

Шаблон отчёта по лабораторной работе

Простейший вариант

Дмитрий Сергеевич Кулябов

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
4 Выводы	19
Список литературы	20

Список иллюстраций

3.1 терминалы	7
3.2 журнал каталога /var/log/messages	8
3.3 выход из режима администратора	8
3.4 неправильный пароль	9
3.5 сообщение о ошибке	9
3.6 logger hello	10
3.7 сообщение hello	10
3.8 завершение журнала	11
3.9 мониторинг сообщений безопасности	11
3.10 установка httpd	12
3.11 запуск утилиты	12
3.12 журнал сообщений об ошибках	13
3.13 пользователь root	13
3.14 изменение файла /etc/httpd/conf/httpd.conf	14
3.15 httpd.conf	14
3.16 новая строка	15
3.17 перезагрузка конфигурацию rsyslogd и веб-службу	15
3.18 конфигурация для мониторинга отладочной информации	16
3.19 перезапуск rsyslogd	16
3.20 мониторинг отладочной информации	17
3.21 logger	17
3.22 закрытие трассироваки файла журнала	18
3.23 Название	18

Список таблиц

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 .
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
3. Продемонстрируйте навыки работы с journalctl.
4. Продемонстрируйте навыки работы с journald.

3 Выполнение лабораторной работы

Сначала я открыл 3 терминала под пользователя root (рис. 3.1).

```
su -
```

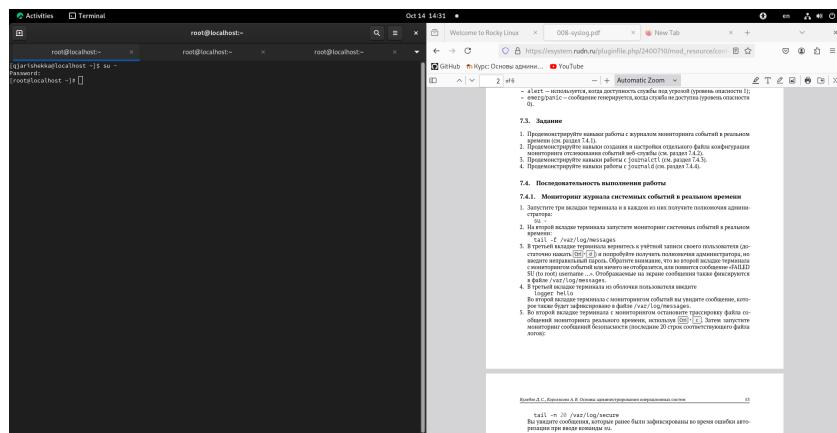


Рис. 3.1: терминалы

Потом во втором терминале я выполнил команду tail чтобы смотреть журнал в каталоге /var/log/messages (рис. 3.2).

```
tail -f var/log/messages
```

```

root@localhost:~$ su -
Password:
root@localhost:~$ tail -f /var/log/messages
Oct 14 14:30:53 localhost su[4698]: (to root) sh@localhost on pts/0
Oct 14 14:30:58 localhost system[1]: Started Hostname Service.
Oct 14 14:30:58 localhost system[1]: /etc/hostname: /etc/hostname
Oct 14 14:31:21 localhost system[1]: /etc/init.d/avahi-daemon start
Oct 14 14:31:29 localhost system[2427]: Created slice slice /app dbus-1.2.org.gnome.Daemon.
Oct 14 14:31:30 localhost gdm[2884]: Started session "gdm" of user "root".
Oct 14 14:32:00 localhost system[1]: system-hostnamed.service: Deactivated successfully.
Oct 14 14:32:00 localhost system[1]: system-hostnamed.service: Deactivated successfully.

```

Рис. 3.2: журнал каталога /var/log/messages

Дальше в третьем терминале я вышел из режима администратора нажая клавиши Ctrl+d (рис. 3.3).

