

Шаблон отчёта по лабораторной работе

Простейший вариант

Дмитрий Сергеевич Кулябов

Содержание

1 Цель работы	6
2 Задание	7
3 Выполнение лабораторной работы	8
4 Выводы	28
Список литературы	29

Список иллюстраций

3.1 терминалы	8
3.2 журнал каталога /var/log/messages	9
3.3 выход из режима администратора	9
3.4 неправильный пароль	10
3.5 сообщение о ошибке	10
3.6 logger hello	11
3.7 сообщение hello	11
3.8 завершение журнала	12
3.9 мониторинг сообщений безопасности	12
3.10 установка httpd	13
3.11 запуск утилиты	13
3.12 журнал сообщений об ошибках	14
3.13 пользователь root	14
3.14 изменение файла /etc/httpd/conf/httpd.conf	15
3.15 httpd.conf	15
3.16 новая строка	16
3.17 перезагрузка конфигурацию rsyslogd и веб-службу	16
3.18 конфигурация для мониторинга отладочной информации	17
3.19 перезапуск rsyslogd	17
3.20 мониторинг отладочной информации	18
3.21 logger	18
3.22 закрытие трассироваки файла журнала	19
3.23 журнал	19
3.24 enter	20
3.25 q	20
3.26 журнал без использования пейджера	21
3.27 журнал в режиме реального времени	21
3.28 Закрытие журнала	22
3.29 журнал событий для UID0	22
3.30 журнал событий для отображения последний 20 строк	23
3.31 журнал событий для отображения ошибках	23
3.32 данные журнала со вчерашнего дня	24
3.33 данные журнала об ошибках со вчерашнего дня	24
3.34 журнал с детальной информацией	25
3.35 дополнительная информация в журнале	25
3.36 новый каталог journal	26
3.37 изменение прав доступа каталога journal	26

3.38 перезапуск службы systemd-journald	27
3.39 сообщения в журнале	27

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 -
```

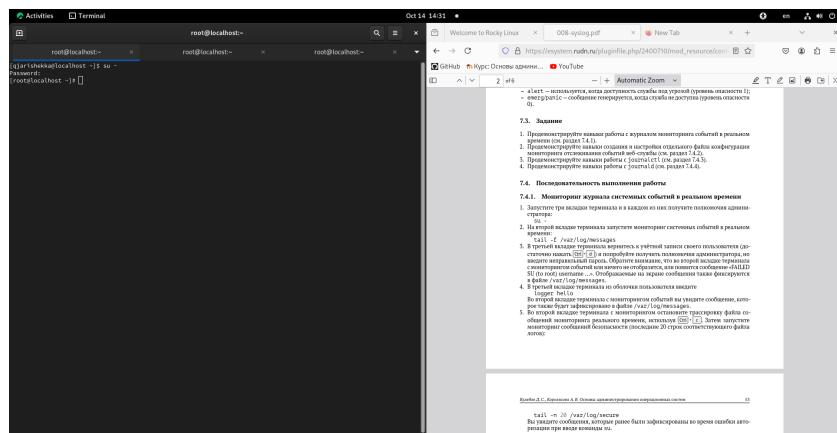


Рис. 3.1: терминалы

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 14:30:54 localhost su[4698]: (to root) sh@localhost on pts/0
Oct 14 14:30:58 localhost systemd[1]: Started Hostname Service.
Oct 14 14:30:58 localhost systemd[1]: Started Network Service.
Oct 14 14:31:01 localhost systemd[1]: Started Journal Service.
Oct 14 14:31:21 localhost systemd[1]: Fired rc.service: Deactivated successfully.
Oct 14 14:31:29 localhost systemd[2427]: Created slice slice /app dbus-1.2.org.gnome.Bluetooth.
Oct 14 14:31:30 localhost gdm[2884]: Started session gdm-1 for user root.
Oct 14 14:32:00 localhost systemd[1]: system-hostnamed.service: Deactivated successfully.
Oct 14 14:32:00 localhost systemd[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:~$ tail -f /var/log/messages

