Лабараторная работа №7

Отчет

Славинский Владислав Вадимович

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Выполнение лабораторной работы

Запустим три вкладки терминала и в каждом из них получим полномочия администратора:. (рис. 1)

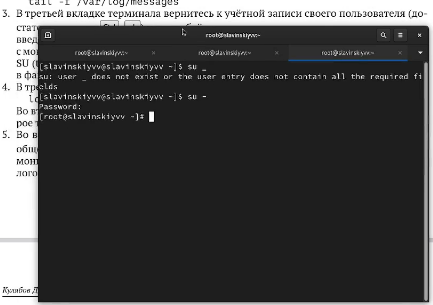


Рис. 1: Переход в режим суперпользователя

На второй вкладке терминала запустим мониторинг системных событий в реальном времени: tail -f /var/log/messages.(рис. 2)

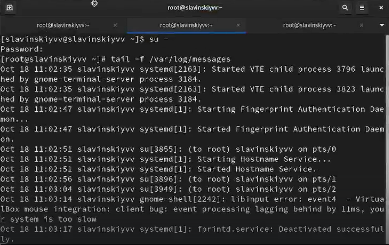


Рис. 2: Запуск мониторинга системных событий в реальном времени

В третьей вкладке терминала вернемся к учётной записи своего пользователя. Попробуем войти в режим суперпользователя, но при этом введем неправильный пароль и посмотрим вторую вкладку терминала. (рис. 3)

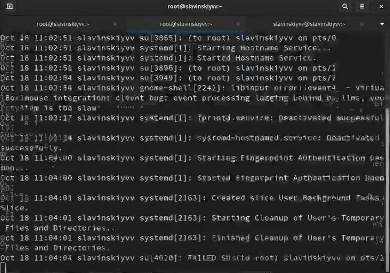


Рис. 3: Ввод неверого пароля

В третьей вкладке терминала из оболочки пользователя введем logger hello. (рис. 4)

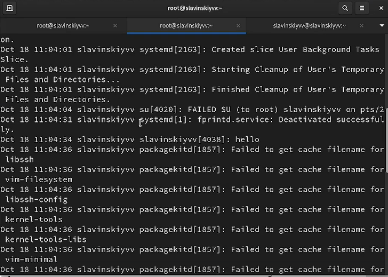


Рис. 4: Logger hello

Во второй вкладке терминала с мониторингом остановите трассировку файла сообщений мониторинга реального времени, используя ctrl+c. Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов): tail -n 20 /var/log/secure. (рис. 5)

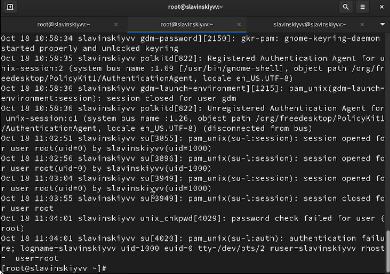


Рис. 5: Запуск мониторига сообщений безопасности

В первой вкладке терминала установим Apache: dnf -y install httpd (рис. 6)

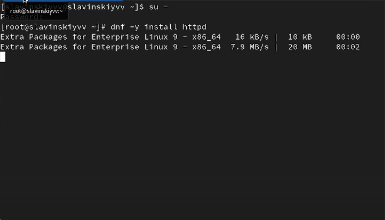


Рис. 6: Установка Apache

После окончания процесса установки запустим веб-службу: systemctl start httpd, systemctl enable httpd. (рис. 7)

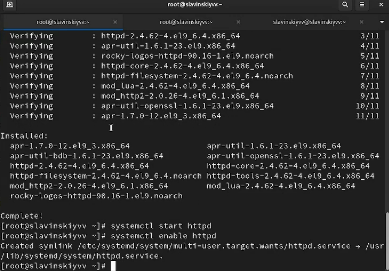


Рис. 7: Запуск веб-службы

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: tail -f /var/log/httpd/error\_log.(рис. 8)

