Отчёт по лабораторной работе №7

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Задание

1. Продемонстрировать навыки работы с журналом мониторинга событий в реальном времени
2. Продемонстрировать навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы
3. Продемонстрировать навыки работы с journalctl
4. Продемонстрировать навыки работы с journald

# 3 Выполнение лабораторной работы

## 3.1 Мониторинг журнала системных событий в реальном времени

Запускаем три вкладки терминала и в каждой из них получаем полномочия суперпользователя, используя *su -* (рис. 1)

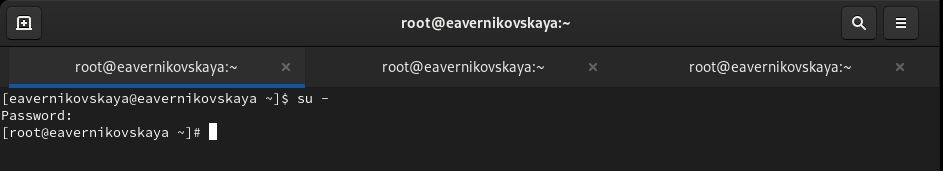


Рис. 1: Режим суперпользователя

На второй вкладке терминала запустите мониторинг системных событий в реальном времени, с помощью *tail -f /var/log/messages* (рис. 2)

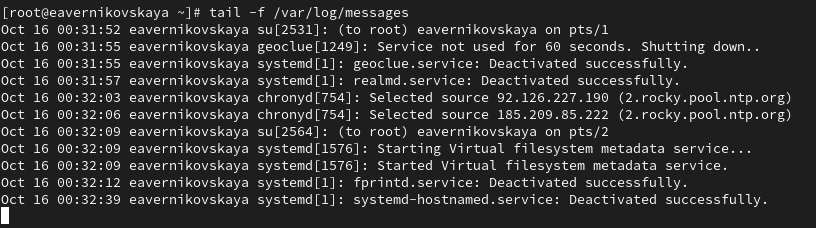


Рис. 2: Мониторинг системных событий в реальном времени

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя (для этого нажимаем ctrl+d) и пробуем получить полномочия администратора, но на этот раз вводим неправильный пароль (рис. 3)

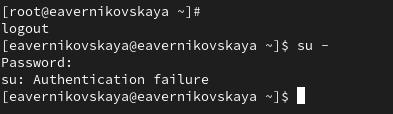


Рис. 3: Попытка получить права суперпользователя

Во второй вкладке терминала с мониторингом событий после неудачной попытки получить права администратора появится сообщение «FAILED SU (to root) username …» (рис. 4)

Сообщение о неудачной попытки получить права root

Рис. 4: Сообщение о неудачной попытки получить права root

В третьей вкладке терминала из оболочки пользователя вводим *logger hello* (рис. 5)

Послание тестового сообщения “hello”

Рис. 5: Послание тестового сообщения “hello”

Во второй вкладке терминала с мониторингом событий мы увидим сообщение, которое до этого написали с помощью *logger* (рис. 6)

Тестовое сообщение “hello”

Рис. 6: Тестовое сообщение “hello”

Во второй вкладке терминала с мониторингом останавливаем трассировку файла сообщений мониторинга реального времени, используя ctrl+c, а затем запускаем мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов), с помощью *tail -n 20 /var/log/secure*. Там мы увидим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды su (рис. 7)