```

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

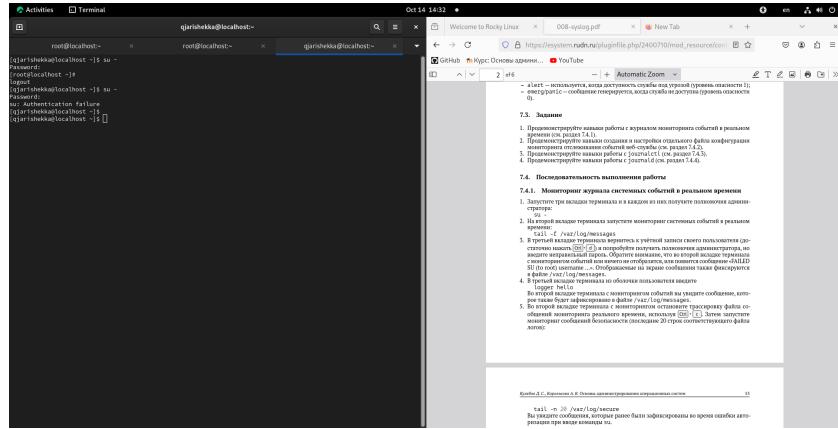


Рис. 3.4: неправильный пароль

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

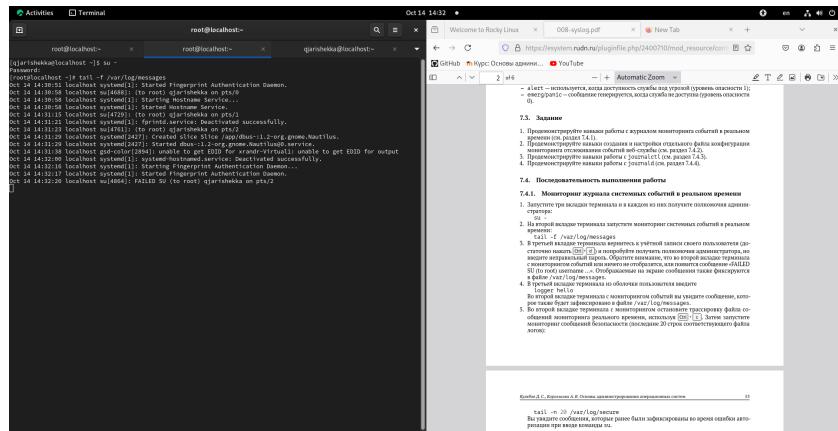


Рис. 3.5: сообщение о ошибке

Дальше я выполнил следующую команду (рис. 3.6):

`logger hello`

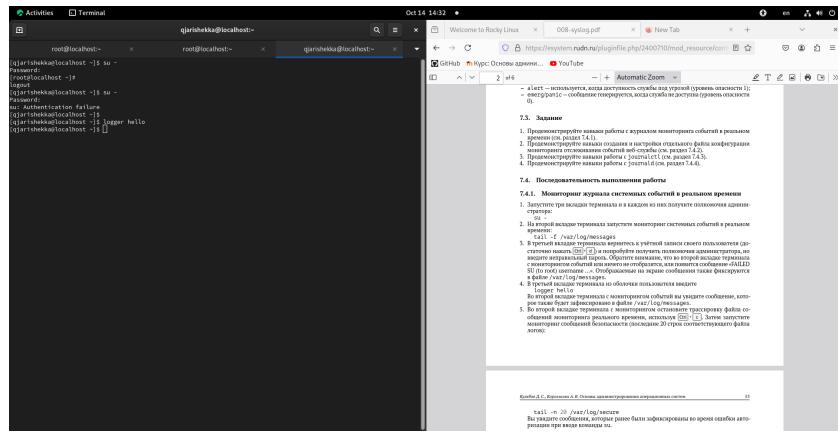


Рис. 3.6: logger hello

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

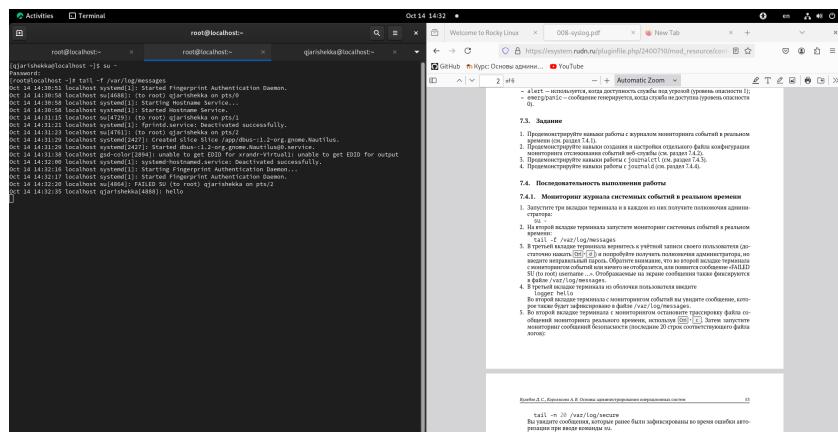


Рис. 3.7: сообщение hello

Потом я завершил просмотр журнала (рис. 3.8).

Ctrl + c

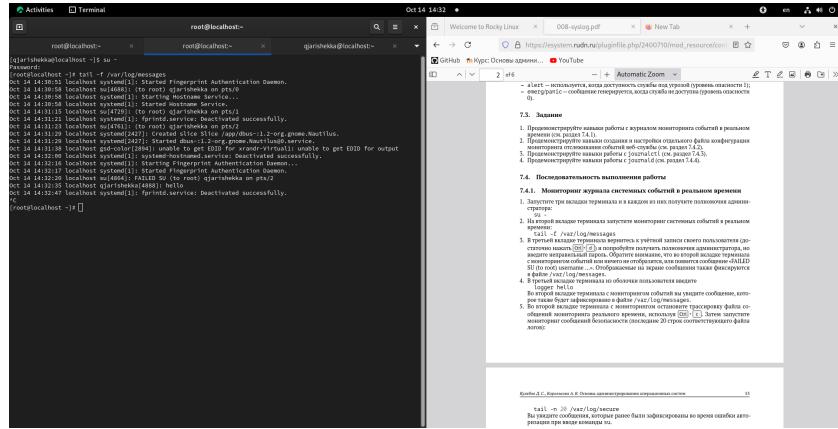


Рис. 3.8: завершение журнала

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

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

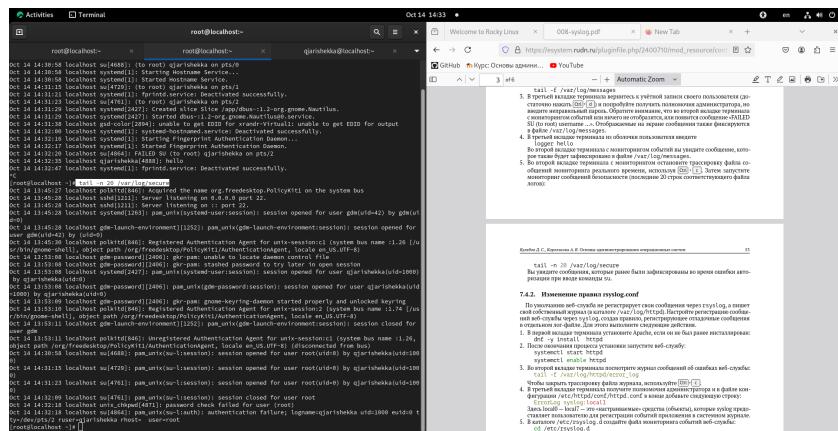


Рис. 3.9: мониторинг сообщений безопасности

Дальше я начал другую часть лабораторной работы.

