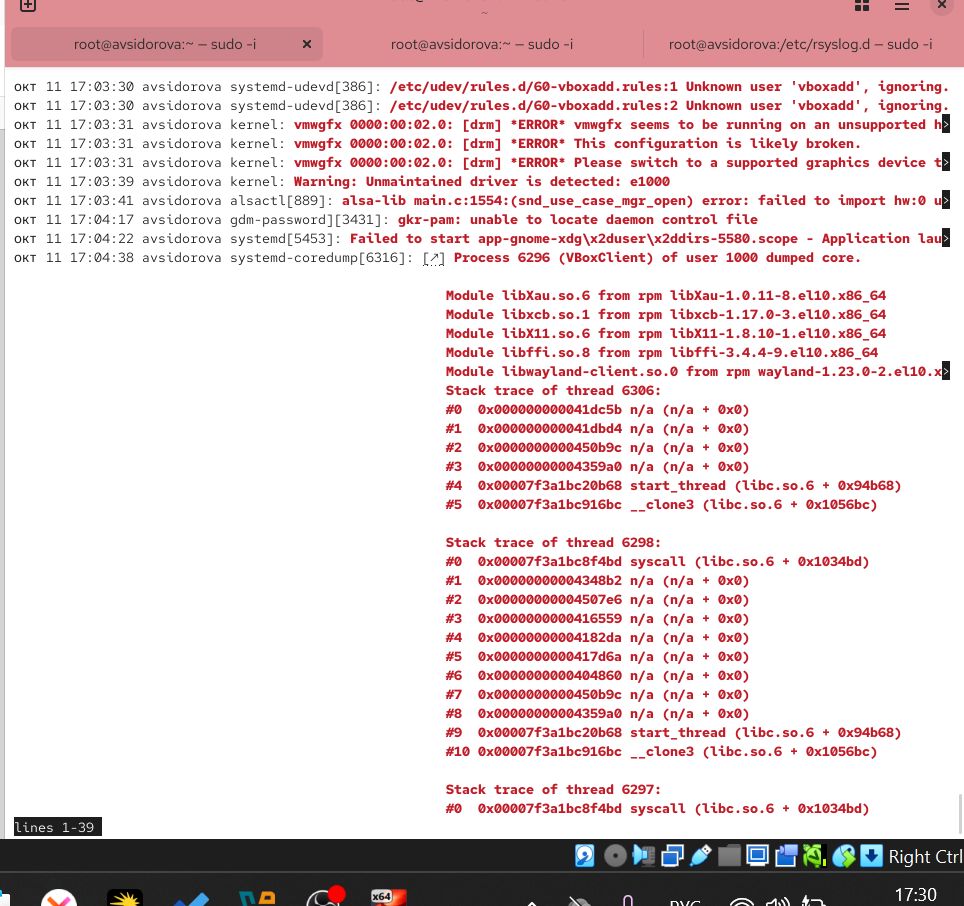


Рис. 22: journalctl –since yesterday -p err

Для детальной информации используем journalctl -o verbose (рис. 23)

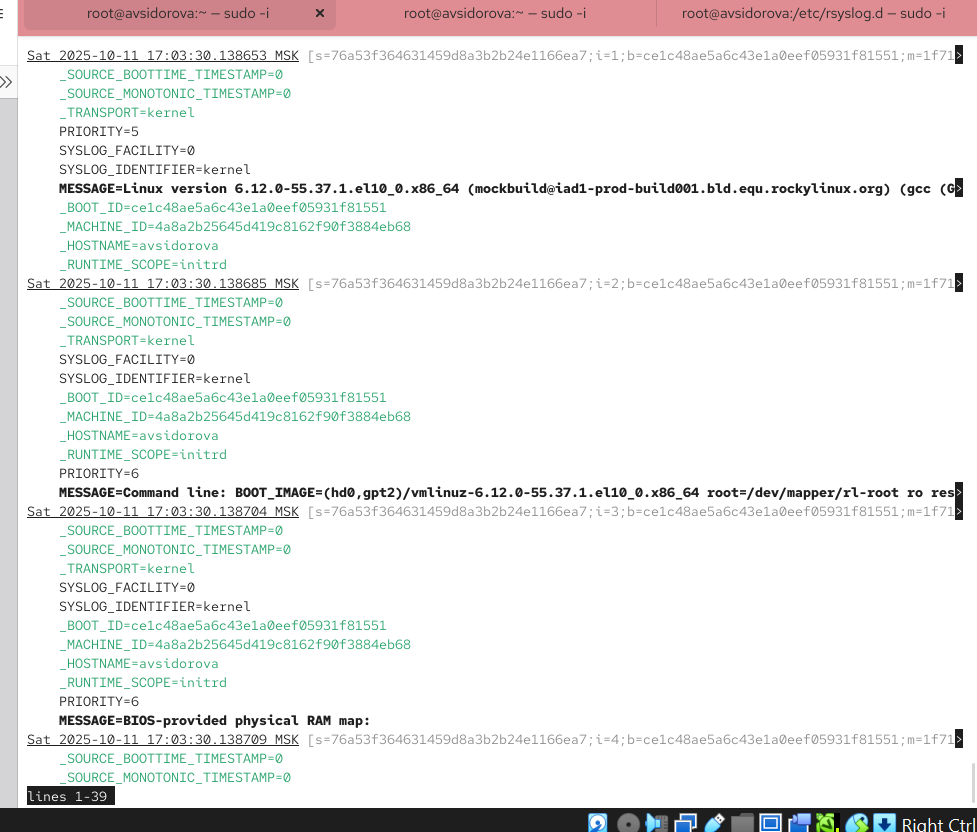


Рис. 23: journalctl -o verbose

Для просмотра дополнительной информации о модуле sshd введем journalctl \_SYSTEMD\_UNIT=sshd.service (рис. 24)

