

Отчёт о лабораторной работе

Лабораторная работа №7

Приходько Иван Иванович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	11
5	Ответы на контрольные вопросы	12

Список иллюстраций

3.1	Вывод сообщений в журнале действий	7
3.2	Изменение файла httpd.conf	8
3.3	Вывод сообщений через файл	8
3.4	Вывод сообщений через иной способ	9
3.5	Открытие сорддержимого терминала	9
3.6	Открытие сорддержимого терминала	9
3.7	Открытие сорддержимого терминала	10
3.8	Сорздание инастройка каталога для записи журнала	10

Список таблиц

1 Цель работы

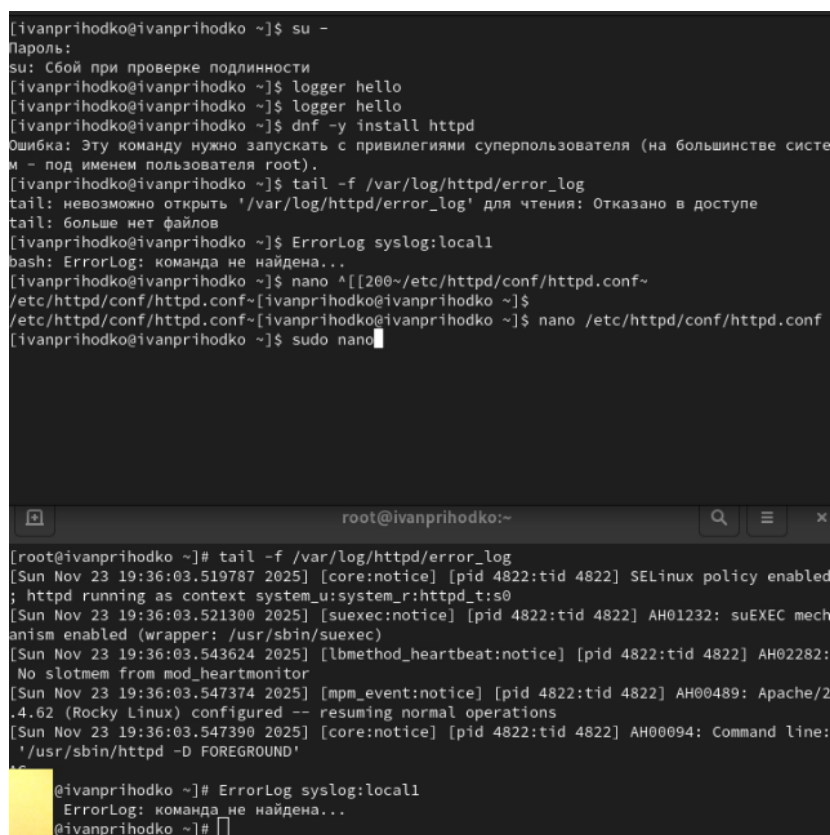
Получить навыки работы с журналами мониторинга различных событий в системе.

2 Задание

Поработать с журналом мониторинга событий в системе

3 Выполнение лабораторной работы

Для начала запустим журнал событий в другом терминале и попробуем вывести пару сообщений (рис. [3.1]).



```
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
su: Сбой при проверке подлинности
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ dnf -y install httpd
Ошибка: Эту команду нужно запускать с привилегиями суперпользователя (на большинстве систе
м - под именем пользователя root).
[ivanprihodko@ivanprihodko ~]$ tail -f /var/log/httpd/error_log
tail: невозможно открыть '/var/log/httpd/error_log' для чтения: Отказано в доступе
tail: больше нет файлов
[ivanprihodko@ivanprihodko ~]$ ErrorLog syslog:local1
bash: ErrorLog: команда не найдена...
[ivanprihodko@ivanprihodko ~]$ nano ^[[200~/etc/httpd/conf/httpd.conf~
/etc/httpd/conf/httpd.conf~[ivanprihodko@ivanprihodko ~]$
/etc/httpd/conf/httpd.conf~[ivanprihodko@ivanprihodko ~]$ nano /etc/httpd/conf/httpd.conf
[ivanprihodko@ivanprihodko ~]$ sudo nano
```

```
root@ivanprihodko:~
[root@ivanprihodko ~]# tail -f /var/log/httpd/error_log
[Sun Nov 23 19:36:03.519787 2025] [core:notice] [pid 4822:tid 4822] SELinux policy enabled
; httpd running as context system_u:system_r:httpd_t:s0
[Sun Nov 23 19:36:03.521300 2025] [suexec:notice] [pid 4822:tid 4822] AH01232: suEXEC mech
anism enabled (wrapper: /usr/sbin/suexec)
[Sun Nov 23 19:36:03.543624 2025] [lbmethod_heartbeat:notice] [pid 4822:tid 4822] AH02282:
No slotmem from mod_heartbeat
[Sun Nov 23 19:36:03.547374 2025] [mpm_event:notice] [pid 4822:tid 4822] AH00489: Apache/2
.4.62 (Rocky Linux) configured -- resuming normal operations
[Sun Nov 23 19:36:03.547390 2025] [core:notice] [pid 4822:tid 4822] AH00094: Command line:
'/usr/sbin/httpd -D FOREGROUND'
@ivanprihodko ~]# ErrorLog syslog:local1
ErrorLog: команда не найдена...
@ivanprihodko ~]#
```

Рис. 3.1: Вывод сообщений в журнале действий

Изменим файл httpd.conf (рис. [3.2]).



