

# **Лабораторная работа №7**

**Управление журналами событий в системе**

Юсупова Ксения Равиловна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>16</b>
<b>5</b>	<b>Выводы</b>	<b>17</b>

# Список иллюстраций

3.1	Выполнили пункты 1, 2 и 5 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени) . . . . .	7
3.2	Выполнили пункты 3 и 4 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени) . . . . .	8
3.3	Выполнили пункты 1 и 2 из раздела 7.4.2 (Изменение правил rsyslog.conf) . . . . .	8
3.4	Выполнили пункт 3 из раздела 7.4.2 (Изменение правил rsyslog.conf) . . . . .	9
3.5	Выполнили пункты 4, 5, 7, 10 из раздела 7.4.2 (Изменение правил rsyslog.conf) . . . . .	9
3.6	Выполнили пункты 6 и 8 из раздела 7.4.2 (Изменение правил rsyslog.conf) . . . . .	10
3.7	Выполнили пункт 9 и 11 из раздела 6.5 (Самостоятельная работа) и 6.5.2 (Задание 2) . . . . .	10
3.8	Выполнили пункты 1 и 2 из раздела 7.4.3. (Использование journalctl) . . . . .	11
3.9	Выполнили пункты 3 и 4 из раздела 7.4.3. (Использование journalctl) . . . . .	12
3.10	Выполнили пункты 4-5 из раздела 7.4.3. (Использование journalctl) . . . . .	13
3.11	Выполнили пункты 8-11 из раздела 7.4.3. (Использование journalctl) . . . . .	14
3.12	Выполнили пункты 1-5 из раздела 7.4.4. (Постоянный журнал journald) . . . . .	15

## **Список таблиц**

# **1 Цель работы**

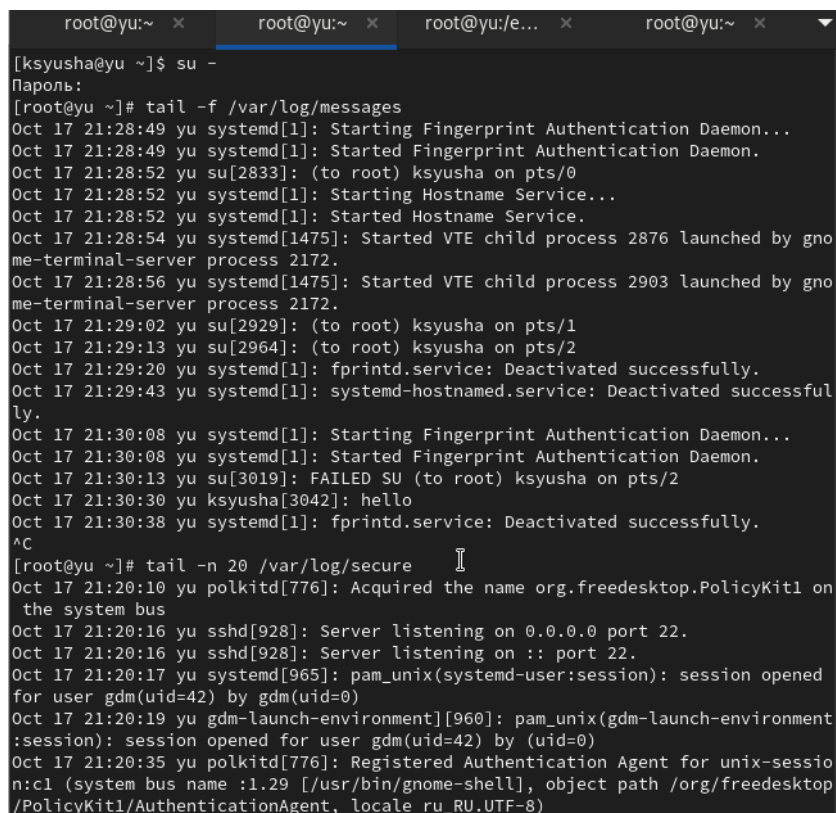
Получить навыки работы с журналами мониторинга различных событий в системе.

## 2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (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 `journal` (см. раздел 7.4.4).