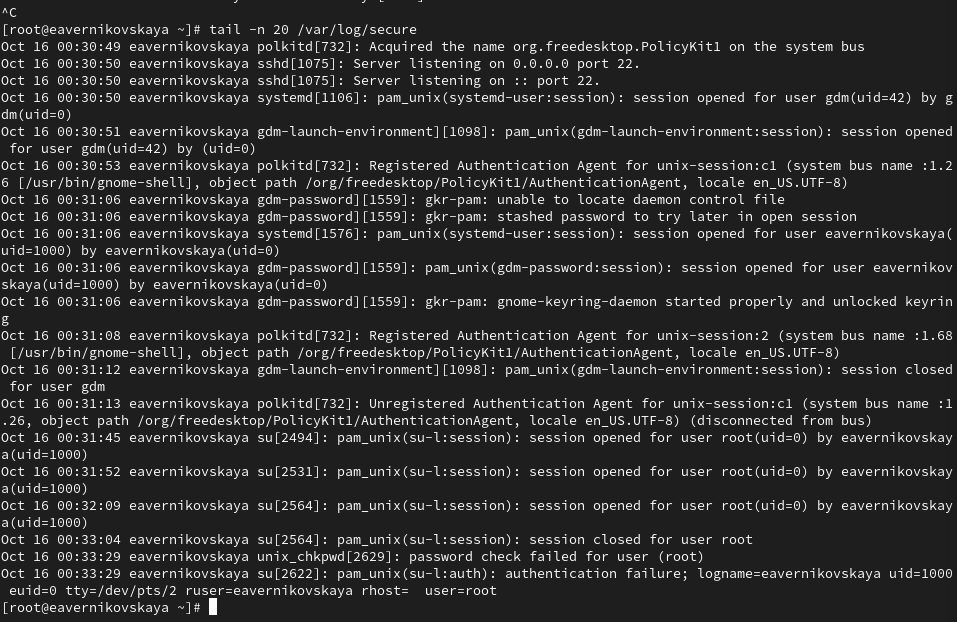


Рис. 7: Мониторинг сообщений безопасности

## 3.2 Изменение правил rsyslog.conf

По умолчанию веб-служба не регистрирует свои сообщения через rsyslog, а пишет свой собственный журнал (в каталоге /var/log/httpd). Настроим регистрацию сообщений веб-службы через syslog, создав правило, регистрирующее отладочные сообщения в отдельном лог-файле.

В первой вкладке терминала установим Apache командой *dnf -y install httpd* (рис. 8)

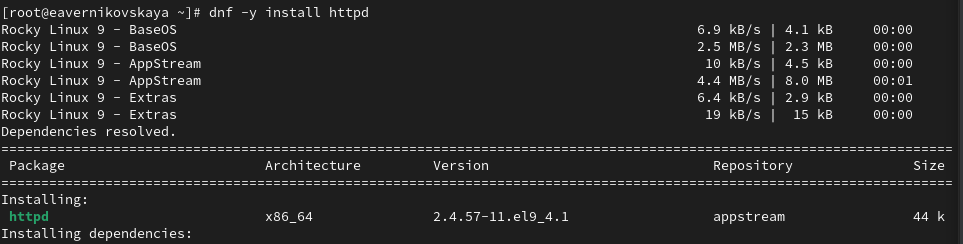


Рис. 8: Установка Apache

После окончания процесса установки запускаем веб-служб командами *systemctl start httpd* и *systemctl enable httpd* (рис. 9)

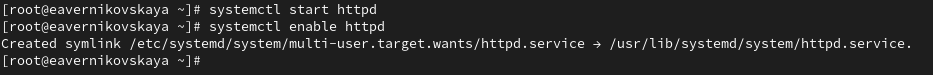


Рис. 9: Запуск службы httpd

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы, с помощью *tail -f /var/log/httpd/error\_log*. Для закрытия используем ctrl+c (рис. 10)

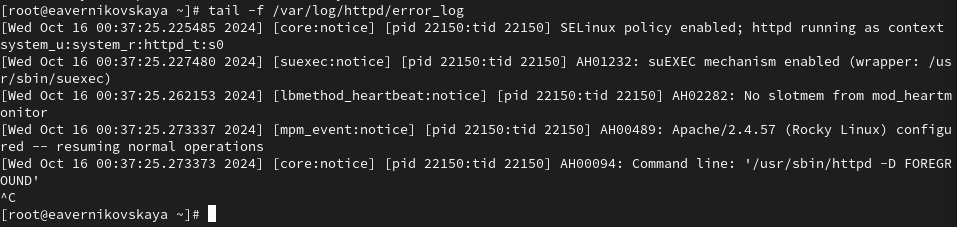


Рис. 10: Журнал сообщений об ошибках веб-службы httpd

В третьей вкладке терминала получаем полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавляем строку *ErrorLog syslog:local1*. Добавление этой строки в конец файла конфигурации изменит способ регистрации ошибок веб-сервера. Ошибки будут отправляться на систему журналирования через syslog в локальную категорию local1 (рис. 11), (рис. 12)

Получение прав пользователя root и открытие файла /etc/httpd/conf/httpd.conf

Рис. 11: Получение прав пользователя root и открытие файла /etc/httpd/conf/httpd.conf