Ctrl + d

```

root@localhost:~$ su -
Password:
root@localhost:~$ exit
qjirishkai@localhost:~$ 

```

Рис. 3.3: выход из режима администратора

Затем я попытался входить в режим суперпользователя но с неправильным паролем не удаваясь (рис. 3.4).

su -

asdfasdlkfj

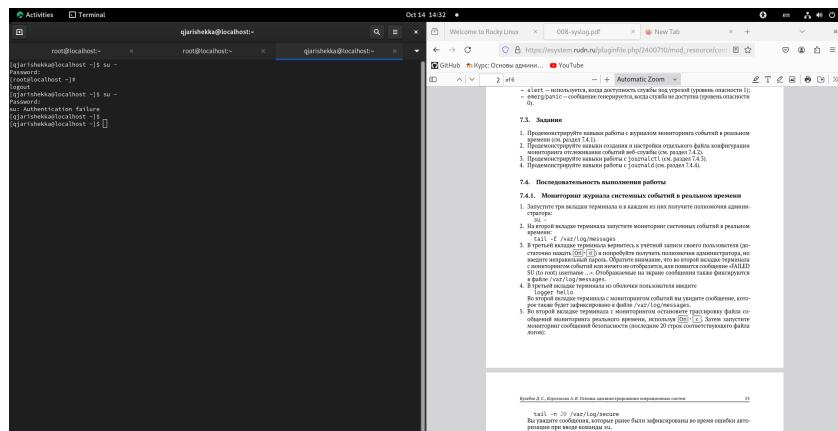


Рис. 3.4: неправильный пароль

Потом я вернулся в первую вкладку и там я смог смотреть сообщение “Failed su (to root) username....”(рис. 3.5).

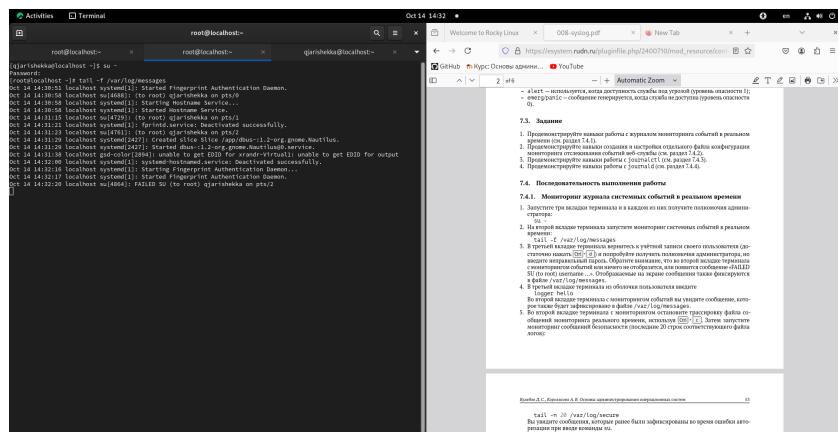


Рис. 3.5: сообщение о ошибке

Дальше я выполнил следующую команду (рис. 3.6):

`logger hello`

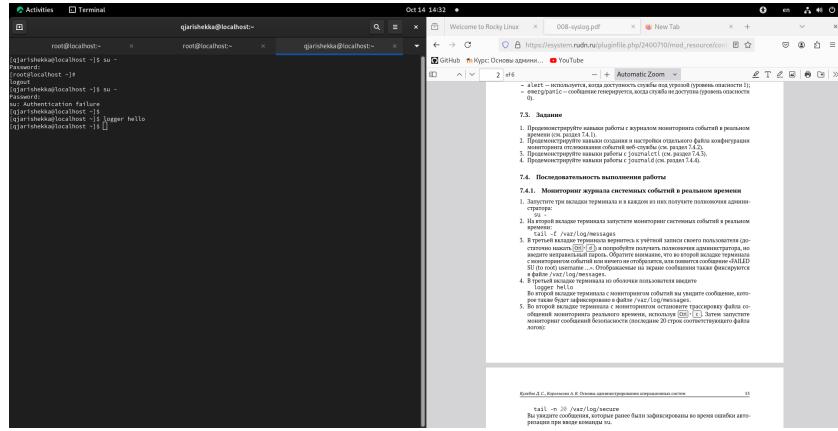


Рис. 3.6: logger hello

Тогда когда я вернулся во вторую вкладку там появились сообщение “hello” (рис. 3.7).