Сначала я установил утилиту httpd (рис. 3.10).

`dnf -y install httpd`

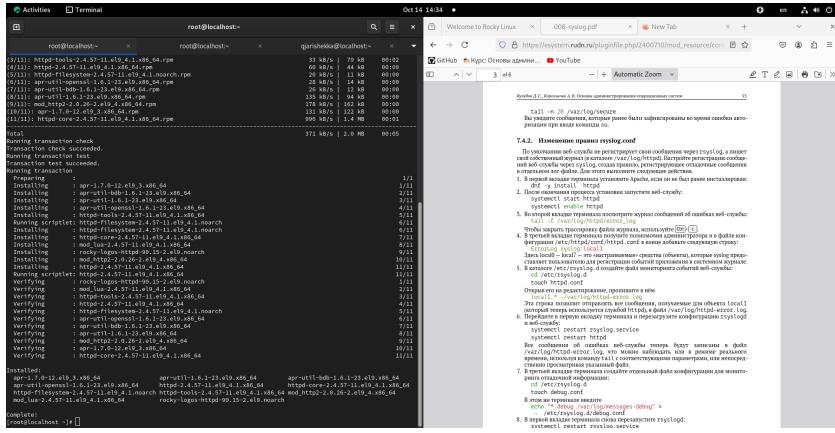


Рис. 3.10: установка httpd

Потом я инициализировал его (рис. 3.11).

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

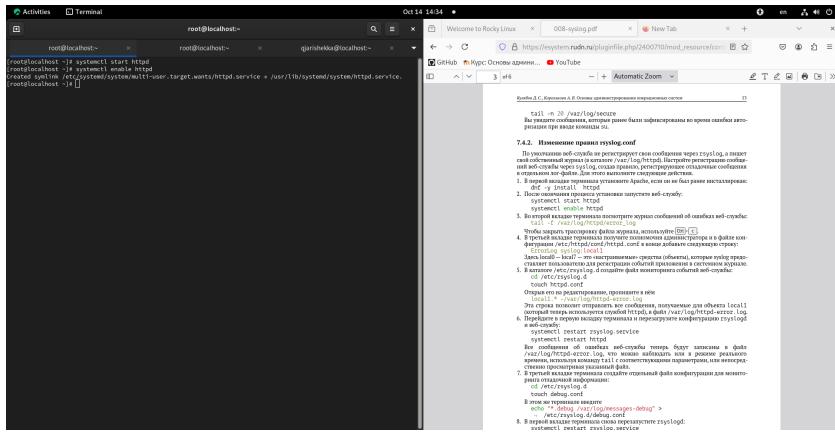


Рис. 3.11: запуск утилиты

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

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

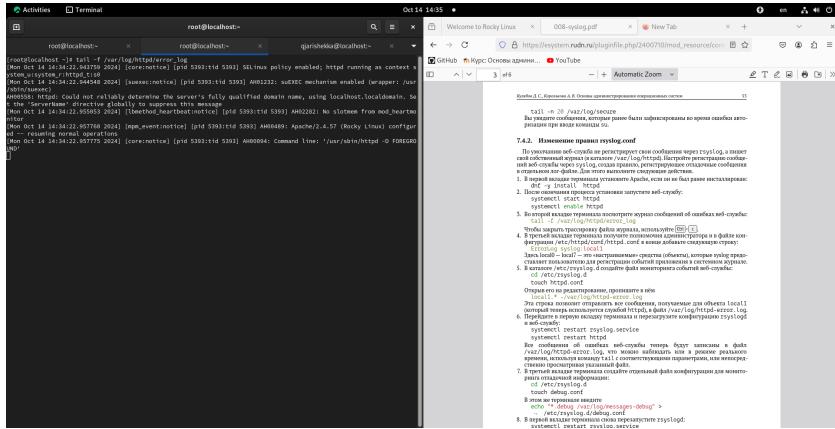


Рис. 3.12: журнал сообщений об ошибках

Потом я перешел в третью 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
```

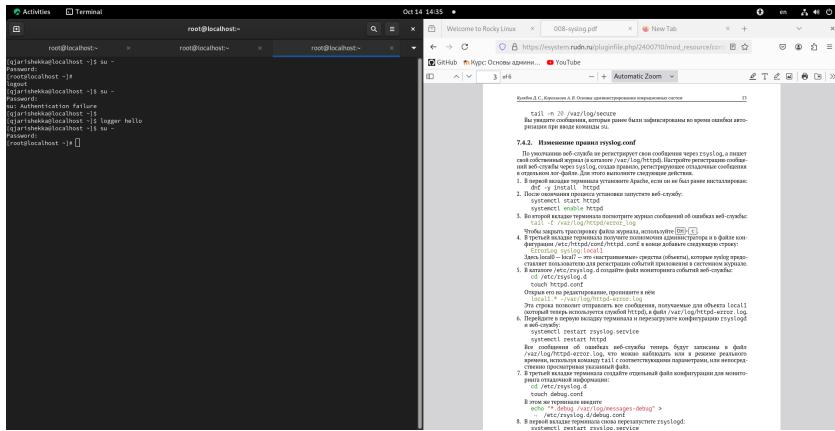


Рис. 3.13: пользователь root