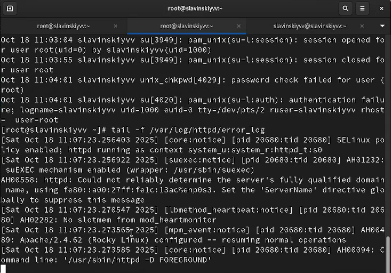


Рис. 8: Просмотр журнала с сообщениями об ошибках веб службы

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавим следующую строку: ErrorLog syslog:local1.(рис. 9)

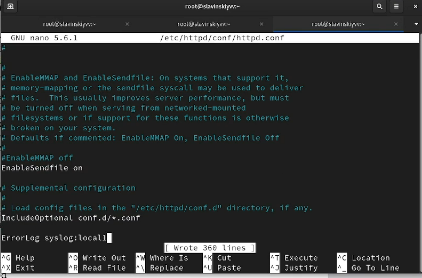


Рис. 9: Добавление строки в файле конфигурации

В каталоге /etc/rsyslog.d создадим файл мониторинга событий веб-службы:cd /etc/rsyslog.d, touch httpd.conf. Потом пропишем в нем local1.\* -/var/log/httpd-error.log. Эта строка позволит отправлять все сообщения, получаемые для объекта local1 в файл /var/log/httpd-error.log. (рис. 10)

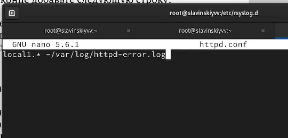


Рис. 10: Создание файла мониторига событий веб-службы

Перейдем в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу:systemctl restart rsyslog.service, systemctl restart httpd. (рис. 11)

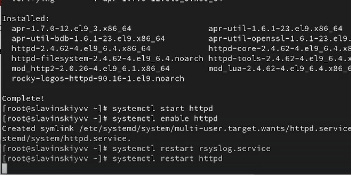


Рис. 11: Перезагрузка конфигурации rsyslogd и веб-службы

В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации: cd /etc/rsyslog.d, touch debug.conf. И в этом же терминале введем echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf. (рис. 12)

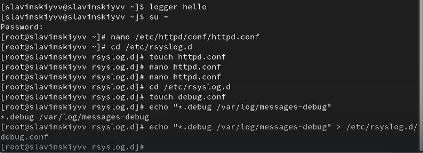


Рис. 12: Создание отдельного файла конфигурации для мониторинга отладочной информации

В первой вкладке терминала снова перезапустим rsyslogd: systemctl restart rsyslog.service. (рис. 13)

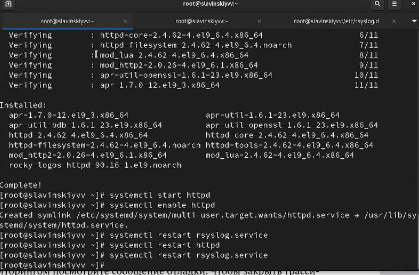


Рис. 13: Перезапуск rsyslog

Во второй вкладке терминала запустим мониторинг отладочной информации: tail -f /var/log/messages-debug.(рис. 14)

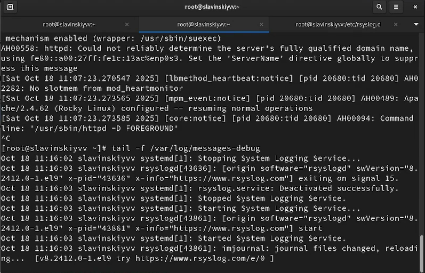


Рис. 14: Запуск мониторинга отладочной информации

В третьей вкладке терминала введем: logger -p daemon.debug “Daemon Debug Message”.(рис. 15)

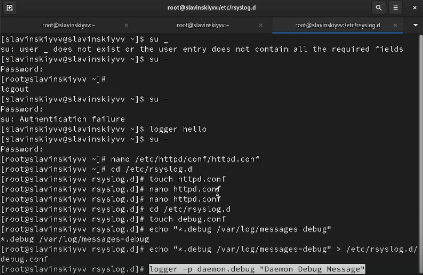


Рис. 15: Ввод команды

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: journalctl.(рис. 16)

