Лабораторная работа №7

Отчет

Устинова Виктория Вадимовна

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с journalctl (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с journald (см. раздел 7.4.4).

# 3 Выполнение лабораторной работы

Запустите три вкладки терминала и в каждом из них получите полномочия администратора.В третьей вкладке терминала вернитесь к учётной записи своего пользователя и попробуйте получить полномочия администратора, но введите неправильный пароль. (рис. 1).

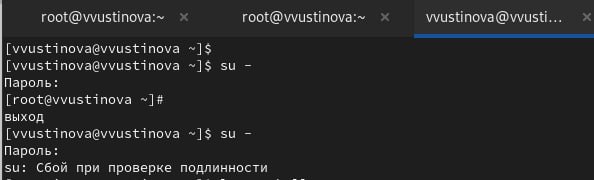


Рис. 1: Запускаем три терминала и вводим неверный пароль

На второй вкладке терминала запустите мониторинг системных событий в реальном времени(рис. 2).

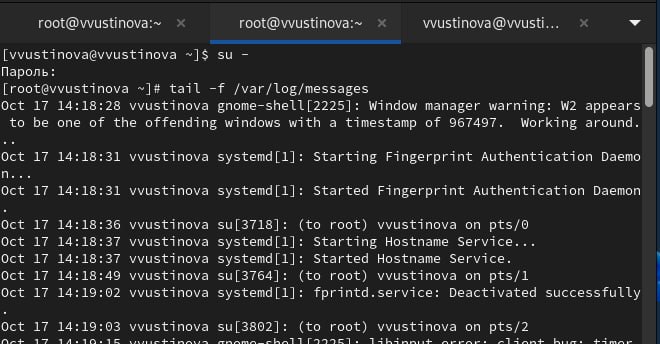


Рис. 2: Запускаем мониторинг

Обратите внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username .(рис. 3).

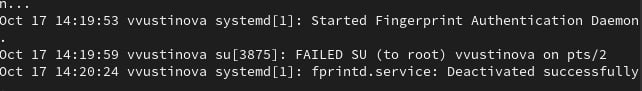


Рис. 3: Сообщение выведенно снизу, из-за тогою. что пытались ввести пароль неверный

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

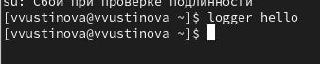


Рис. 4: Вводим logger hello

Во второй вкладке терминала с мониторингом событий вы увидите сообщение, которое также будет зафиксировано в файле /var/log/messages.Запустите мониторинг сообщений безопасности (последние 20 строк)(рис. 5).

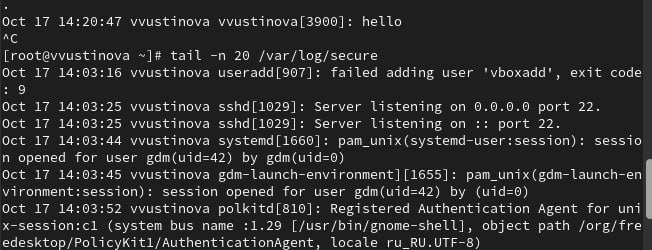


Рис. 5: Отображается hello и выводим 20 строк

В первой вкладке терминала установите Apache.После окончания процесса установки запустите веб-службу:(рис. 6).

Устанавливаем и запускаем, все получилось

Рис. 6: Устанавливаем и запускаем, все получилось

Во второй вкладке терминала посмотрите журнал сообщений об ошибках веб-службы(рис. 7).

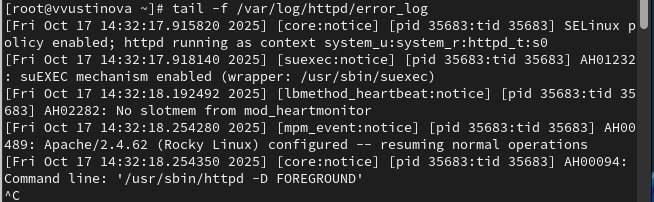


Рис. 7: Смотрим сообщения об ошибках

В третьей вкладке терминала получите полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавьте следующую строку(рис. 8).

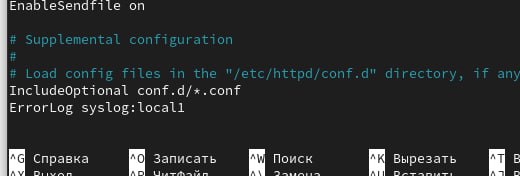


Рис. 8: Открываем файл в редакторе nano и добавляем строку

В каталоге /etc/rsyslog.d создайте файл мониторинга событий веб-службы.Открыв его на редактирование, пропишите в нёмlocal1.\* -/var/log/httpd-error.log(рис. 9).