```

# Specify a default charset for all content served, this enables
# interpretation of all content as UTF-8 by default. To use the
# default charset for a specific file (e.g. index.html) or to allow the HTML tags
# to HTML content to override this directive, comment and HTML
# directives
AddDefaultCharset UTF-8

#Module mod_mime_module

    # The mod_mime module allows the server to read various hints from the
    # content of each file itself to determine its type. The MimeMagicFile
    # directive tells the module where the hint definitions are located.
    # +-----+
    # #MimeMagic conf/magic
    #-----#

```

The file continues with more configuration, including ErrorDocument, LogLevel, and various module configurations for mod_cgi, mod_dav, mod_dav_fs, mod_dir, mod_env, mod_mime, mod_log_config, mod_cgi, mod_cgid, mod_so, mod_setenvif, and mod_version.

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

Потом я перешел в друкой каталог /etc/rsyslog.d и создал один файл “httpd.conf”

(рис. 3.15).

```

cd /etc/rsyslog.d
touch httpd.conf

```

```

root@localhost:~# su -
Password:
root@localhost:~# cd /etc/rsyslog.d
root@localhost:~/etc/rsyslog.d# touch httpd.conf
root@localhost:~/etc/rsyslog.d# cat httpd.conf
local1.* -/var/log/httpd-error.log
root@localhost:~/etc/rsyslog.d#

```

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

```

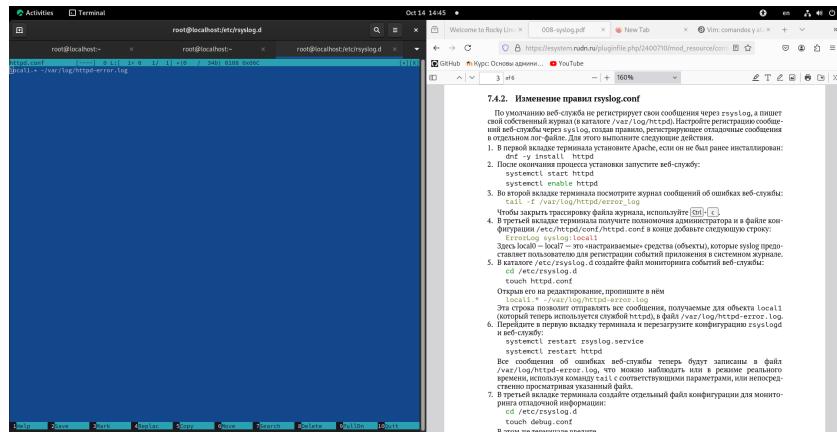


Рис. 3.16: новая строка

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

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

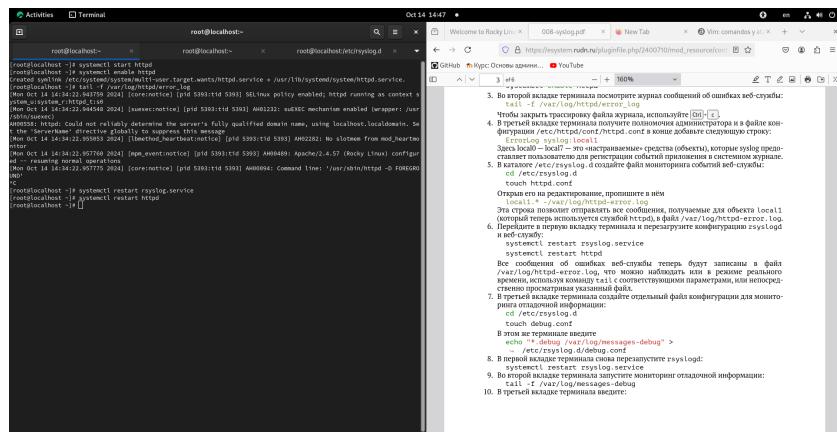


Рис. 3.17: перезагрузка конфигурацию rsyslogd и веб-службу

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

```

```

root@localhost:~# rsyslogd
root@localhost:~# tail -f /var/log/messages-debug

```

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`