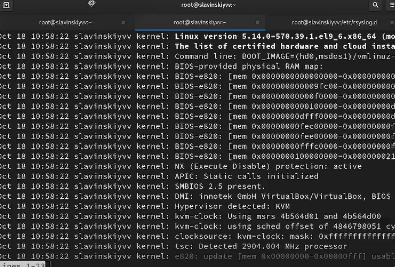


Рис. 16: Содержимое журнала с событиями с момента последнего запуска системы

Просмотр содержимого журнала без использования пейджера: journalctl –no-pager.(рис. 17)

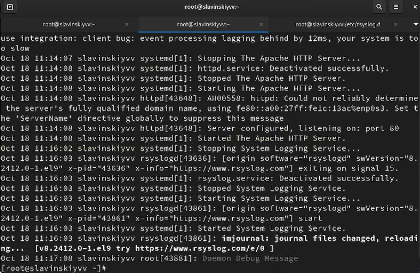


Рис. 17: Просмотр журнала без использования пейджера

Режим просмотра журнала в реальном времени: journalctl -f.(рис. 18)

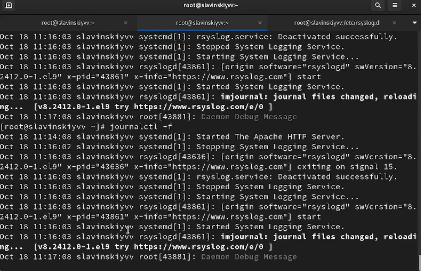


Рис. 18: Просмотр журнала в режиме реального времени

Для использования фильтрации просмотра конкретных параметров журнала введем journalctl и дважды нажмем клавишу tab.(рис. 19)

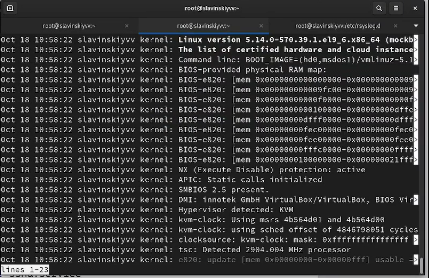


Рис. 19: Использование фильтрации просмотра конкретных параметров журнала

Просмотрим события для UID0: journalctl \_UID=0.(рис. 20)

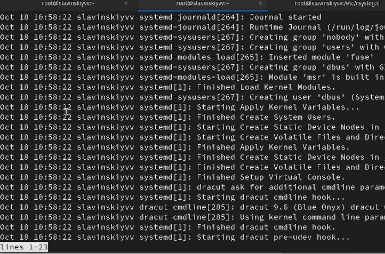


Рис. 20: Просмотр сыбтия для uid 0

Для отображения последних 20 строк журнала введем: journalctl -n 20.(рис. 21)

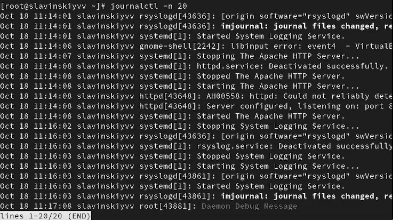


Рис. 21: Отображение последних 20 строк журнала

Для просмотра только сообщений об ошибках введем: journalctl -p err.(рис. 22)

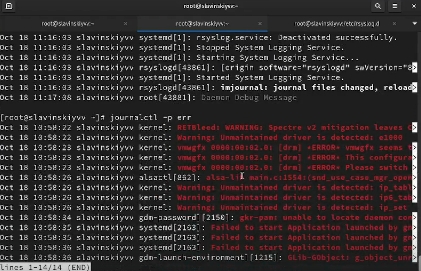


Рис. 22: Просмотр только сообщений об ошибках

Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, мы можем использовать параметры –since и –until. Введем например команду, для просмотра всех сообщений со вчерашнего дня через –since: journalctl –since yesterday.(рис. 23)