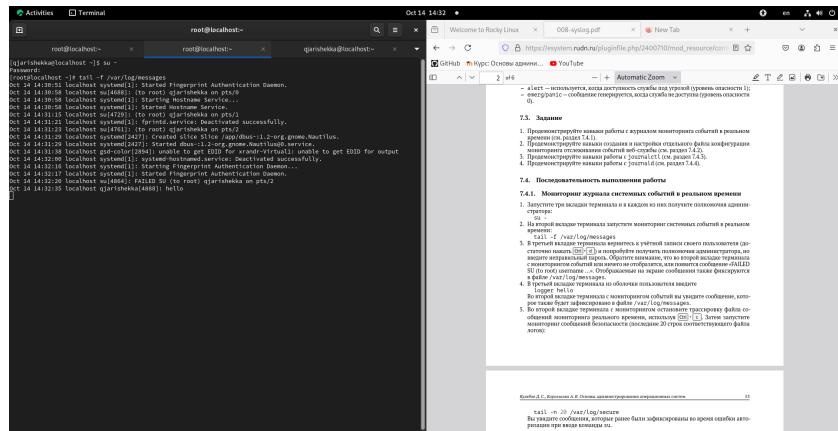


Рис. 3.7: сообщение hello

Потом я завершил просмотр журнала (рис. 3.8).

Ctrl + c

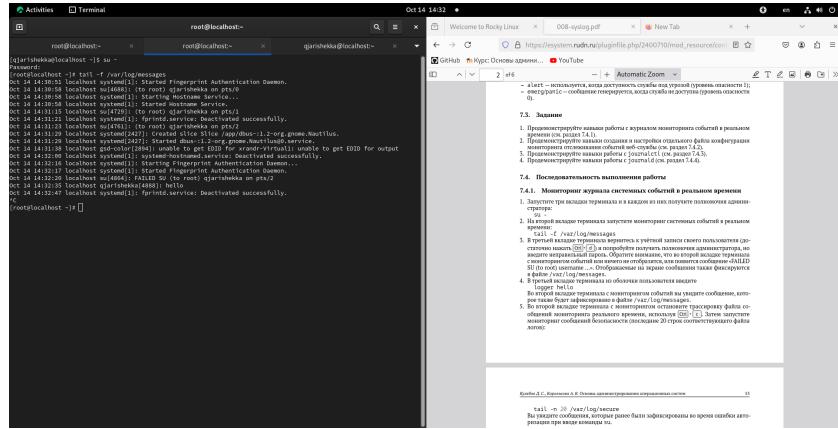


Рис. 3.8: завершение журнала

Дальше я запустил мониторинг сообщений безопасности (рис. 3.9).

`tail -n 20 /var/log/secure`

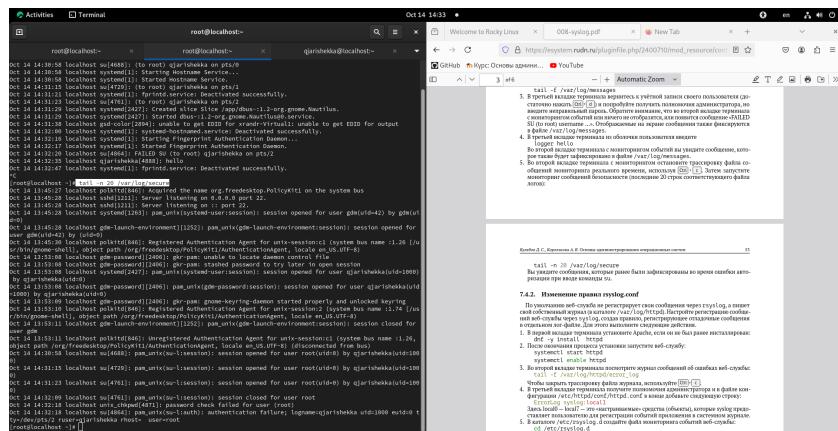


Рис. 3.9: мониторинг сообщений безопасности

Дальше я начал другую часть лабораторной работы.

Сначала я установил утилиту httpd (рис. 3.10).