```

root@localhost:~# systemctl restart rsyslog.service
root@localhost:~# tail -f /var/log/messages-debug

```

Рис. 3.19: перезапуск rsyslogd

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

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

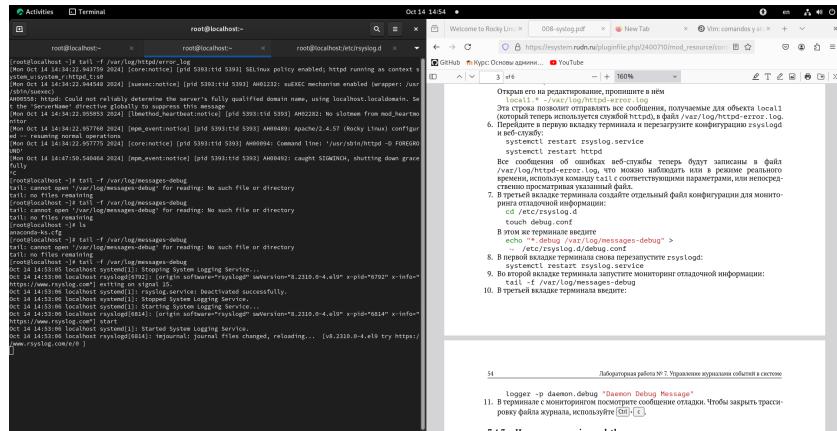


Рис. 3.20: мониторинг отладочной информации

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

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

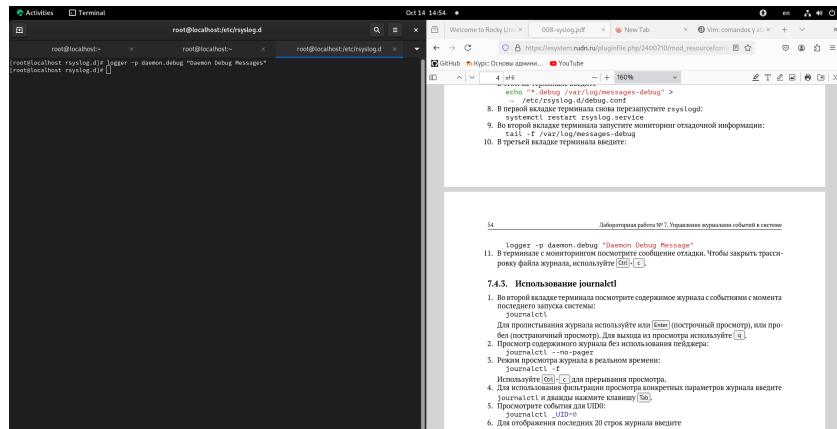


Рис. 3.21: logger

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

Ctrl + c

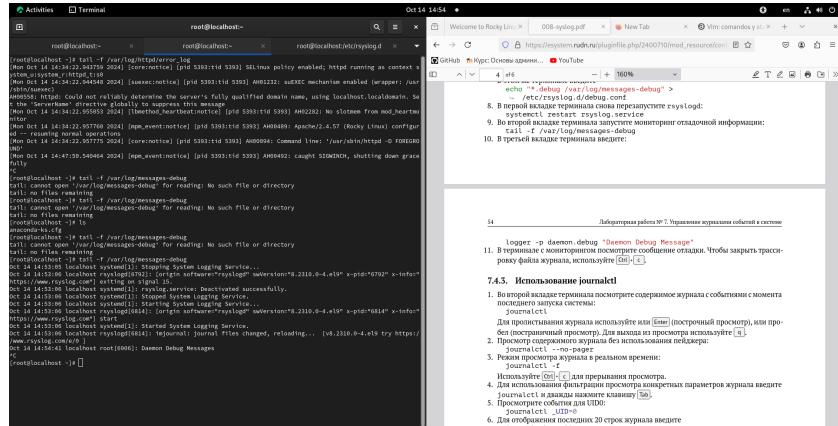


Рис. 3.22: закрытие трассировки файла журнала

Потом я начал следующую часть лабораторной работы (Использование journalctl)

Сначала во второй вкладке терминала я посмотрел содержимое журнала с событиями с момента последнего запуска системы (рис. 3.23).

journalctl

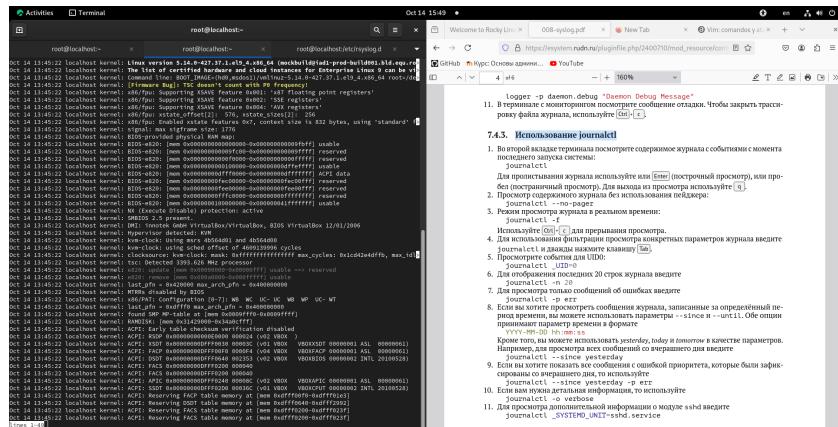


Рис. 3.23: журнал

Потом я делал несколько действия там (`enter` и `q`) (рис. 3.24 и рис. 3.25).

enter

q

Рис. 3.24: enter

Рис. 3.25: q

Потом я выполнил одну команду чтобы смотреть содержимое журнала без использования пейджера (рис. 3.26).

```
journalctl --no-pager
```

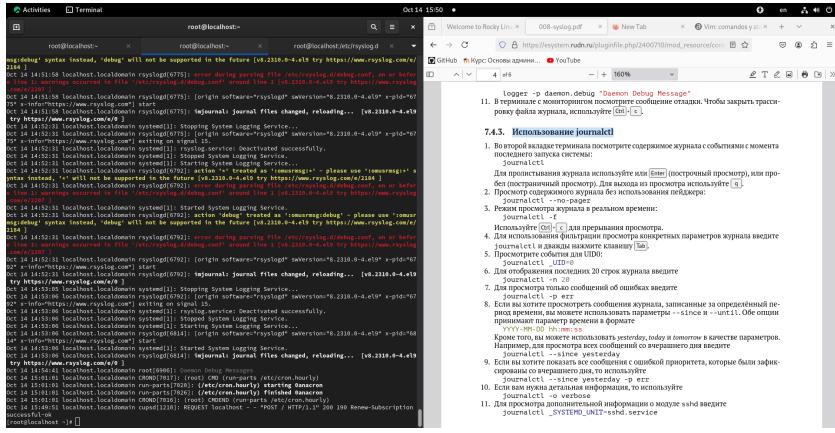


Рис. 3.26: журнал без использования пейджера

Потом я запускал журнал в режиме просмотра в реальном времени (рис. 3.27).