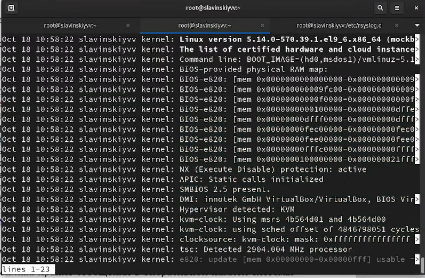


Рис. 23: Просмотр сообщений за определенный период времени

Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафик- сированы со вчерашнего дня, то мы используем: journalctl –since yesterday -p err.(рис. 24)

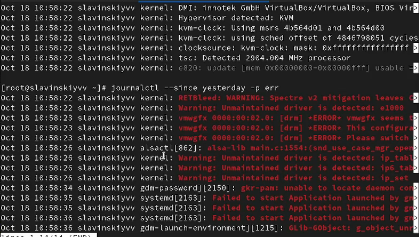


Рис. 24: Все сообщения с ошибкой приоритета

Если нам нужна детальная информация, то будем использовать journalctl -o verbose.(рис. 25)

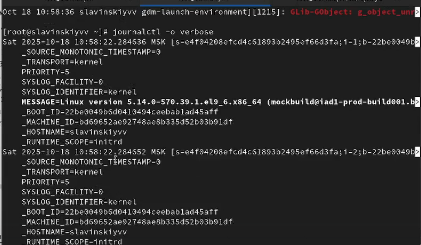


Рис. 25: Вывод детальной информации

Для просмотра дополнительной информации о модуле sshd введем: journalctl \_SYSTEMD\_UNIT=sshd.service(рис. 26)

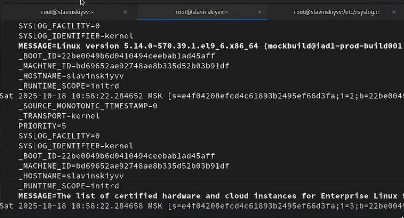


Рис. 26: Дополнительная информация о модуле sshd

Запустим терминал и получим полномочия администратора. Затем создадим каталог для хранения записей журнала: mkdir -p /var/log/journal.(рис. 27)

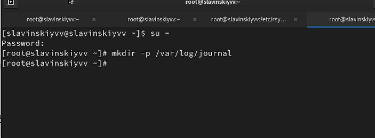


Рис. 27: Создание каталога для хранения записей журнала

Скорректируем 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.(рис. 28)

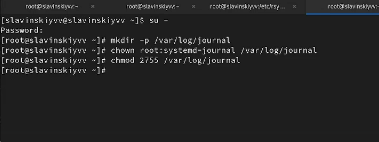


Рис. 28: Корректировка прав доступа

Для принятия изменений нам необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: killall -USR1 systemd-journald.(рис. 29)

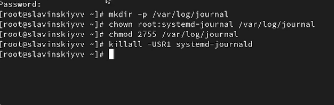


Рис. 29: Принятие изменений

Журнал systemd теперь постоянный. Если мы хотим видеть сообщения журнала с момента последней перезагрузки, то используем: journalctl -b.(рис. 30)

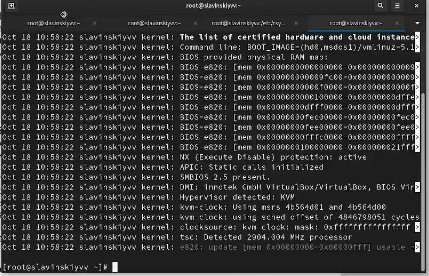


Рис. 30: Включение вывода сообщений после перезагрузки

# 3 Выводы

В ходе выполнения лабораторной работы были получены навыки работы с журналами мониторинга различных событий в системе.

# 4 Ответы на контрольные вопросы

1. /etc/rsyslog.conf
2. /var/log/secure
3. Еженедельная ротация
4. \*.info /var/log/messages
5. tail -f - для rsyslog, а для journald journalctl -f
6. journal ctl –since “09:00:00” –until “15:00:00”
7. journalctl -b
8. mkdir -p /var/log/journal, chown root:systemd-journal /var/log/journal, chmod 2755 /var/log/journal, killall -USR1 systemd-journald