### 3 Выполнение лабораторной работы

Запустили три вкладки терминала и в каждом из них получили полномочия администратора. На второй вкладке терминала запустили мониторинг системных событий в реальном времени, позже также во второй вкладке терминала с мониторингом остановили трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем запустили мониторинг сообщений безопасности (последние 20 строк соответствующего файла)(рис. 3.1).



```
root@yu:~ x root@yu:~ x root@yu:/e... x root@yu:~ x
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# tail -f /var/log/messages
Oct 17 21:28:49 yu systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 21:28:49 yu systemd[1]: Started Fingerprint Authentication Daemon.
Oct 17 21:28:52 yu su[2833]: (to root) ksyusha on pts/0
Oct 17 21:28:52 yu systemd[1]: Starting Hostname Service...
Oct 17 21:28:52 yu systemd[1]: Started Hostname Service.
Oct 17 21:28:54 yu systemd[1475]: Started VTE child process 2876 launched by gno
me-terminal-server process 2172.
Oct 17 21:28:56 yu systemd[1475]: Started VTE child process 2903 launched by gno
me-terminal-server process 2172.
Oct 17 21:29:02 yu su[2929]: (to root) ksyusha on pts/1
Oct 17 21:29:13 yu su[2964]: (to root) ksyusha on pts/2
Oct 17 21:29:20 yu systemd[1]: fprintd.service: Deactivated successfully.
Oct 17 21:29:43 yu systemd[1]: systemd-hostnamed.service: Deactivated successf
ly.
Oct 17 21:30:08 yu systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 21:30:08 yu systemd[1]: Started Fingerprint Authentication Daemon.
Oct 17 21:30:13 yu su[3019]: FAILED SU (to root) ksyusha on pts/2
Oct 17 21:30:30 yu ksyusha[3042]: hello
Oct 17 21:30:38 yu systemd[1]: fprintd.service: Deactivated successfully.
^C
[root@yu ~]# tail -n 20 /var/log/secure
Oct 17 21:20:10 yu polkitd[776]: Acquired the name org.freedesktop.PolicyKit1 on
the system bus
Oct 17 21:20:16 yu sshd[928]: Server listening on 0.0.0.0 port 22.
Oct 17 21:20:16 yu sshd[928]: Server listening on :: port 22.
Oct 17 21:20:17 yu systemd[965]: pam_unix(systemd-user:session): session opened
for user gdm(uid=42) by gdm(uid=0)
Oct 17 21:20:19 yu gdm-launch-environment[960]: pam_unix(gdm-launch-environment
:session): session opened for user gdm(uid=42) by (uid=0)
Oct 17 21:20:35 yu polkitd[776]: Registered Authentication Agent for unix-sessio
n:c1 (system bus name :1.29 [/usr/bin/gnome-shell], object path /org/freedesktop
/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
```

Рис. 3.1: Выполнили пункты 1, 2 и 5 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени)

В третьей вкладке терминала вернулись к учётной записи своего пользователя (достаточно нажать Ctrl + d) и попробовали получить полномочия администратора, но ввели неправильный пароль. Обратили внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение “FAILED SU (to root) username ...”, затем ввели logger hello (рис. 3.2).

```

root@yu:~ × root@yu:~ × root@yu:/e... × root@yu:~ ×
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]#
выход
[ksyusha@yu ~]$ su -
Пароль:
su: Сбой при проверке подлинности
[ksyusha@yu ~]$ logger hello

```

Рис. 3.2: Выполнили пункты 3 и 4 из раздела 7.4.1. (Мониторинг журнала системных событий в реальном времени)