Создаем файл и открываем также в редакторе nano и добавляем строку

Рис. 9: Создаем файл и открываем также в редакторе nano и добавляем строку

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

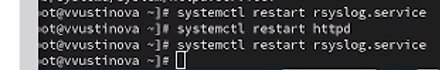


Рис. 10: Перезагружаем введя команды

В третьей вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале введите(рис. 11).

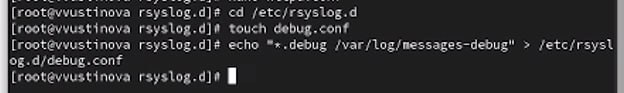


Рис. 11: Записываем строку в файл и создаем его

Во второй вкладке терминала запустите мониторинг отладочной информации:(рис. 12).

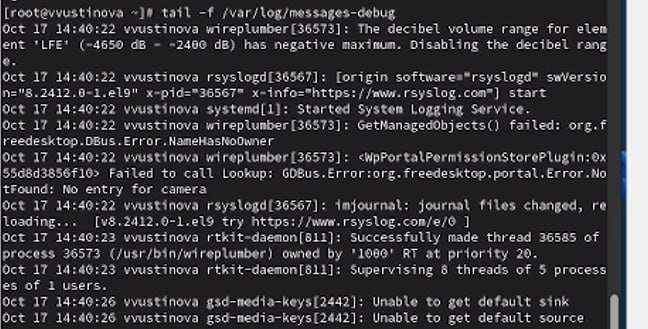


Рис. 12: Снова запускаем мониторинг

В третьей вкладке терминала введите:logger -p daemon.debug “Daemon Debug Message”(рис. 13).

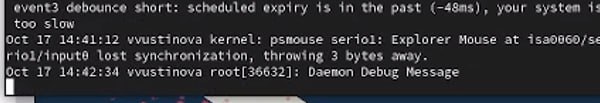


Рис. 13: Переходя на вторую вкладку терминала отображается сразу сообщение

Просмотр содержимого журнала без использования пейджера:(рис. 14).

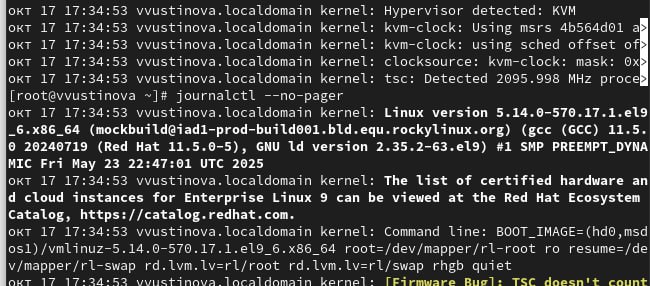


Рис. 14: Команда : journalctl –no-pager

Режим просмотра журнала в реальном времени: journalctl -f и Просмотрите события для UID0: journalctl \_UID=0(рис. 15).

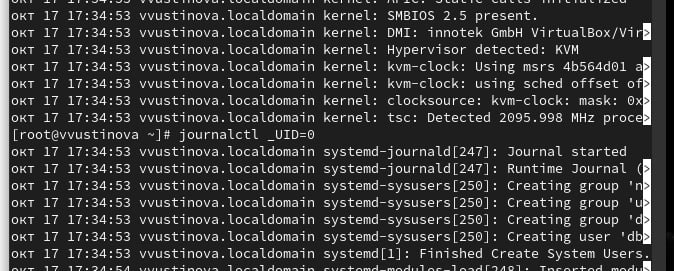


Рис. 15: сверху просмотр в реальном времени снизу события UID0

Для отображения последних 20 строк журнала введите и Для просмотра только сообщений об ошибках введите(рис. 16).