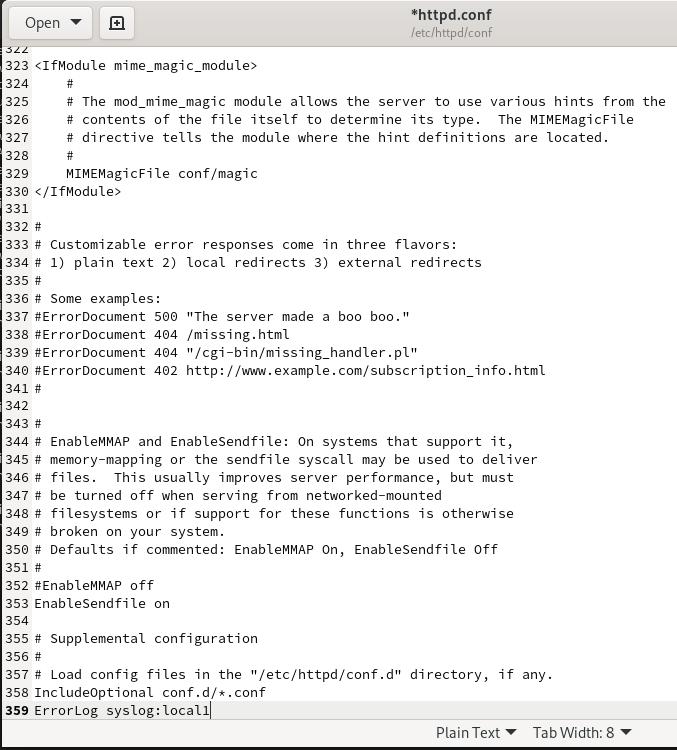


Рис. 12: Редактирование файла /etc/httpd/conf/httpd.conf

Далее в каталоге /etc/rsyslog.d создаём файл мониторинга событий веб-службы (рис. 13)

Создание файла мониторинга событий веб-службы

Рис. 13: Создание файла мониторинга событий веб-службы

Открыв его на редактирование, прописываем в нём строку 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 (рис. 14), (рис. 15)

Открытие файла /etc/rsyslog.d/httpd.conf

Рис. 14: Открытие файла /etc/rsyslog.d/httpd.conf

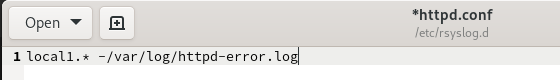


Рис. 15: Редактирование файла /etc/rsyslog.d/httpd.conf

Переходим в первую вкладку терминала и перезагружаем конфигурацию rsyslogd и веб-службу команжой *systemctl 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 (рис. 16)

Перезагрузка конфигурации rsyslogd и веб-службы

Рис. 16: Перезагрузка конфигурации rsyslogd и веб-службы

В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации (рис. 17)

Создание отдельного файла конфигурации для мониторинга отладочной информации

Рис. 17: Создание отдельного файла конфигурации для мониторинга отладочной информации

В этом же терминале пишем команду echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf (рис. 18)

Ввод нужной команды

Рис. 18: Ввод нужной команды

В первой вкладке терминала снова перезапускаем rsyslogd (рис. 19)

Перезапуск rsyslogd

Рис. 19: Перезапуск rsyslogd

Во второй вкладке терминала запускаем мониторинг отладочной информации с помощью *tail -f /var/log/messages-debug* (рис. 20)

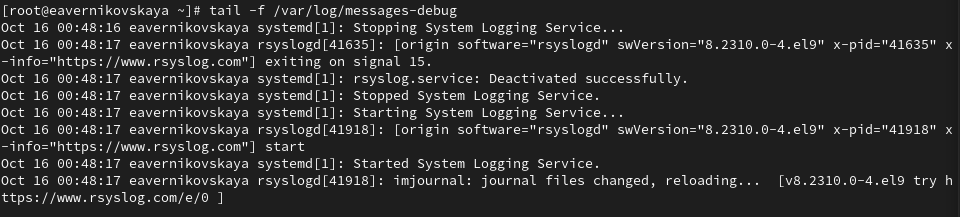


Рис. 20: Мониторинг отладочной информации

В третьей вкладке терминала вводим *logger -p daemon.debug “Daemon Debug Message”* (рис. 21)

Создание тестового сообщения уровня debug

Рис. 21: Создание тестового сообщения уровня debug

После этого мы увидим в терминале с мониторингом отладочной информации наше сообщение, которое мы создали с помощью *logger* (рис. 22)