Рис. 3.2: Изменение файла httpd.conf

Выведем еще пару сообщений в терминале (рис. [3.3]).

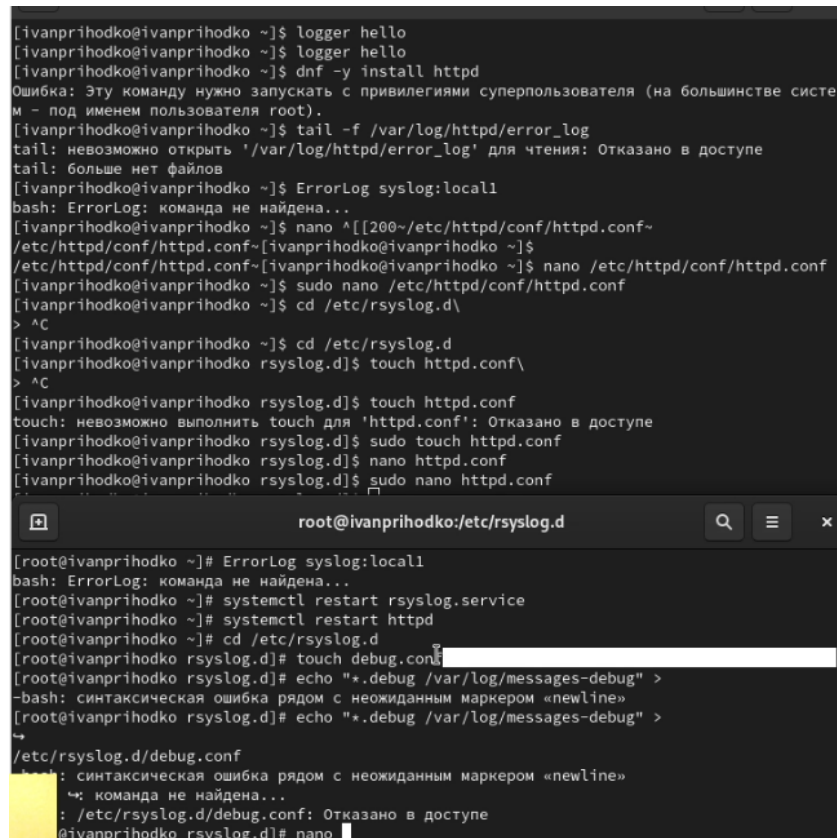
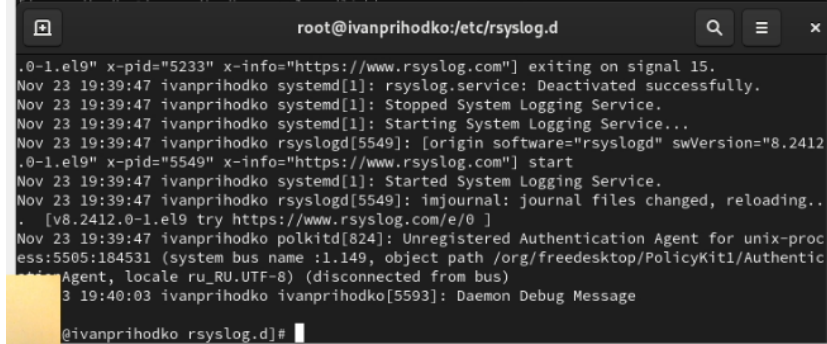


Рис. 3.3: Вывод сообщений через файл

Теперь выведем сообщение через другой способ (рис. [3.4]).


```
[ivanprihodko@ivanprihodko ~]$ cd /etc/rsyslog.d
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf\
> ^C
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf
touch: невозможно выполнить touch для 'httpd.conf': Отказано в доступе
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo touch httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ nano httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo nano httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ systemctl restart rsyslog.service
[ivanprihodko@ivanprihodko rsyslog.d]$ logger -p daemon.debug "Daemon Debug Message"
```

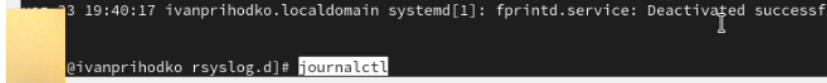


The terminal window shows the process of restarting the rsyslog service. It includes commands like 'touch httpd.conf', 'nano httpd.conf', and 'systemctl restart rsyslog.service'. The output shows the service being stopped and started, with various log messages including 'Starting System Logging Service...' and 'imjournal: journal files changed, reloading...'.