`dnf -y install httpd`

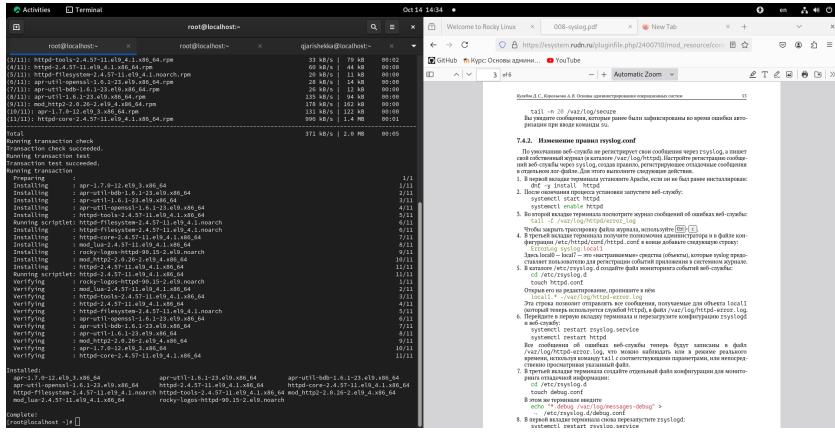


Рис. 3.10: установка httpd

Потом я инициализировал его (рис. 3.11).

```
systemctl start httpd  
systemctl enable http
```

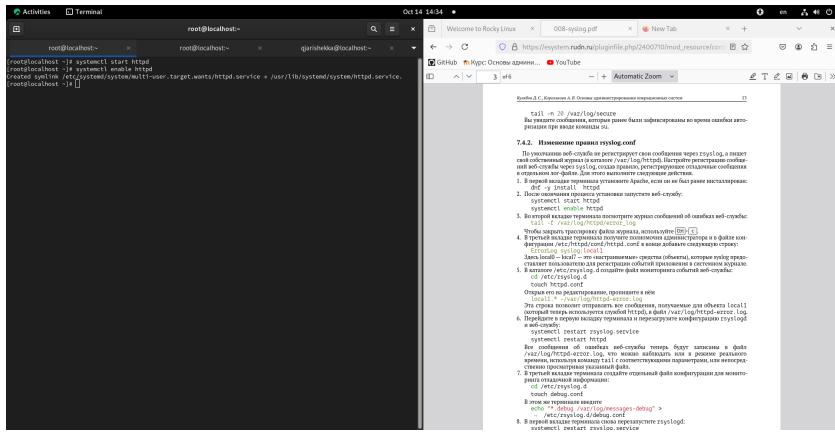


Рис. 3.11: запуск утилиты

Потом во второй вкладке терминала я смотрел журнал сообщений об ошибках веб-службы (рис. 3.12).

```
tail -f /var/log/httpd/error_log
```

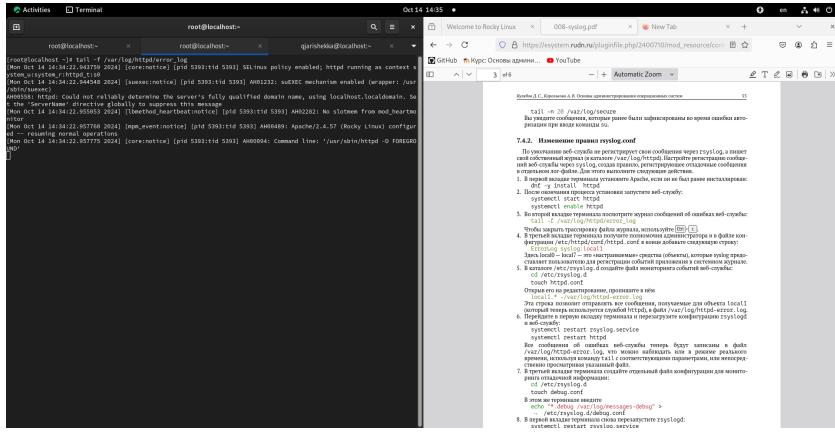


Рис. 3.12: журнал сообщений об ошибках

Потом я перешел в третьюю вкладку и получил полномочия администратора (рис. 3.13). и в файле /etc/httpd/conf/httpd.conf я добавил одну строку (рис. 3.14).

```
su -  
vim /etc/httpd/conf/httpd.conf  
Errorlog syslog:local1  
:wq
```