В первой вкладке терминала установили Apache, после окончания процесса установки запустили веб-службу(рис. 3.3).

```

Установка      : rocky-logos-httpd-90.16-1.el9.noarch      9/11
Установка      : httpd-2.4.62-4.el9_6.4.x86_64          10/11
Запуск скрипта : httpd-2.4.62-4.el9_6.4.x86_64          10/11
Установка      : mod_http2-2.0.26-4.el9_6.1.x86_64       11/11
Запуск скрипта : httpd-2.4.62-4.el9_6.4.x86_64          11/11
Запуск скрипта : mod_http2-2.0.26-4.el9_6.1.x86_64       11/11
Проверка       : apr-util-bdb-1.6.1-23.el9.x86_64        1/11
Проверка       : httpd-tools-2.4.62-4.el9_6.4.x86_64     2/11
Проверка       : httpd-2.4.62-4.el9_6.4.x86_64           3/11
Проверка       : apr-util-1.6.1-23.el9.x86_64            4/11
Проверка       : rocky-logos-httpd-90.16-1.el9.noarch     5/11
Проверка       : httpd-core-2.4.62-4.el9_6.4.x86_64      6/11
Проверка       : httpd-filesystem-2.4.62-4.el9_6.4.noarch 7/11
Проверка       : mod_lua-2.4.62-4.el9_6.4.x86_64         8/11
Проверка       : mod_http2-2.0.26-4.el9_6.1.x86_64       9/11
Проверка       : apr-util-openssl-1.6.1-23.el9.x86_64    10/11
Проверка       : apr-1.7.0-12.el9_3.x86_64              11/11

Установлен:
apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64
apr-util-bdb-1.6.1-23.el9.x86_64 apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.62-4.el9_6.4.x86_64 httpd-core-2.4.62-4.el9_6.4.x86_64
httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x86_64
mod_http2-2.0.26-4.el9_6.1.x86_64 mod_lua-2.4.62-4.el9_6.4.x86_64
rocky-logos-httpd-90.16-1.el9.noarch

Выполнено!
[root@yu ~]# systemctl start httpd
[root@yu ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.

```

Рис. 3.3: Выполнили пункты 1 и 2 из раздела 7.4.2 (Изменение правил rsyslog.conf)



о второй вкладке терминала посмотрели журнал сообщений об ошибках веб-службы(рис. 3.4).

```
[root@yu ~]# tail -f /var/log/httpd/error_log
[Fri Oct 17 21:32:16.616026 2025] [core:notice] [pid 3532:tid 3532] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 17 21:32:16.617162 2025] [suexec:notice] [pid 3532:tid 3532] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 17 21:32:16.766628 2025] [lbmethod_heartbeat:notice] [pid 3532:tid 3532] AH02282: No slotmem from mod_heartbeat
[Fri Oct 17 21:32:16.774704 2025] [mpm_event:notice] [pid 3532:tid 3532] AH00489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 17 21:32:16.774741 2025] [core:notice] [pid 3532:tid 3532] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
```

Рис. 3.4: Выполнили пункт 3 из раздела 7.4.2 (Изменение правил rsyslog.conf)

В третьей вкладке терминала получили полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавьте следующую строку: `ErrorLog syslog:local1`. Здесь `local0` — `local7` — это «настраиваемые» средства (объекты), которые `syslog` предоставляет пользователю для регистрации событий приложения в системном журнале. В каталоге /etc/rsyslog.d создали файл мониторинга событий веб-службы. Открыв его на редактирование, прописали в нём `local1.* -/var/log/httpd-error.log`. Эта строка позволит отправлять все сообщения, получаемые для объекта `local1`. Позже создали отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале ввели `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf` и `logger -p daemon.debug "Daemon Debug Message"`(рис. 3.5).

```
[root@yu ~]# nano /etc/httpd/conf/httpd.conf
[root@yu ~]# cd /etc/rsyslog.d
[root@yu rsyslog.d]# touch httpd.conf
[root@yu rsyslog.d]# nano httpd.conf
[root@yu rsyslog.d]# cd /etc/rsyslog.d
[root@yu rsyslog.d]# touch debug.conf
[root@yu rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@yu rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
```

Рис. 3.5: Выполнили пункты 4, 5, 7, 10 из раздела 7.4.2 (Изменение правил rsyslog.conf)

Перешли в первую вкладку терминала и перезагрузили конфигурацию `rsyslogd` и веб-службу, позже снова перезапустили `rsyslogd`(рис. 3.6).

```
[root@yu ~]# systemctl restart rsyslog.service
[root@yu ~]# systemctl restart httpd
[root@yu ~]# systemctl restart rsyslog.service
```