Рис. 3.4: Вывод сообщений черезиной способ

Теперь откроем содержимое терминала (рис. [3.5]-[3.7]).

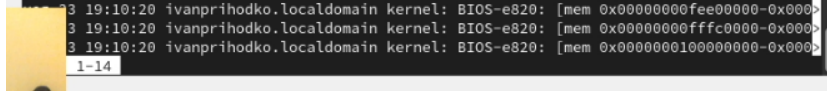
```
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Stopped System Logging Service.
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Starting System Logging Service...
ноя 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: [origin software="rsyslogd" swVer
sion="8.2412.0-1.el9" x-pid="5549" x-info="https://www.rsyslog.com"] start
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Started System Logging Service.
ноя 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: imjournal: journal files changed,
reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
ноя 23 19:39:47 ivanprihodko.localdomain polkitd[824]: Unregistered Authentication Agent f
or unix-process:5505:184531 (system bus name :1.149, object path /org/freedesktop/PolicyKi
t1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)
ноя 23 19:40:03 ivanprihodko.localdomain ivanprihodko[5593]: Daemon Debug Message
ноя 23 19:40:17 ivanprihodko.localdomain systemd[1]: fprintd.service: Deactivated successf
```



The terminal window shows the output of the 'journalctl' command. It displays a series of log messages from the system, including the stopping and starting of the rsyslog service, and a daemon debug message. The prompt is '[ivanprihodko rsyslog.d]# journalctl'.

Рис. 3.5: Открытие сордержимого терминала

```
ноя 23 19:10:20 ivanprihodko.localdomain kernel: [Firmware Bug]: TSC doesn't count with P
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-provided physical RAM map:
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000dffff000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fff00000-0x000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x000>
```



The terminal window shows kernel log messages. The first line is '[Firmware Bug]: TSC doesn't count with P'. The subsequent lines show the BIOS-provided physical RAM map and a series of BIOS-e820 entries with memory addresses. The prompt is '1-14'.

Рис. 3.6: Открытие сордержимого терминала

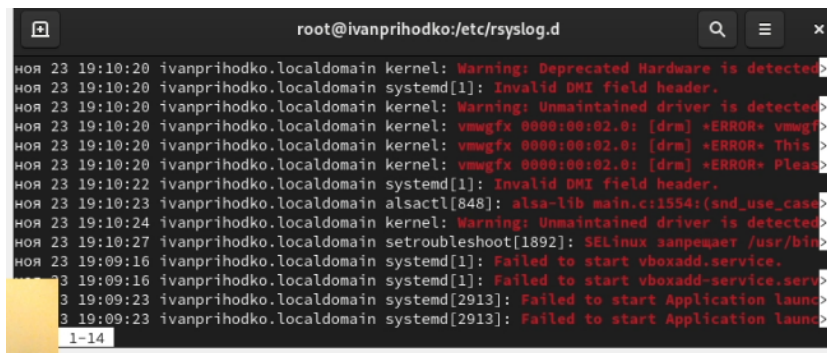


Рис. 3.7: Открытие сордержимого терминала

Теперь создадим и настроим каталог для записи журнала (рис. [3.8]).

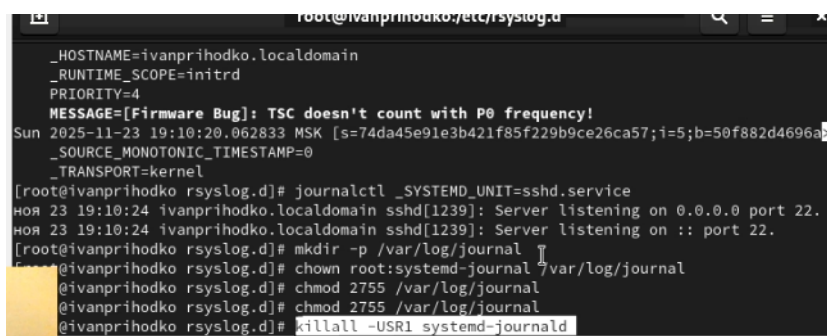


Рис. 3.8: Сорздание инастройка каталога для записи журнала

4 Выводы

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

5 Ответы на контрольные вопросы

1. `/etc/rsyslog.conf` или `/etc/rsyslog.d/`
2. `/etc/rsyslog.conf` или файлы в `/etc/rsyslog.d/`, связанные с `auth` или `authpriv`
3. Зависит от настроек, обычно — несколько секунд или минут, сразу после триггера ротации.
4. `*.info /var/log/messages.info`
5. `tail -f /var/log/messages` или `journalctl -f`
6. `journalctl _PID=1 --since "09:00" --until "15:00"`
7. `journalctl --boot` или `journalctl -b`
8. Использовать `systemctl restart systemd-journald` после настройки `/etc/systemd/journald.conf`.