```
journalctl -f
```

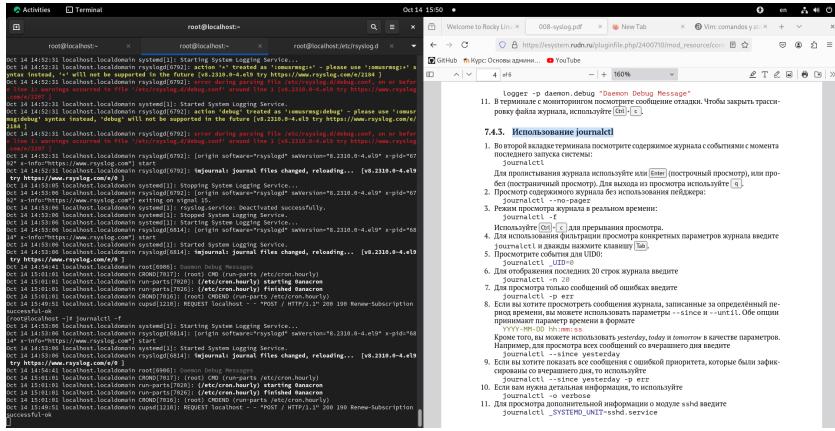


Рис. 3.27: журнал в режиме реального времени

Потом я закрыл журнал нажая клавиши Ctrl + c (рис. 3.28).

Ctrl + c

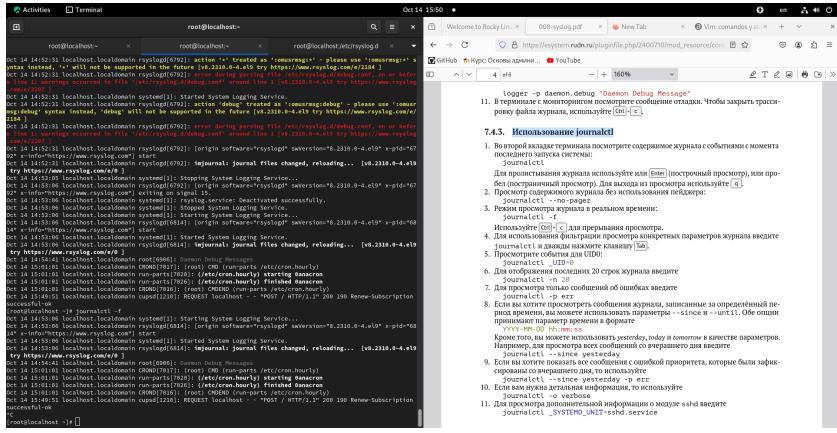


Рис. 3.28: Закрытие журнала

Потом я смотрел события для UID0 (рис. 3.29).

```
journalctl _UID=0
```

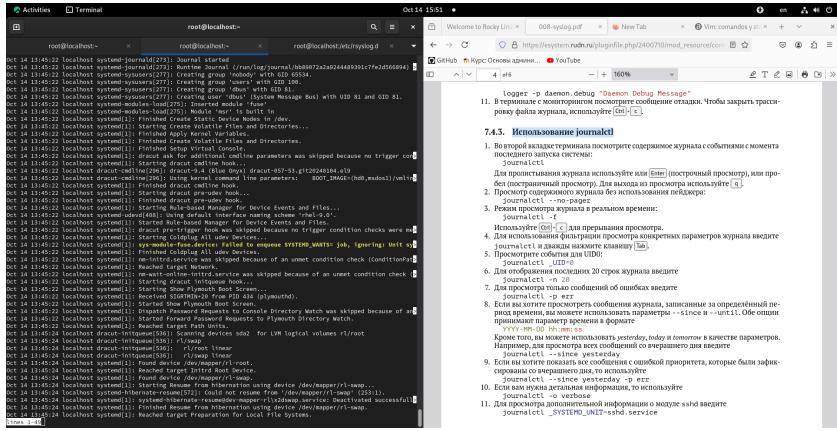


Рис. 3.29: журнал событий для UIDO

Дальше я смотрел события для отображения последних 20 строк журнала (рис. 30).

```
journalctl -n 20
```

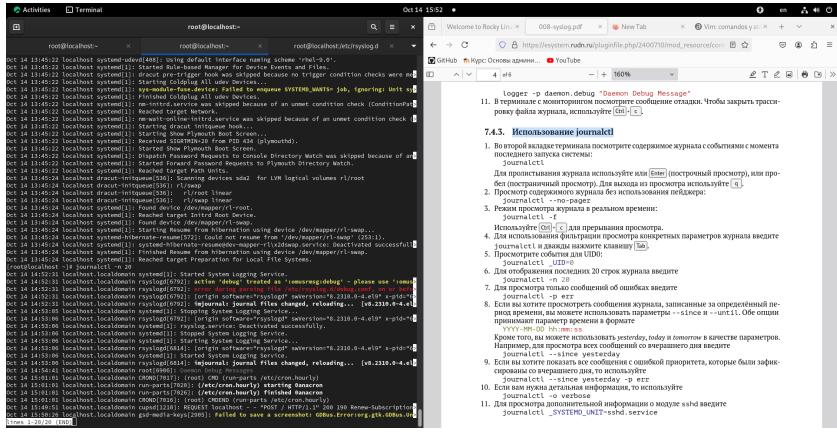


Рис. 3.30: журнал событий для отображения последний 20 строк

и для просмотра только сообщений об ошибках (рис. 3.31).

