**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

*дисциплина: Основы администрирования операционных систем*

Студент: Накова Амина Михайловна

Студ. билет № 1132232887

Группа: НПИбд-02-23

**МОСКВА**

2025 г.

# Цель работы:

# Целью данной работы является получение навыков работы с журналами мониторинга различных событий в системе.

**Выполнение работы:**

**Мониторинг журнала системных событий в реальном времени:**

Для начала запустим три вкладки терминала и в каждом из них получим полномочия администратора: **su -**. На второй вкладке терминала запустим мониторинг системных событий в реальном времени: **tail -f /var/log/messages** (Рис. 1):

**Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание**

**Рис. 1.** Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.

В третьей вкладке терминала вернёмся к учётной записи своего пользователя (нажав **Ctrl + d**) и попробуем получить полномочия администратора, но при этом вводим неправильный пароль (Рис. 2):

**Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание**

**Рис. 2.** Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора.

Обратим внимание, что во второй вкладке терминала с мониторингом событий появилось сообщение **«FAILED SU (to root) ismakhorin on pts/2»**. Отображаемые на экране сообщения также фиксируются в файле **/var/log/messages** (Рис. 3):

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

**Рис. 3.** Новое сообщение в мониторинге событий во второй вкладке терминала.

В третьей вкладке терминала из оболочки пользователя введём: **logger hello** (Рис. 4):

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

**Рис. 4.** Ввод в третьей вкладке терминала.

Далее возвращаемся во вторую вкладку терминала с мониторингом событий и видим сообщение, которое также будет зафиксировано в файле **/var/log/messages** («**hello**»). В этой же 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): **tail -n 20 /var/log/secure**. Мы видим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды **su -**

**Изменение правил rsyslog.conf:**

В первой вкладке терминала установим Apache: **dnf -y install httpd** (Рис. 5).

**Изображение выглядит как текст, Шрифт, программное обеспечение, снимок экрана

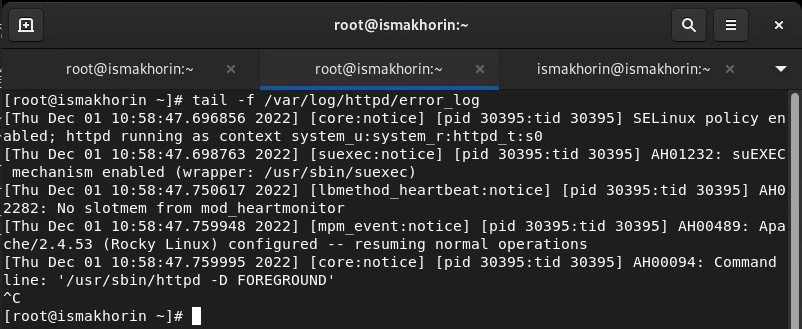
Автоматически созданное описание**

**Рис. 5.** Установка Apache.

После окончания процесса установки запустим веб-службу: **systemctl start httpd и systemctl enable httpd**

.

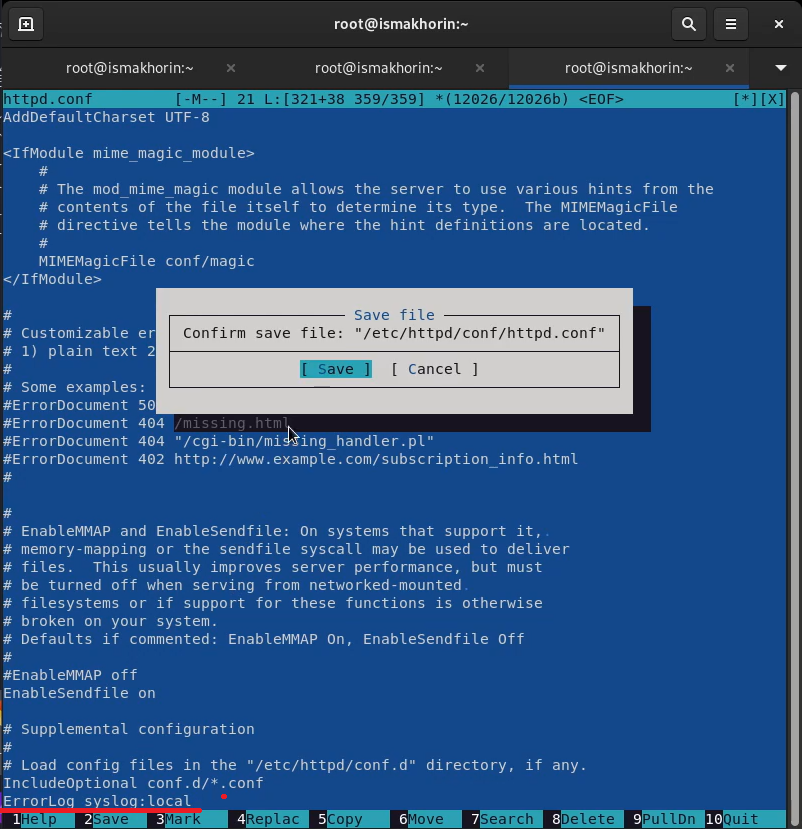
Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: **tail -f /var/log/httpd/error\_log.** Чтобы закрыть трассировку файла журнала, используем **Ctrl + c** (Рис. 6).

****

**Рис. 6.** Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала.

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации **/etc/httpd/conf/httpd.conf** в конце добавляем (Рис. 7) следующую строку: **ErrorLog syslog:local** (Рис. 8).