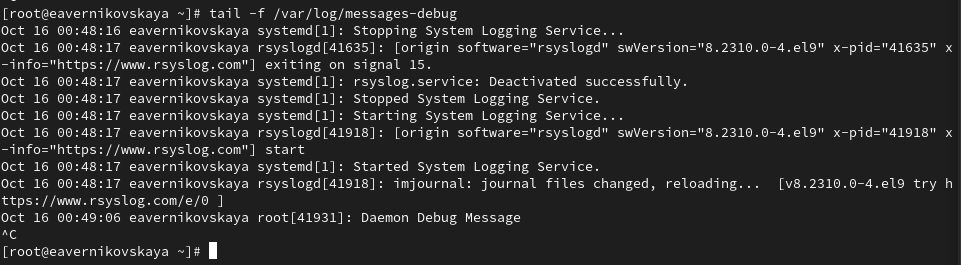


Рис. 22: Тестовое сообщение уровня debug

## 3.3 Использование journalctl

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы с помощью *journalctl* (рис. 23)

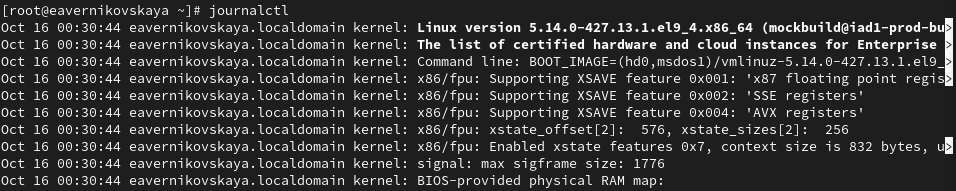


Рис. 23: Просмотр содержимого журнала событий с момента последнего запуска системы

Далее посмотрим содержимоге журнала без использования пейджера с помощью *journalctl –no-pager*. Это означает, что вывод соообщений будет отображатся сразу весь, без возможности прокручивания содержимого (рис. 24)

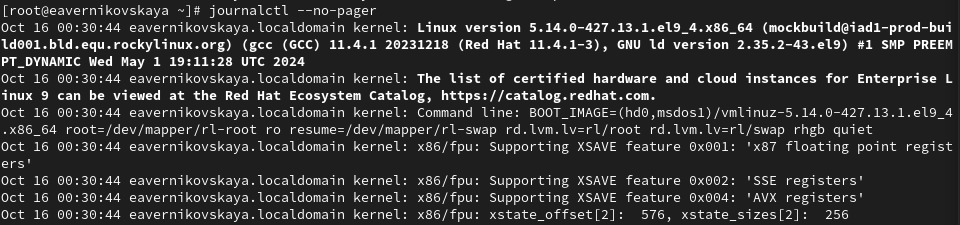


Рис. 24: Просмотр содержимого журнала событий без использования пейджера

Далее посмотрим журнал в реальном времени командой *journalctl -f*. Для прерывания просмотра используем также ctrl+c (рис. 25)

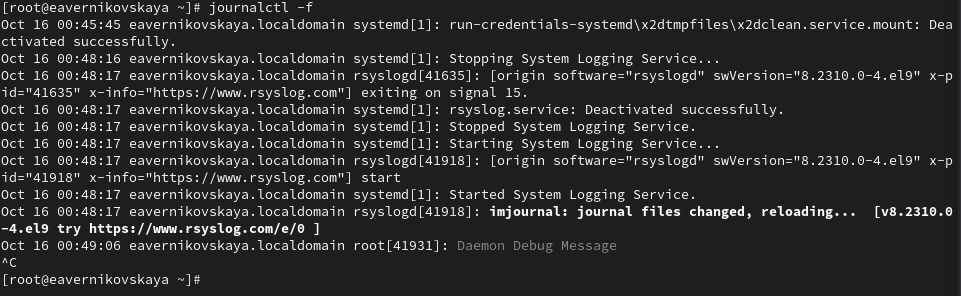


Рис. 25: Просмотр журнала в реальном времени

Для использования фильтрации просмотра конкретных параметров журнала вводим *journalctl* и дважды нажимаем на клавишу *Tab* (рис. 26)

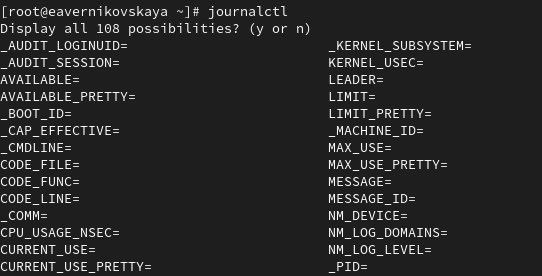


Рис. 26: Просмотр конкретных параметров. Надеюсь это то))))