Рис. 3.6: Выполнили пункты 6 и 8 з раздела 7.4.2 (Изменение правил rsyslog.conf)

Во второй вкладке терминала запустили мониторинг отладочной информации, позже посмотрели сообщение отладки.(рис. 3.7).

```
[root@yu ~]# tail -f /var/log/messages-debug
Oct 17 21:41:02 yu systemd[1]: Stopping System Logging Service...
Oct 17 21:41:02 yu rsyslogd[3912]: [origin software="rsyslogd" swVersion="8.2412
.0-1.el9" x-pid="3912" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 17 21:41:02 yu systemd[1]: rsyslog.service: Deactivated successfully.
Oct 17 21:41:02 yu systemd[1]: Stopped System Logging Service.
Oct 17 21:41:02 yu systemd[1]: Starting System Logging Service...
Oct 17 21:41:02 yu rsyslogd[4127]: [origin software="rsyslogd" swVersion="8.2412
.0-1.el9" x-pid="4127" x-info="https://www.rsyslog.com"] start
Oct 17 21:41:02 yu systemd[1]: Started System Logging Service.
Oct 17 21:41:02 yu rsyslogd[4127]: imjournal: journal files changed, reloading..
. [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 17 21:41:28 yu root[4140]: Daemon Debug Message
^C
```

Рис. 3.7: Выполнили пункт 9 и 11 из раздела 6.5 (Самостоятельная работа) и 6.5.2 (Задание 2)

Во второй вкладке терминала посмотрели содержимое журнала с событиями с момента последнего запуска системы и содержимого журнала без использования пейджера(рис. 3.8).

```

ОКТ 17 21:19:52 yu.k.r kernel: VFS: Disk quotas dquot_6.6.0
ОКТ 17 21:19:52 yu.k.r kernel: VFS: Dquot-cache hash table entries: 512 (order 2)
ОКТ 17 21:19:52 yu.k.r kernel: pnp: PnP ACPI init
ОКТ 17 21:19:52 yu.k.r kernel: pnp: PnP ACPI: found 2 devices
ОКТ 17 21:19:52 yu.k.r kernel: clocksource: acpi_pm: mask: 0xffffffff max_cycles: 2147483647
ОКТ 17 21:19:52 yu.k.r kernel: NET: Registered PF_INET protocol family
ОКТ 17 21:19:52 yu.k.r kernel: IP idents hash table entries: 131072 (order: 8, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: tcp_listen_portaddr_hash hash table entries: 4096 (order: 16, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: Table-perturb hash table entries: 65536 (order: 16, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: TCP established hash table entries: 65536 (order: 16, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: TCP bind hash table entries: 65536 (order: 8, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: TCP: Hash tables configured (established 65536 bind 65536)
ОКТ 17 21:19:52 yu.k.r kernel: MPTCP token hash table entries: 8192 (order: 5, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: UDP hash table entries: 4096 (order: 5, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: UDP-Lite hash table entries: 4096 (order: 5, 131072 bytes)
ОКТ 17 21:19:52 yu.k.r kernel: NET: Registered PF_UNIX/PF_LOCAL protocol family
ОКТ 17 21:19:52 yu.k.r kernel: NET: Registered PF_XDP protocol family
ОКТ 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 4 [io 0x0000-0x0cf7 window 0x0000-0x0cf7]
ОКТ 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 5 [io 0x0d00-0xffff window 0x0000-0xffff]
ОКТ 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 6 [mem 0x000a0000-0x000bffff window 0x0000-0xffff]
[root@yu ~]# journalctl --no-pager
ОКТ 17 21:19:52 yu.k.r kernel: Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockb
uild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red
Hat 11.5.0-5), GNU ld version 2.35.2-63.el9) #1 SMP PREEMPT_DYNAMIC Fri May 23 2
2:47:01 UTC 2025
ОКТ 17 21:19:52 yu.k.r kernel: The list of certified hardware and cloud instance
s for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https:/
/catalog.redhat.com.
ОКТ 17 21:19:52 yu.k.r kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.1
4.0-570.17.1.el9_6.x86_64 root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap
rd.lvm.lv=rl/root rd.lvm.lv=rl/swap rhgb quiet
ОКТ 17 21:19:52 yu.k.r kernel: [Firmware Bug]: TSC doesn't count with P0 frequen
cy!
ОКТ 17 21:19:52 yu.k.r kernel: BIOS-provided physical RAM map:

```

Рис. 3.8: Выполнили пункты 1 и 2 из раздела 7.4.3. (Использование journalctl)

Посмотрели режим просмотра журнала в реальном времени. Для использования фильтрации просмотра конкретных параметров журнала ввели journalctl и дважды нажали клавишу Tab(рис. 3.9).

```

[root@yu ~]# journalctl -f
окт 17 21:40:55 yu.k.r gnome-shell[1570]: libinput error: event3 - ImExPS/2 Gen
eric Explorer Mouse: client bug: event processing lagging behind by 11ms, your s
ystem is too slow
окт 17 21:41:02 yu.k.r systemd[1]: Stopping System Logging Service...
окт 17 21:41:02 yu.k.r rsyslogd[3912]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="3912" x-info="https://www.rsyslog.com"] exiting on signal 1
5.
окт 17 21:41:02 yu.k.r systemd[1]: rsyslog.service: Deactivated successfully.
окт 17 21:41:02 yu.k.r systemd[1]: Stopped System Logging Service.
окт 17 21:41:02 yu.k.r systemd[1]: Starting System Logging Service...
окт 17 21:41:02 yu.k.r rsyslogd[4127]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="4127" x-info="https://www.rsyslog.com"] start
окт 17 21:41:02 yu.k.r systemd[1]: Started System Logging Service.
окт 17 21:41:02 yu.k.r rsyslogd[4127]: imjournal: journal files changed, reloadi
ng... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
окт 17 21:41:28 yu.k.r root[4140]: Daemon Debug Message
^C
[root@yu ~]# journalctl
Display all 111 possibilities? (y or n)
_AUDIT_LOGINUID=
_AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
COMMAND=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=

```

Рис. 3.9: Выполнили пункты 3 и 4 из раздела 7.4.3. (Использование journalctl)

Просмотрели события для UID0. Для отображения последних 20 строк журнала ввели `journalctl -n 20` и для просмотра только сообщений об ошибках `journalctl -p err` (рис. 3.10).

```

ОКТ 17 21:19:55 yu.k.r systemd[1]: Finished File System Check on /dev/mapper/rl
ОКТ 17 21:19:55 yu.k.r systemd[1]: Mounting /sysroot...
ОКТ 17 21:19:56 yu.k.r systemd[1]: Mounted /sysroot.
ОКТ 17 21:19:56 yu.k.r systemd[1]: Reached target Initrd Root File System.
ОКТ 17 21:19:56 yu.k.r systemd[1]: Starting Mountpoints Configured in the Real
ОКТ 17 21:19:56 yu.k.r systemd[1]: initrd-parse-etc.service: Deactivated succes
ОКТ 17 21:19:56 yu.k.r systemd[1]: Finished Mountpoints Configured in the Real
ОКТ 17 21:19:56 yu.k.r systemd[1]: Reached target Initrd File Systems.
[root@yu ~]# journalctl -n 20
ОКТ 17 21:39:21 yu.k.r systemd[1]: Starting System Logging Service...
ОКТ 17 21:39:21 yu.k.r systemd[1]: Started System Logging Service.
ОКТ 17 21:39:21 yu.k.r rsyslogd[3912]: [origin software="rsyslogd" swVersion="8
ОКТ 17 21:39:21 yu.k.r rsyslogd[3912]: imjournal: journal files changed, reload
ОКТ 17 21:39:27 yu.k.r systemd[1]: Stopping The Apache HTTP Server...
ОКТ 17 21:39:28 yu.k.r systemd[1]: httpd.service: Deactivated successfully.
ОКТ 17 21:39:28 yu.k.r systemd[1]: Stopped The Apache HTTP Server.
ОКТ 17 21:39:28 yu.k.r systemd[1]: Starting The Apache HTTP Server...
ОКТ 17 21:39:28 yu.k.r httpd[3924]: Server configured, listening on: port 80
ОКТ 17 21:39:28 yu.k.r systemd[1]: Started The Apache HTTP Server.
ОКТ 17 21:40:55 yu.k.r gnome-shell[1570]: libinput error: event3 - ImExPS/2 Ge
ОКТ 17 21:41:02 yu.k.r systemd[1]: Stopping System Logging Service...
ОКТ 17 21:41:02 yu.k.r rsyslogd[3912]: [origin software="rsyslogd" swVersion="8
ОКТ 17 21:41:02 yu.k.r systemd[1]: rsyslog.service: Deactivated successfully.
ОКТ 17 21:41:02 yu.k.r systemd[1]: Stopped System Logging Service.
ОКТ 17 21:41:02 yu.k.r systemd[1]: Starting System Logging Service...
ОКТ 17 21:41:02 yu.k.r rsyslogd[4127]: [origin software="rsyslogd" swVersion="8
ОКТ 17 21:41:02 yu.k.r systemd[1]: Started System Logging Service.
ОКТ 17 21:41:02 yu.k.r rsyslogd[4127]: imjournal: journal files changed, reload
ОКТ 17 21:41:28 yu.k.r root[4140]: Daemon Debug Message
[root@yu ~]# journalctl -p err
ОКТ 17 21:19:52 yu.k.r kernel: Warning: Deprecated Hardware is detected: x86_64
ОКТ 17 21:19:52 yu.k.r systemd[1]: Invalid DMI field header.
ОКТ 17 21:19:53 yu.k.r kernel: Warning: Unmaintained driver is detected: e1000
ОКТ 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems
ОКТ 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configur
ОКТ 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch
ОКТ 17 21:20:01 yu.k.r systemd[1]: Invalid DMI field header.
ОКТ 17 21:20:08 yu.k.r alsactl[806]: alsa-lib main.c:1554:(snd_use_case_mgr_ope