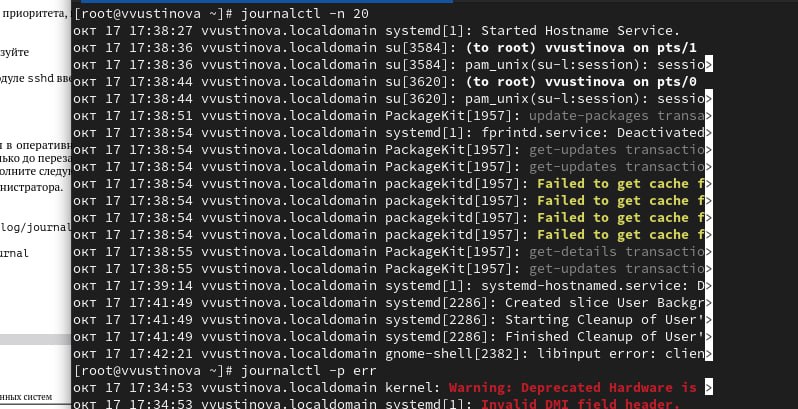


Рис. 16: Смотрим последнии 20 строк и сообщения об ошибках

ля 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(рис. 17).

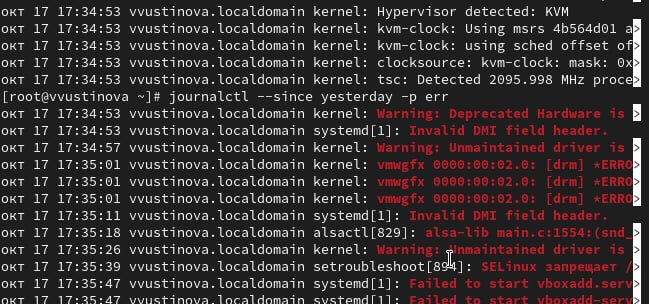


Рис. 17: Смотрим события прошлого дня

Если вам нужна детальная информация, то используйте journalctl -o verbose Для просмотра дополнительной информации о модуле sshd введите(рис. 18).

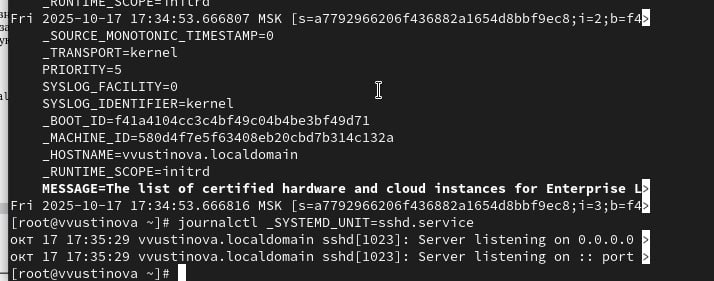


Рис. 18: Выполняем команды

Создаейте каталог, скорректируйте права доступа, Для принятия изменений необходимо или перезагрузить систему, чтобы видеть сообщения журнала с момента последней перезагрузки, используйте:(рис. 19).

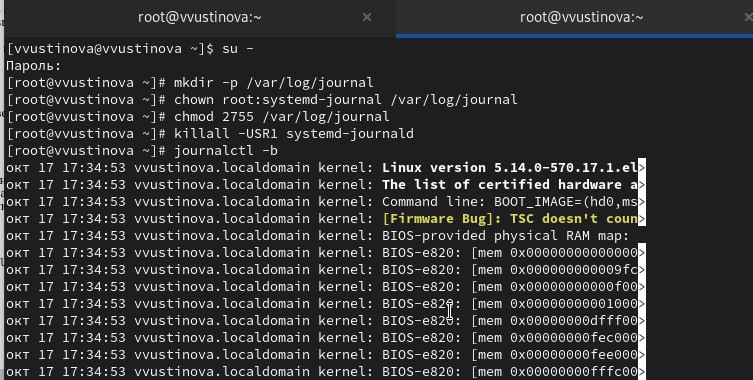


Рис. 19: Выполяем все перечисленные команды

# 4 Выводы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 5 Ответы на контрольные вопросы

1. Файл конфигурации rsyslogd: /etc/rsyslog.conf (или файлы в /etc/rsyslog.d/, включенные в /etc/rsyslog.conf).
2. Файл журнала аутентификации rsyslogd: /var/log/auth.log или /var/log/secure (зависит от конфигурации).
3. Период ротации журналов по умолчанию: Еженедельно (weekly).
4. Строка конфигурации для записи сообщений info в /var/log/messages.info: \*.info /var/log/messages.info
5. Команда для просмотра журналов в реальном времени: Rsyslog: tail -f /var/log/syslog Journald: journalctl -f
6. Команда для просмотра сообщений PID 1 между 9:00 и 15:00 (journald): journalctl \_PID=1 –since “09:00” –until “15:00”
7. Команда для просмотра сообщений journald после последней перезагрузки: journalctl -b
8. Процедура для обеспечения постоянного хранения журналов journald: sudo mkdir /var/log/journal sudo systemctl restart systemd-journald