

# Управление журналами событий в системе

## Лабораторная работа №7

---

Казначеев С.И.

10 октября 2025

Российский университет дружбы народов, Москва, Россия

## Информация

---

::::::::::: {.columns align=center} :: {.column width="70%"}  
:::

- Казначеев Сергей Ильич
- Студент
- Российский университет дружбы народов
- [1132240693@pfur.ru] :: {.column width="30%"}  
::

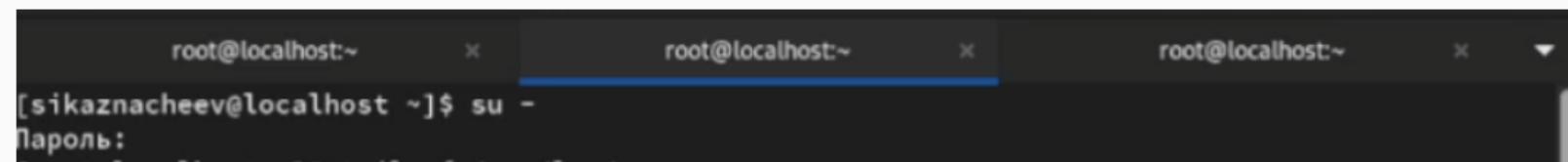
## Цель работы

---

Получить навыки работы с журналами мониторинга различных событий в системе.

## Выполнение лабораторной работы

Для начала откроем три вкладки терминала и в каждом из них получим полномочия администратора



The screenshot shows three separate terminal windows, each with a dark background and white text. The first window on the left has the prompt `[sikaznacheev@localhost ~]$`. The second window in the middle has the prompt `root@localhost:~`. The third window on the right also has the prompt `root@localhost:~`. A blue horizontal bar highlights the second window, indicating it is active. In the active window, the command `su -` is being typed, followed by a password prompt `Пароль:`.

Рис. 1: 1

## Действия во втором терминале

Теперь во второй вкладке пропишем команду tail -f /var/log/messages чтобы вывести события в реальном времени. После чего перейдем в 3 терминал и попробуем зайти в супер пользователя введя неправильный пароль и у нас во 2 терминале появится сообщение «FAILED SU (to root) username ...».

```
[root@localhost ~]# tail -f /var/log/messages
Oct 10 12:49:51 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 10 12:49:51 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 10 12:49:53 localhost su[4087]: (to root) sikaznacheev on pts/0
Oct 10 12:49:53 localhost systemd[1]: Starting Hostname Service...
Oct 10 12:49:53 localhost systemd[1]: Started Hostname Service.
Oct 10 12:49:54 localhost systemd[2305]: Started VTE child process 4132 launched by gnome-terminal-server process 3847.
Oct 10 12:50:00 localhost su[4161]: (to root) sikaznacheev on pts/1
Oct 10 12:50:07 localhost systemd[2305]: Started VTE child process 4218 launched by gnome-terminal-server process 3847.
Oct 10 12:50:14 localhost su[4247]: (to root) sikaznacheev on pts/2
Oct 10 12:50:21 localhost systemd[1]: fprintd.service: Deactivated successfully.
Oct 10 12:50:44 localhost systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 10 12:50:57 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
```

## Действия в третьем терминале

После в 3 терминале введем из оболочки пользователя logger hello

```
[sikaznacheev@localhost ~]$ logger hello  
[sikaznacheev@localhost ~]$ █ █
```

Рис. 3: 3

## Проверка действий

Далее открываем второй терминал и проверяя то что hello записалось

```
Oct 10 12:51:23 localhost sikaznacheev[4334]: hello
```

Рис. 4: 4

## Проверка сообщений

Затем введем команду tail -n 20 /var/log/secure чтобы увидеть сообщения, которые ранее были зафиксированы во время ошибки

```
[root@localhost ~]# tail -n 20 /var/log/secure
```

Рис. 5: 5

## Установка нового пакета

В первой вкладке установим httpd

```
[root@localhost ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64           15 kB/s | 13 kB     00
Extra Packages for Enterprise Linux 9 - x86_64           6.0 MB/s | 20 MB     00
Rocky Linux 9 - BaseOS      [=====] --- B/s | 0 B     --
```

Рис. 6: 6

## Запуск веб-служб

После окончания процесса установки запустим веб-службу

```
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/s
ystem/httpd.service.
[root@localhost ~]
```