```

Рис. 3.10: Выполнили пункты 4-5 из раздела 7.4.3. (Использование journalctl)

Для просмотра всех сообщений со вчерашнего дня ввели `journalctl -since yesterday`, чтобы показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то использовали `journalctl -since yesterday -p err`, для детальной информации ввели `journalctl -o verbose`, для просмотра дополнительной информации о модуле `sshd` ввели `journalctl _SYSTEMD_UNIT=sshd.service` (рис. 3.11).

```

окт 17 21:19:52 yu.k.r kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
окт 17 21:19:52 yu.k.r kernel: RAMDISK: [mem 0x30aa5000-0x3454afff]
окт 17 21:19:52 yu.k.r kernel: ACPI: Early table checksum verification disabled
окт 17 21:19:52 yu.k.r kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
окт 17 21:19:52 yu.k.r kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX )
[root@yu ~]# journalctl --since yesterday -p err
окт 17 21:19:52 yu.k.r kernel: Warning: Deprecated Hardware is detected: x86_64
окт 17 21:19:52 yu.k.r systemd[1]: Invalid DMI field header.
окт 17 21:19:53 yu.k.r kernel: Warning: Unmaintained driver is detected: el000
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configur
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch
окт 17 21:20:01 yu.k.r systemd[1]: Invalid DMI field header.
окт 17 21:20:08 yu.k.r alsactl[806]: alsa-lib main.c:1554:(snd_use_case_mgr_ope
окт 17 21:20:15 yu.k.r kernel: Warning: Unmaintained driver is detected: ip_set
окт 17 21:20:27 yu.k.r setroubleshoot[823]: SELinux запрещает /usr/bin/lsmd doc
окт 17 21:20:54 yu.k.r systemd[1475]: Failed to start Application launched by g
окт 17 21:21:01 yu.k.r gdm-wayland-session[1023]: GLib: Source ID 2 was not fou
окт 17 21:21:01 yu.k.r gdm-launch-environment[960]: GLib-GObject: g_object_unr
[root@yu ~]# journalctl -o verbose
Fri 2025-10-17 21:19:52.950551 MSK [s=ce6273bddcf5474ba775f0e3c93e99b3;i=1;b=98
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockbuild@iad1-prod-bui
_BOOT_ID=984507a3bf2645daaec282806b0eb29d
_MACHINE_ID=fea32d02ff8b4e2695eb396f08cec4f5
_HOSTNAME=yu.k.r
_RUNTIME_SCOPE=initrd
Fri 2025-10-17 21:19:52.950581 MSK [s=ce6273bddcf5474ba775f0e3c93e99b3;i=2;b=98
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=984507a3bf2645daaec282806b0eb29d