Смотрим события UID0 командой \*journalctl \_UID=0\* (рис. 27)

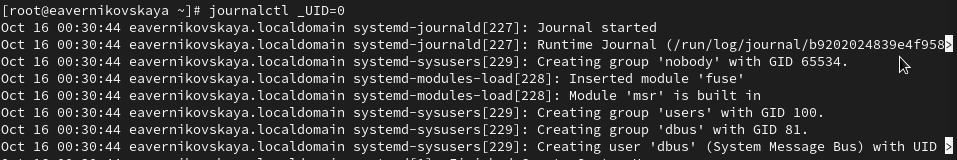


Рис. 27: События UID0

Для отображения последних 20 строк журнала вводим команду *journalctl -n 20* (рис. 28)

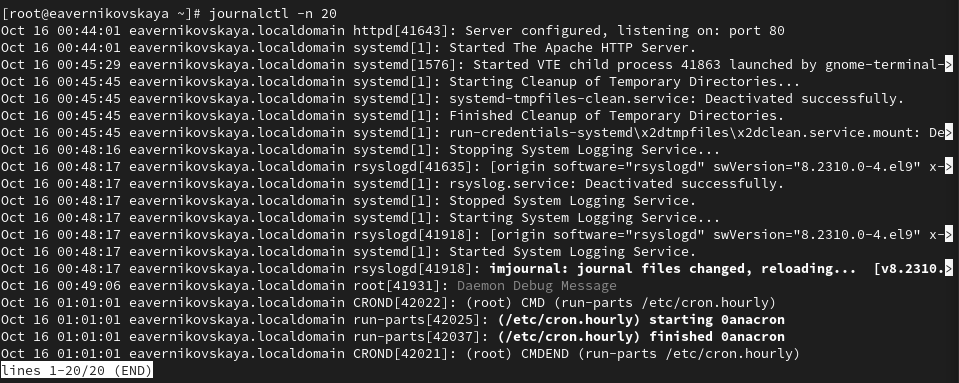


Рис. 28: Просмотр последних 20 строк журнала

Для просмотра только сообщений об ошибках вводим *journalctl -p err* (рис. 29)

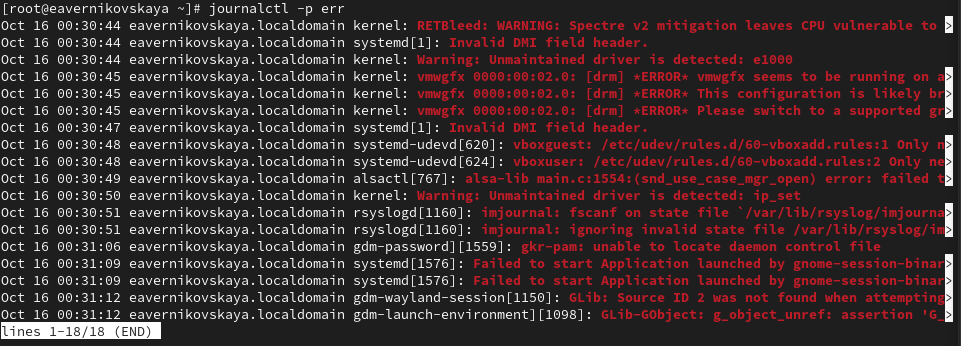


Рис. 29: Просмотр сообщений только об ошибках

Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, мы можем использовать параметры –since и –until. Обе опции принимают параметр времени в формате YYYY-MM-DD hh:mm:ss. Кроме того, мы можем использовать yesterday, today и tomorrow в качестве параметров.

Для просмотра всех сообщений со вчерашнего дня вводим *journalctl –since yesterday* (рис. 30)

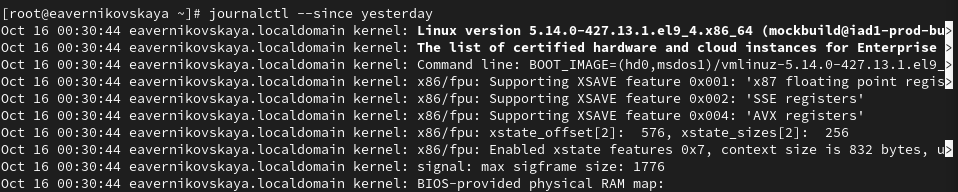


Рис. 30: Просмотр всех сообщений со вчерашнего дня

Далее просматриваем все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Для этого используем команду *journalctl –since yesterday -p err* (рис. 31)