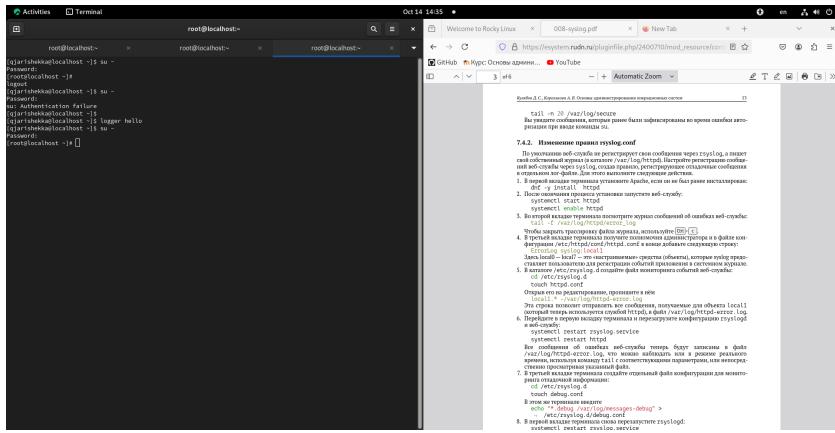


Рис. 3.13: пользователь root

Рис. 3.14: изменение файла /etc/httpd/conf/httpd.conf

Потом я перешел в другой каталог /etc/rsyslog.d и создал один файл “httpd.conf” (рис. 3.15).

```
cd /etc/rsyslog.d  
touch httpd.conf
```

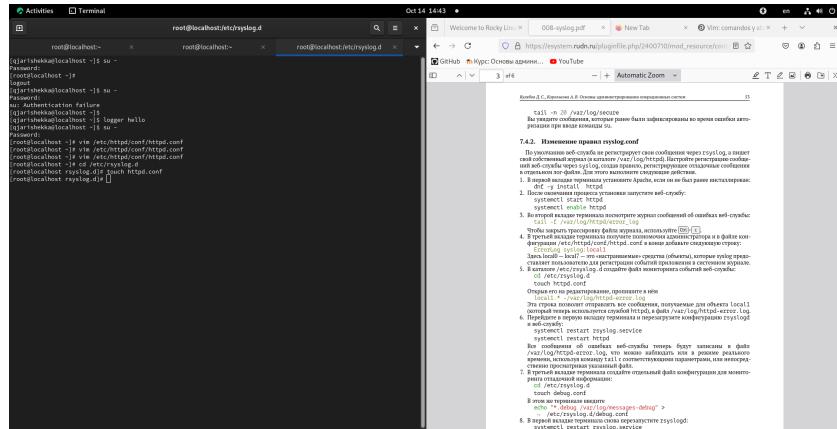


Рис. 3.15: httpd.conf

В этом файле я добавил одну строку и сохранил его (рис. 3.16).

```
mcedit httpd.conf  
local1.* -/var/log/httpd-error.log
```

f10

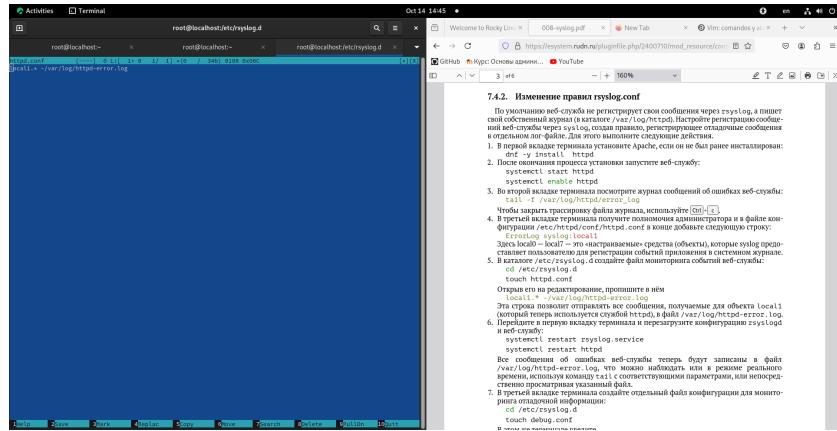


Рис. 3.16: новая строка

Дальше я перешел в первую вкладку терминала и перезагрузил конфигурацию rsyslogd и веб-службу (рис. 3.17).

```
systemctl restart rsyslog.service  
systemctl restart httpd
```