```

Рис. 3.11: Выполнили пункты 8-11 из раздела 7.4.3. (Использование journalctl)

Запустили терминал и получили полномочия администратора. Создали каталог для хранения записей журнала, скорректировали права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: killall -USR1 systemd-journald. Журнал systemd теперь постоянный, чтобы видеть сообщения журнала с момента последней перезагрузки journalctl -b(рис. 3.12).

```

[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# mkdir -p /var/log/journal
[root@yu ~]# chown root:systemd-journal /var/log/journal
[root@yu ~]# chmod 2755 /var/log/journal
[root@yu ~]# killall -USR1 systemd-journald
[root@yu ~]# journalctl -b
окт 17 21:19:52 yu.k.r kernel: Linux version 5.14.0-570.17.1.el9_6.x86_64 (mock>
окт 17 21:19:52 yu.k.r kernel: The list of certified hardware and cloud instanc>
окт 17 21:19:52 yu.k.r kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.>
окт 17 21:19:52 yu.k.r kernel: [Firmware Bug]: TSC doesn't count with P0 frequ>
окт 17 21:19:52 yu.k.r kernel: BIOS-provided physical RAM map:
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000dffa>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x000000000dffff0000-0x00000000dffa>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffa>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x0000000100000000-0x000000021ffa>
окт 17 21:19:52 yu.k.r kernel: NX (Execute Disable) protection: active
окт 17 21:19:52 yu.k.r kernel: APIC: Static calls initialized
окт 17 21:19:52 yu.k.r kernel: SMBIOS 2.5 present.
окт 17 21:19:52 yu.k.r kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vi>
окт 17 21:19:52 yu.k.r kernel: Hypervisor detected: KVM
окт 17 21:19:52 yu.k.r kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
окт 17 21:19:52 yu.k.r kernel: kvm-clock: using sched offset of 8008313700 cycl>
окт 17 21:19:52 yu.k.r kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff>
окт 17 21:19:52 yu.k.r kernel: tsc: Detected 2295.690 MHz processor
окт 17 21:19:52 yu.k.r kernel: e820: update [mem 0x00000000-0x000000ffff] usable >
окт 17 21:19:52 yu.k.r kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
окт 17 21:19:52 yu.k.r kernel: last_pfn = 0x220000 max_arch_pfn = 0x400000000
окт 17 21:19:52 yu.k.r kernel: MTRRs disabled by BIOS
окт 17 21:19:52 yu.k.r kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB>
окт 17 21:19:52 yu.k.r kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000

```

Рис. 3.12: Выполнили пункты 1-5 из раздела 7.4.4. (Постоянный журнал journald)

## 4 Ответы на контрольные вопросы

1. Для настройки rsyslogd используется файл `/etc/rsyslog.conf`.
2. Сообщения, связанные с аутентификацией, содержатся в файле `/var/log/secure`.
3. Без дополнительной настройки ротация файлов журналов выполняется еженедельно.
4. Для записи сообщений с приоритетом `info` в файл `/var/log/messages.info` следует добавить строку: `*.info /var/log/messages.info`
5. Команда `tail -f /var/log/messages` позволяет просматривать сообщения журнала в реальном времени.
6. Команда `journalctl _PID=1 -since "09:00" -until "15:00"` показывает сообщения для PID 1 за указанный период.
7. Команда `journalctl -b` отображает сообщения `journald` с последней перезагрузки системы.
8. Для создания постоянного журнала `journald` необходимо создать директорию `/var/log/journal` и перезапустить службу `systemd-journald`.



## **5 Выводы**

В ходе лабораторной работы мы получили навыки работы с журналами мониторинга различных событий в системе.