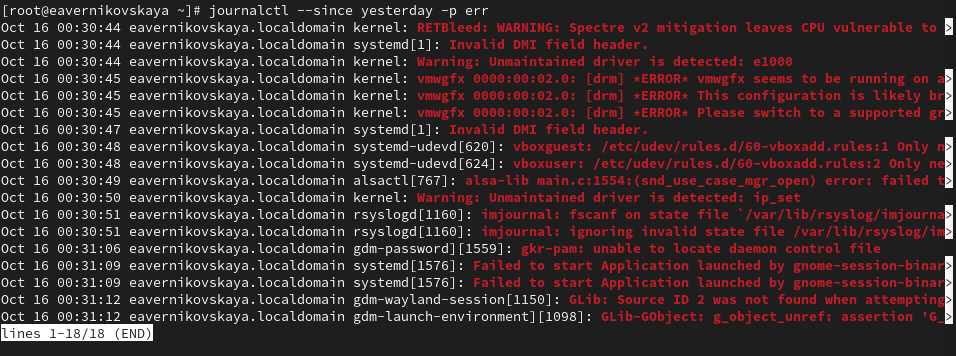


Рис. 31: Просмотр всех сообщений с ошибкой приоритета со вчерашнего дня

Посмотрим детальную информацию с помощью *journalctl -o verbose* (рис. 32)

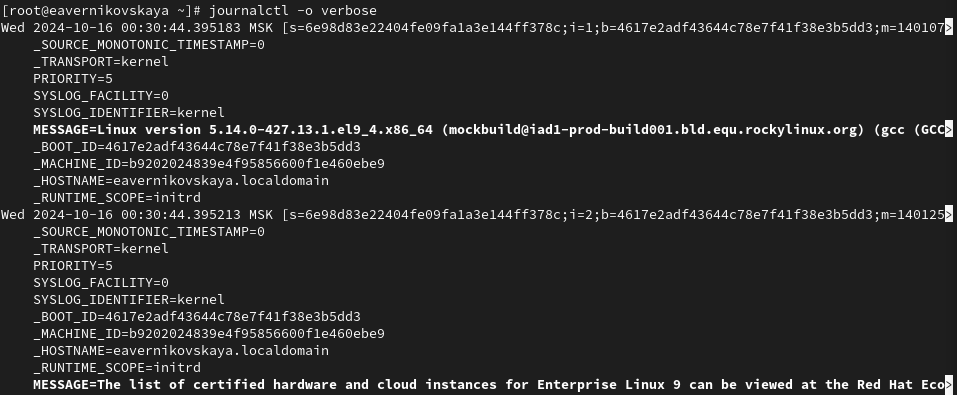


Рис. 32: Просмотр детальной информации

Для просмотра дополнительной информации о модуле sshd вводим \*journalctl \_SYSTEMD\_UNIT=sshd.service\* (рис. 33)

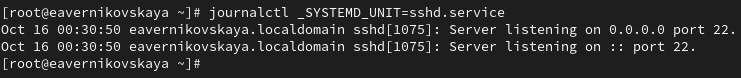


Рис. 33: Просмотр дополнительной информации о модуле sshd

## 3.4 Постоянный журнал journald

Запускаем терминал и получаем полномочия администратора (рис. 34)

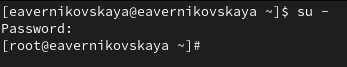


Рис. 34: Режим root

Создаём каталог для хранения записей журнала *mkdir -p /var/log/journal* (рис. 35)

Создание каталога для хранения записей журнала

Рис. 35: Создание каталога для хранения записей журнала

Скорректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Для этого введём команды *chown root:systemd-journal /var/log/journal* и *chmod 2755 /var/log/journal* (рис. 36)

Установление прав доступа для каталога /var/log/journal

Рис. 36: Установление прав доступа для каталога /var/log/journal

Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду *killall -USR1 systemd-journald*, что мы и делаем (рис. 37)

Команда killall -USR1 systemd-journald

Рис. 37: Команда killall -USR1 systemd-journald

Журнал systemd теперь постоянный. Теперь посмотрим сообщения журнала с момента последней перезагрузки с помошью команды *journalctl -b* (рис. 38)

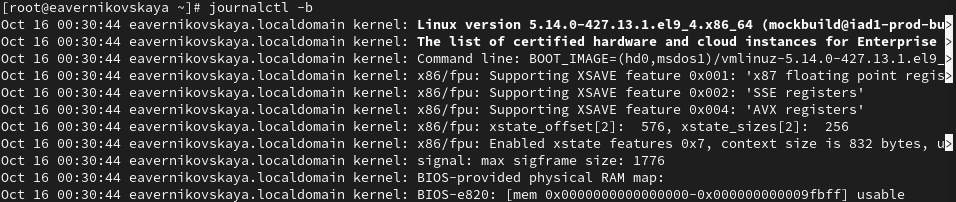


Рис. 38: Сообщения журнала с момента последней перезагрузки

# 4 Контрольные вопросы + ответы

1. Какой файл используется для настройки rsyslogd?