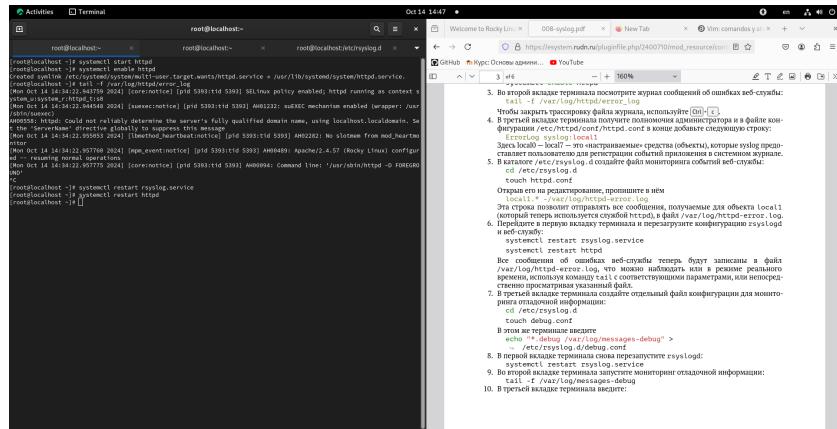


Рис. 3.17: перезагрузка конфигурацию rsyslogd и веб-службу

Затем я перешел в третьюю вкладку и создал отдельный файл конфигурации для мониторинга отладочной информации (рис. 3.18).

```

cd /etc/rsyslog.d
touch debug.conf
echo ".*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf

```

The terminal window shows the following command sequence:

```

cd /etc/rsyslog.d
touch debug.conf
echo ".*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf

```

The second window is a help guide titled "Лабораторная работа №7. Управление журнализацией событий в системе". It provides instructions for monitoring logs, including:

- Откройте его на редакторе, пропишите в нем
- Эта строка определяет лог-файл журналирования, получаемое для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log.
- Перезапустите первую вкладку терминала и перезапустите конфигурацию rsyslogd и веб-сервер.
- systemctl restart rsyslog service
- systemctl restart httpd service
- Все сообщения об ошибках веб-сервиса теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени с помощью команды tail -f /var/log/httpd-error.log.
- Проверьте правильность конфигурации и внесите изменения, если это необходимо.
- В первом вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации:

```

cat > /etc/rsyslog.d/debug.conf << EOF
*.* @localhost:514 debug
EOF

```

- В второй вкладке терминала запустите мониторинг отладочной информации:

```

tail -f /var/log/messages-debug

```

- В третьей вкладке терминала введите:

Рис. 3.18: конфигурация для мониторинга отладочной информации

Потом еще раз в первой вкладке терминала снова перезапустил rsyslogd (рис. 3.19).

`systemctl restart rsyslog.service`

The terminal window shows the following command:

```

systemctl restart rsyslog.service

```

The second window is a help guide titled "Лабораторная работа №7. Управление журнализацией событий в системе". It provides instructions for monitoring logs, including:

- Откройте его на редакторе, пропишите в нем
- Эта строка определяет лог-файл журналирования, получаемое для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log.
- Перезапустите первую вкладку терминала и перезапустите конфигурацию rsyslogd и веб-сервер.
- systemctl restart rsyslog service
- systemctl restart httpd service
- Все сообщения об ошибках веб-сервиса теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени с помощью команды tail -f /var/log/httpd-error.log.
- Проверьте правильность конфигурации и внесите изменения, если это необходимо.
- В первом вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации:

```

cat > /etc/rsyslog.d/debug.conf << EOF
*.* @localhost:514 debug
EOF

```

- В второй вкладке терминала запустите мониторинг отладочной информации:

```

tail -f /var/log/messages-debug

```

- В третьей вкладке терминала введите:

Рис. 3.19: перезапуск rsyslogd

Затем во второй вкладке терминала я запустил мониторинг отладочной информации (рис. 3.20).

```
tail -f /var/log/messages-debug
```