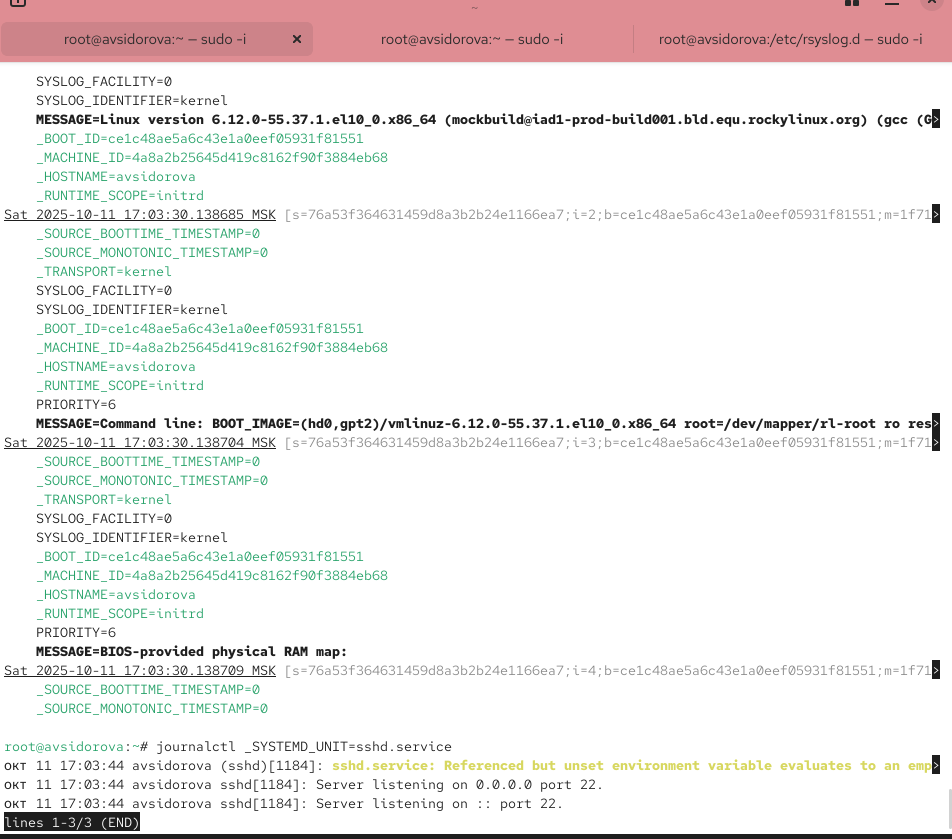


Рис. 24: journalctl \_SYSTEMD\_UNIT=sshd.service

## 2.4 Постоянный журнал journald

Запустим терминал и получим полномочия администратора. Создадим каталог для хранения записей журнала Скорректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию Для принятия изменений необходимо или перезагрузить систему Журнал systemd теперь постоянный. Мы хотим видеть сообщения журнала с момента последней перезагрузки, используем journalctl -b (рис. 25)

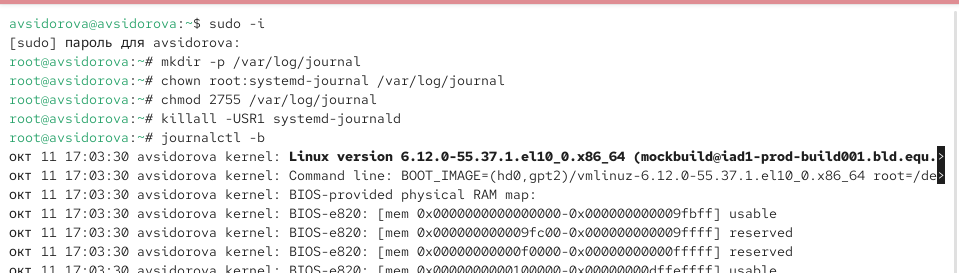


Рис. 25: Постоянный журнал journald

# 3 Ответы на контрольные вопросы

1. /etc/rsyslog.conf и файлы в /etc/rsyslog.d/
2. /var/log/secure
3. Зависит от настройки logrotate, обычно - еженедельно.
4. \*.info /var/log/messages.info
5. journalctl -f или tail -f /var/log/имя\_файла
6. journalctl \_PID=1 –since “09:00” –until “15:00”
7. journalctl -b
8. Создать каталог /var/log/journal, назначить права chown root:systemd-journal /var/log/journal, chmod 2755 /var/log/journal и перезапустить systemd-journald.

# 4 Выводы

Получили навыки работы с журналами мониторинга различных событий в системе.