/etc/rsyslog.conf (рис. 39)

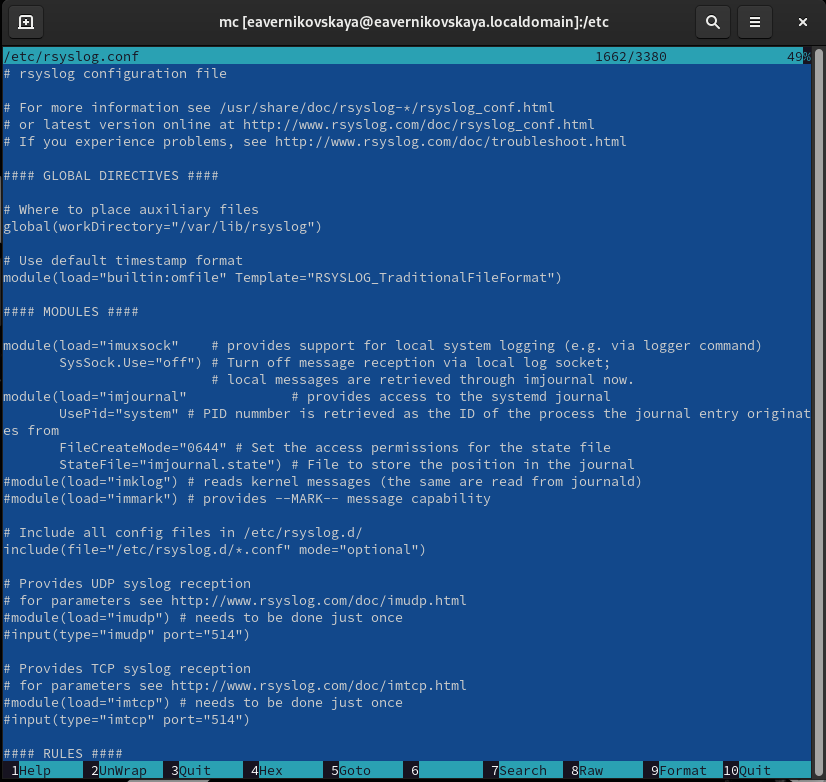


Рис. 39: Вопрос №1

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

/var/log/secure (рис. 40)