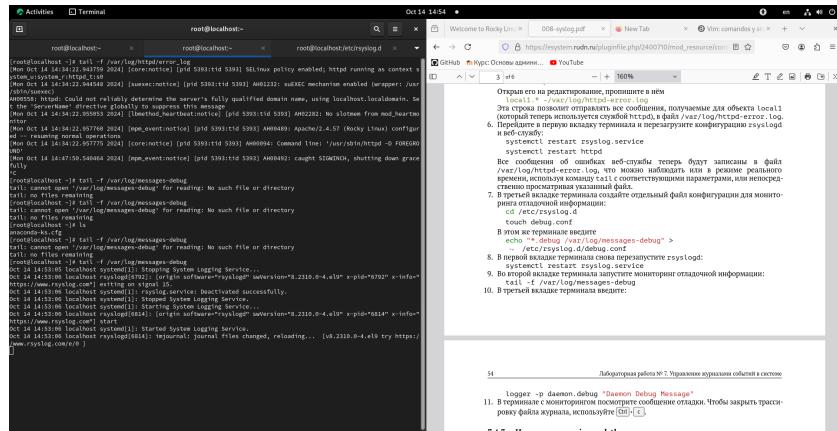


Рис. 3.20: мониторинг отладочной информации

Потом я в третьей вкладке терминала выполнил команду logger (рис. 3.21).

```
logger -p daemon.debug "Daemon Debug Message"
```

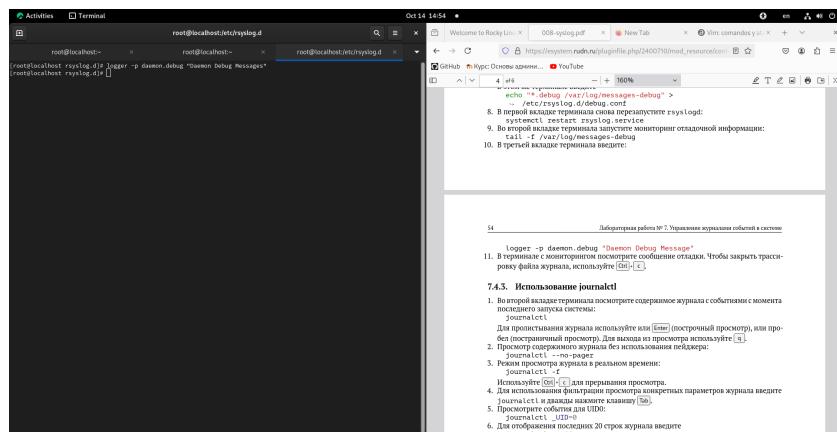


Рис. 3.21: logger

Затем я закрыл трассиворку файла журнала во второй вкладке (рис. 3.22).

Ctrl + c

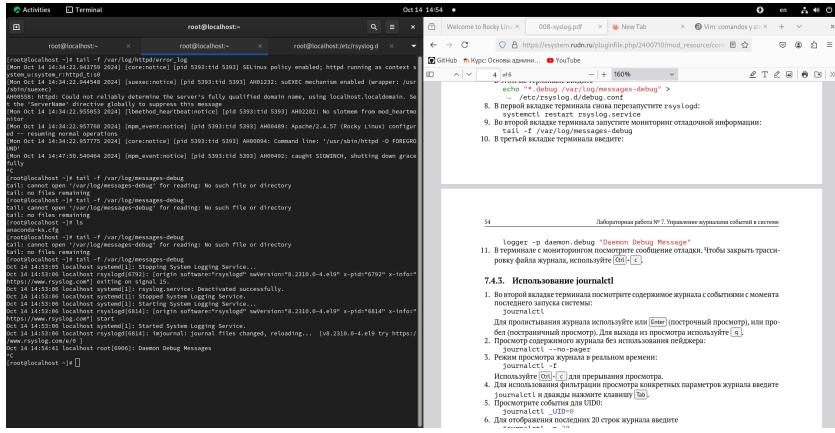


Рис. 3.22: закрытие трассировки файла журнала

(рис. 3.23).

Название

Рис. 3.23: Название

4 Выводы

После выполнения лабораторной работы я смог смотреть работу команд tail и journalctl чтобы смотреть журналы, которые сохраняют все выполненные процессы и как настройт его.

Список литературы