```
journalctl -p err
```

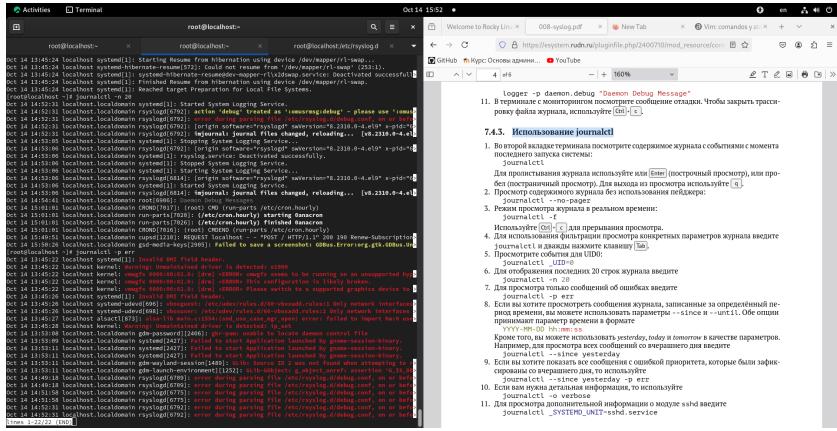


Рис. 3.31: журнал событий для отображения ошибках

Потом я упорядочил журнал по дате (рис. 3.32).

```
journalctl --since yesterday
```

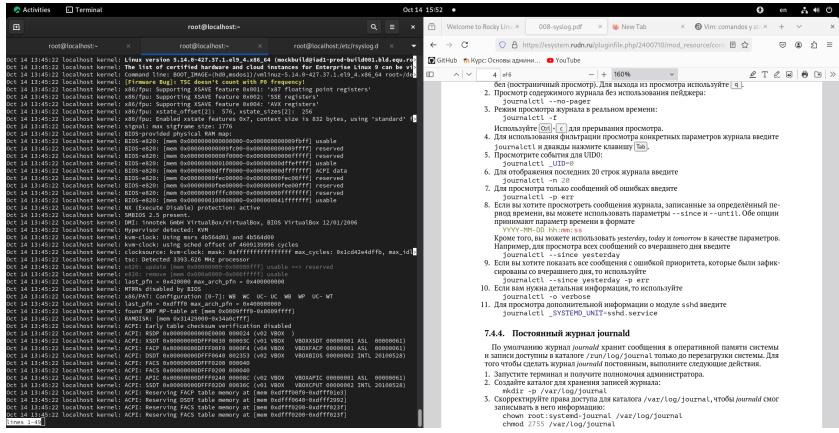


Рис. 3.32: данные журнала со вчерашнего дня

Потом только ошибки с вчерашнего дня (рис. 3.33).

```
journalctl --since yesterday -p err
```

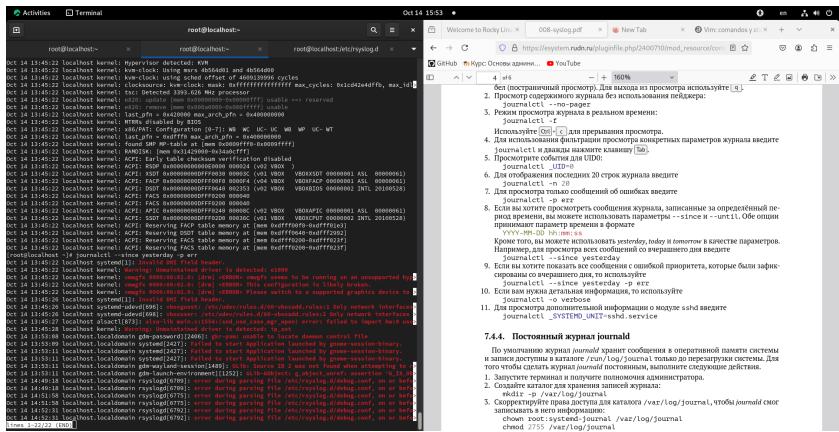


Рис. 3.33: данные журнала об ошибках со вчерашнего дня

для детальной информации я использовал следующую команду (рис. 3.34).

```
journalctl -o verbose
```

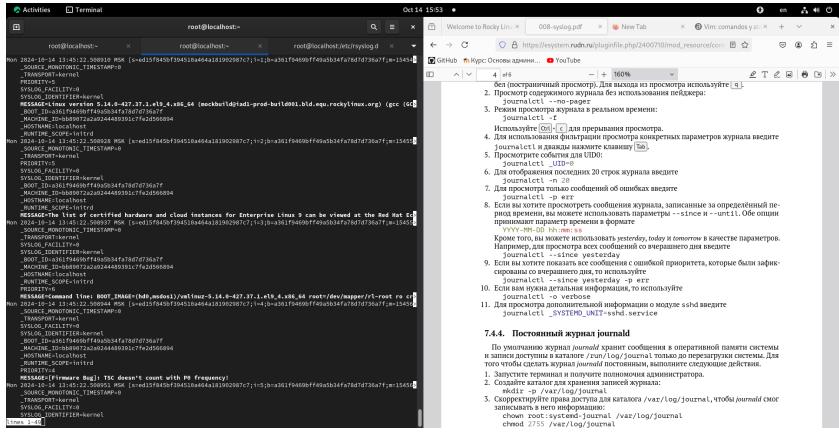


Рис. 3.34: журнал с детальной информацией

и для просмотра дополнительной информации я написал следующую команду (рис. 3.35).