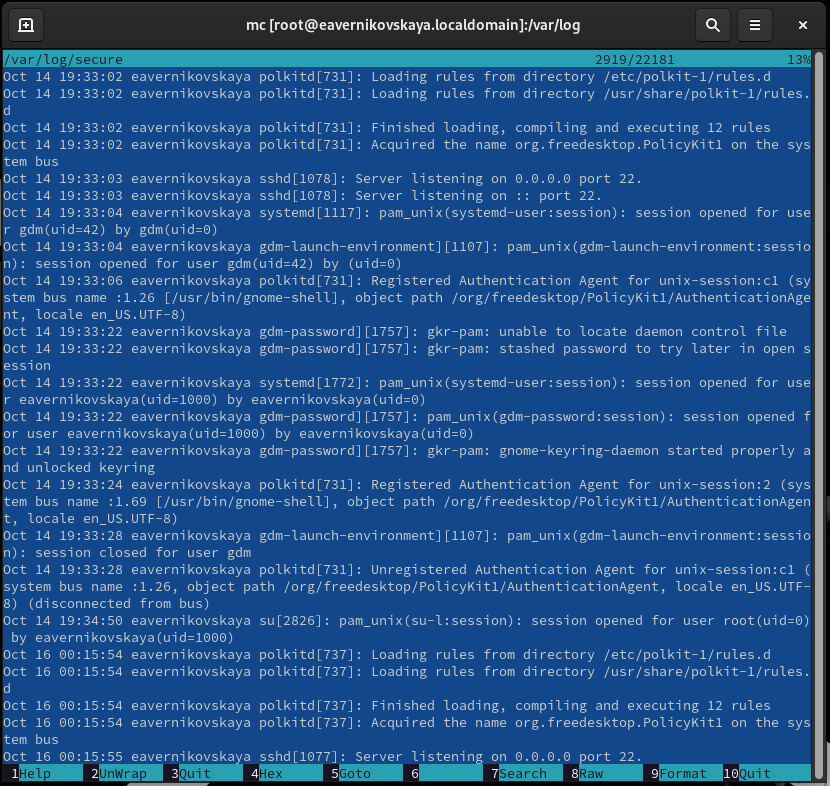


Рис. 40: Вопрос №2

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

Неделя (рис. 41)

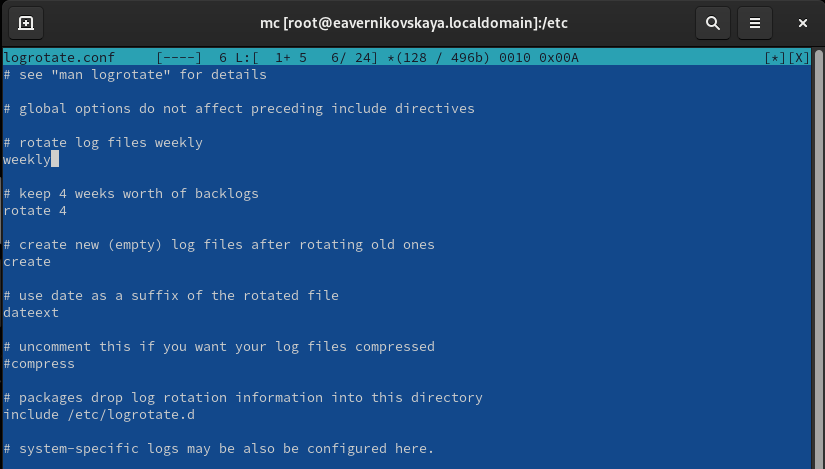


Рис. 41: Вопрос №3

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 /var/log/messages (рис. 42)

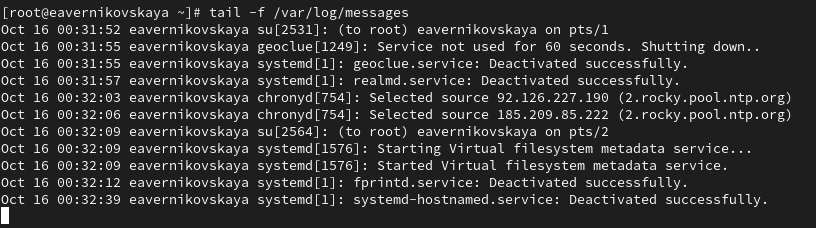


Рис. 42: Вопрос №5

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 “2024-10-16 09:00:00” –until “2024-10-16 15:00:00”

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

journalctl -b (рис. 43)

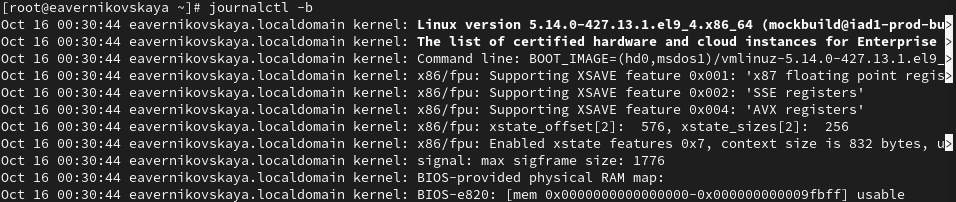


Рис. 43: Вопрос №7

1. Какая процедура позволяет сделать журнал journald постоянным?

* запустить терминал и получить права пользователя root
* создать каталог для хранения записей журнала: *mkdir -p /var/log/journal* (рис. 44)
* скорректировать права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию: *chown root:systemd-journal /var/log/journal* и *chmod 2755 /var/log/journal* (рис. 45)
* для принятия изменений используем команду *killall -USR1 systemd-journald* (рис. 46)

Вопрос №8 (1)

Рис. 44: Вопрос №8 (1)

Вопрос №8 (2)

Рис. 45: Вопрос №8 (2)

Вопрос №8 (3)

Рис. 46: Вопрос №8 (3)

# 5 Выводы

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

# 6 Список литературы

1. Лаборатораня работа №7 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/2400710/mod\_resource/content/4/008-syslog.pdf