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

****

**Рис. 7.** Добавление строки в файл и сохранение.

В каталоге /etc/rsyslog.d создаём файл мониторинга событий веб-службы:

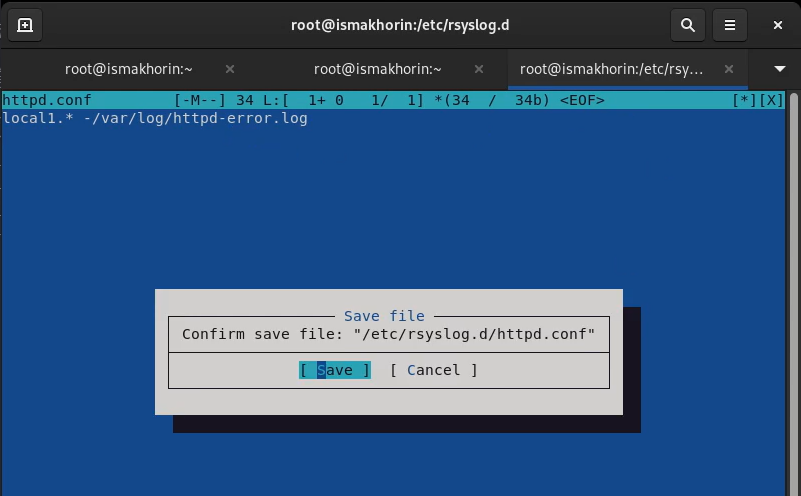
**cd /etc/rsyslog.d**

**touch httpd.conf**

Открыв его на редактирование, пропишем в нём **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/httpderror.log.

****

**Рис. 8.** Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование.

****

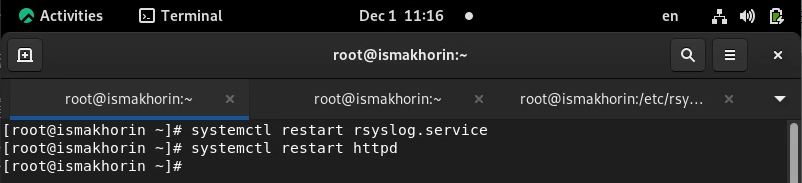
**Рис. 9.** Добавление строки в файл и сохранение.

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

**systemctl restart rsyslog.service**

**systemctl restart httpd**

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. 10.** Открытие первой вкладки терминала и перезагрузка конфигурации rsyslogd и веб-службы.

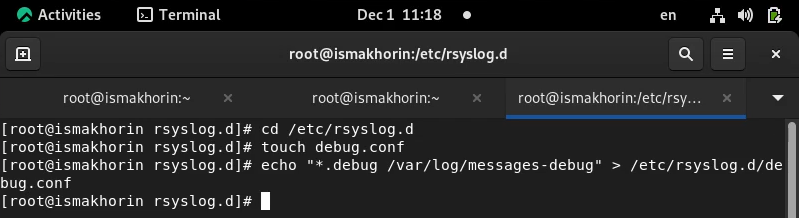
В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации:

**cd /etc/rsyslog.d**

**touch debug.conf**

В этом же терминале вводим:

**echo "\*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf** (Рис. 11):

****

**Рис. 11.** Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.

В первой вкладке терминала снова перезапустим rsyslogd: **systemctl restart rsyslog.service** (Рис. 12):

****

**Рис. 12.** Открытие первой вкладки терминала и перезапуск rsyslogd.

Во второй вкладке терминала запустим мониторинг отладочной информации: **tail -f /var/log/messages-debug**

В третьей вкладке терминала введём: **logger -p daemon.debug "Daemon Debug Message"** (Рис. 13):

****

**Рис. 13.** Открытие третьей вкладки терминала и ввод команды.

В терминале с мониторингом посмотрим сообщение отладки. Чтобы закрыть трассировку файла журнала, используем Ctrl + c

**Использование journalctl:**

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: **journalctl**. Для пролистывания журнала можно использовать или **Enter** (построчный просмотр), или **пробел** (постраничный просмотр). Для выхода из просмотра используется **q**

Просмотрим содержимое журнала без использования пейджера: **journalctl --no-pager**

Режим просмотра журнала в реальном времени: **journalctl -f**. Для прерывания просмотра: **Ctrl + c**

Просмотрим события для UID0: **journalctl \_UID=0**

Для отображения последних 20 строк журнала введём: **journalctl -n 20**

Для просмотра только сообщений об ошибках введём: **journalctl -p err**

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. Например, для просмотра всех сообщений со вчерашнего дня введём: **journalctl --since yesterday**

Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используем: **journalctl --since yesterday -p err**, а если нам нужна детальная информация, то используем: **journalctl -o verbose**

Для просмотра дополнительной информации о модуле sshd введём: **journalctl \_SYSTEMD\_UNIT=sshd.service**

**Постоянный журнал journald:**

Запустим терминал и получим полномочия администратора: **su -**. Далее создадим каталог для хранения записей журнала: **mkdir -p /var/log/journal** и 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**

Для принятия изменений необходимо использовать команду: **killall -USR1 systemd-journald**. Журнал systemd теперь постоянный. Если мы хотим видеть сообщения журнала с момента последней перезагрузки, используем: **journalctl -b**

**Ответы на контрольные вопросы:**

1. Какой файл используется для настройки rsyslogd? **/etc/rsyslog.conf**

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? **/var/log/secure**

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

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

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени? **tail -f /var/log/messages**

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00? **journalctl \_PID=1 -since “2022-02-01 09:00:00” –until “2022-02-01 15:00:00”**

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы? **journalctl - b**

8. Какая процедура позволяет сделать журнал journald постоянным?

Запустите терминал и получите полномочия администратора: **su –**

Создайте каталог для хранения записей журнала: **mkdir -p /var/log/journal**

Скорректируйте 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**

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

(1-4 задание в последнем блоке)

**Вывод:**

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