```
journalctl _SYSTEMD_UNIT=sshd.service
```

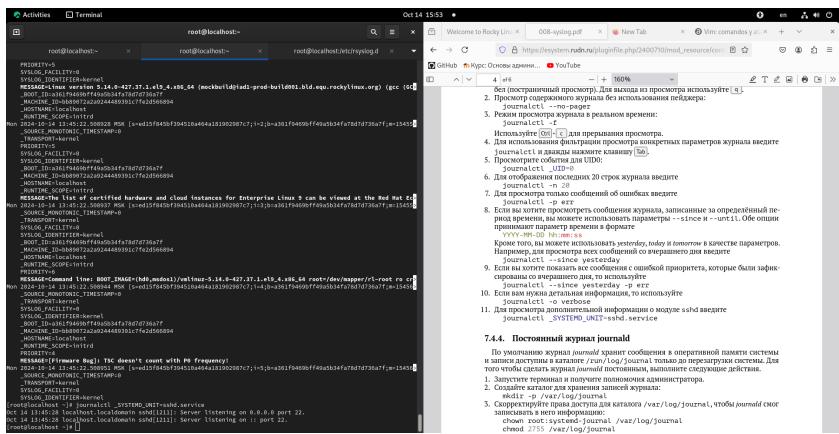


Рис. 3.35: дополнительная информация в журнале

Потом я начал следующую часть (Постоянный журнал journald). Сначала я создал новый каталог journal (рис. 3.36).

```
mkdir -p /var/log/journal
```

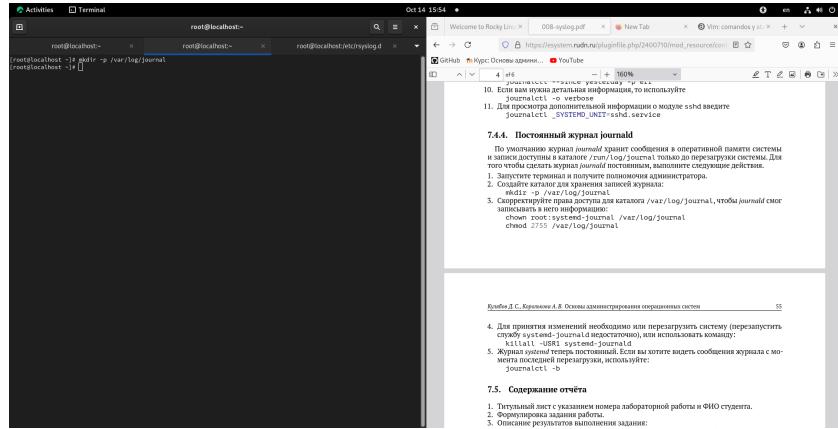


Рис. 3.36: новый каталог journal

Потом я изменил права доступа для каталога journal чтобы смог записывать в него информацию (рис. 3.37).

```
chown root:systemd-journal /var/log/journal
```

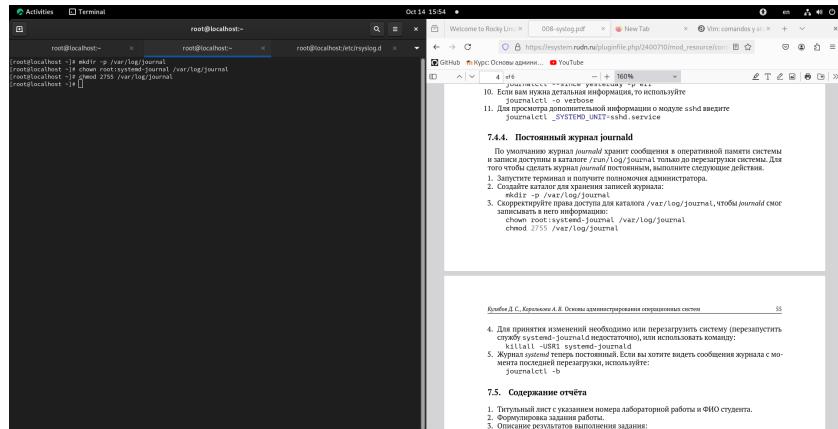


Рис. 3.37: изменение прав доступа каталога journal

Потом чтобы принимать все действия я перезапустил службу systemd-journald (рис. 3.38).

```
killall -USR1 systemd-journald
```

7.4.4. Постановка журнала journald

По умолчанию журнал выводится в оперативной памяти системы и записывается в каталог /run/согласно только до перезапуска системы. Для того чтобы сывать журналы journald постоянно, выполните следующие действия:

1. Создайте каталог для хранения записей журнала:

```
root@localhost ~%
```

2. Создайте каталог для хранения записей журнала:

```
root@localhost ~%
```

3. Создайте ссылку на каталог /var/log/journal, чтобы journald смог записывать в него информацию:

```
root@localhost ~%
```

4. Для проверки изменений необходимо или перезапустить службу journald (если это необходимо), или использовать команду:

```
journalctl -f
```

5. Журнал будет теперь постоянный. Если вы хотите видеть сообщение журнала с момента последней перезагрузки, используйте:

```
journalctl -b
```

Рис. 3.38: перезапуск службы systemd-journald

Теперь systemd постоянный и чтобы смотреть сообщения журнала с момента последней перезагрузки я ввел последнюю команду (рис. 3.39).

7.4.4. Постоянный журнал journald

По умолчанию журнал выводится в оперативной памяти системы и записывается в каталог /run/согласно только до перезапуска системы. Для того чтобы сывать журналы journald постоянно, выполните следующие действия:

1. Создайте каталог для хранения записей журнала:

```
root@localhost ~%
```

2. Создайте каталог для хранения записей журнала:

```
root@localhost ~%
```

3. Создайте ссылку на каталог /var/log/journal, чтобы journald смог записывать в него информацию:

```
root@localhost ~%
```

4. Для проверки изменений необходимо или перезапустить службу journald (если это необходимо), или использовать команду:

```
journalctl -f
```

5. Журнал будет теперь постоянный. Если вы хотите видеть сообщение журнала с момента последней перезагрузки, используйте:

```
journalctl -b
```

Рис. 3.39: сообщения в журнале

4 Выводы

После выполнения лабораторной работы я смог смотреть работу команд tail и journalctl чтобы смотреть журналы, которые сохраняют все сообщения выполнений команд или других действий и как настройт его.

Список литературы