Рис. 7: 7

## Работа во втором терминале

После во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-служб командой tail -f /var/log/httpd/error\_log

```
on): session opened for user gdm(uid=42) by (uid=0)
Oct 10 12:37:11 localhost polkitd[879]: Registered Authentication Agent for unix-session:c1 (system bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: unable to locate daemon control file
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: stashed password to try later in open session
Oct 10 12:39:28 localhost systemd[2305]: pam_unix(systemd-user:session): session opened for user sikaznacheev(uid=1000) by sikaznacheev(uid=0)
Oct 10 12:39:28 localhost gdm-password[2283]: pam_unix(gdm-password:session): session opened for user sikaznacheev(uid=1000) by sikaznacheev(uid=0)
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 12:39:31 localhost polkitd[879]: Registered Authentication Agent for unix-session:2 (system bus name :1.73 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 10 12:39:39 localhost polkitd[879]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)
Oct 10 12:39:39 localhost gdm-launch-environment[1266]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 10 12:49:53 localhost su[4087]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:00 localhost su[4161]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:14 localhost su[4247]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:55 localhost su[4247]: pam_unix(su-l:session): session closed for user root
Oct 10 12:50:59 localhost unix_chkpwd[4324]: password check failed for user (root)
Oct 10 12:50:59 localhost su[4317]: pam_unix(su-l:auth): authentication failure; logname=sikaznacheev uid=1000 euid=0 tty/dev/pts/2 ruser=sikaznacheev rhost= user=root
[root@localhost ~]# tail -f /var/log/httpd/error_log
[Fri Oct 10 12:53:54.282931 2025] [core:notice] [pid 14466:tid 14466] SELinux policy enabled;
httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 10 12:53:54.283326 2025] [suexec:notice] [pid 14466:tid 14466] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
```

## Работа в третьем терминале

Далее в 3 терминале запишем в файл конфигурации /etc/httpd/conf/httpd.conf в конце добавим ErrorLog syslog:local1

```
# Load configuration files in the /etc/httpd/conf.d directory, if any.  
IncludeOptional conf.d/*.conf  
  
ErrorLog syslog:local1
```

Рис. 9: 9

## Создание нового файла

После чего переходим в каталог /etc/rsyslog.d и создаем файл мониторинга событий веб-службы

```
[root@localhost ~]# cd /etc/rsyslog.d
[root@localhost rsyslog.d]# touch httpd.conf
```

Рис. 10: 10

## Редактируем его

Далее открыв его на редактировании запишем local1.\* -/var/log/httpd-error.log

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

Рис. 11: 11

## Работа в первом терминале

После чего переходим в первую вкладку терминала и перезагружаем конфигурацию rsyslogd и веб-службу

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

Рис. 12: 12

## Работа в третьей вкладке

После в третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации и в том же терминале вводим echo “\*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf

```
[root@localhost ~]# cd /etc/rsyslog.d
[root@localhost rsyslog.d]# touch debug.conf
[root@localhost rsyslog.d]# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
[root@localhost rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@localhost rsyslog.d]# █
```

Рис. 13: 13

## Работа в первом терминале

Затем в первой вкладке терминала снова перезапускаем rsyslogd

```
[root@localhost ~]# systemctl restart rsyslog.service  
[root@localhost ~]# █
```

Рис. 14: 14

## Работа во второй вкладке

Далее переходим во вторую вкладку терминала запускаем мониторинг отладочной информации tail -f /var/log/messages-debug

```
^C
[root@localhost ~]# tail -f /var/log/messages-debug
```

Рис. 15: 15

## Работа в третьей вкладке

Далее в третьей вкладке терминала введем logger -p daemon.debug "Daemon Debug Message"

```
[root@localhost rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"  
[root@localhost rsyslog.d]# █
```

Рис. 16: 16

## Проверка действий

Проверим это

```
Oct 10 13:00:39 localhost root[46274]: Daemon Debug Message
```

Рис. 17: 17

## Работа во второй вкладке

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы

```
окт 10 12:36:43 localhost kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-  
окт 10 12:36:43 localhost kernel: The list of certified hardware and cloud instances for Enter  
окт 10 12:36:43 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.  
окт 10 12:36:43 localhost kernel: BIOS-provided physical RAM map:  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usab  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserv  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000f0000-0x0000000000ffff] reserv  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfffffff] usab  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserv  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserv  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserv  
окт 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000021fffffff] usab  
окт 10 12:36:43 localhost kernel: NX (Execute Disable) protection: active  
окт 10 12:36:43 localhost kernel: APIC: Static calls initialized  
окт 10 12:36:43 localhost kernel: SMBIOS 2.5 present.  
окт 10 12:36:43 localhost kernel: DMI: innotech GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12  
окт 10 12:36:43 localhost kernel: Hypervisor detected: KVM  
окт 10 12:36:43 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
окт 10 12:36:43 localhost kernel: kvm-clock: using sched offset of 6225533528 cycles  
окт 10 12:36:43 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles  
окт 10 12:36:43 localhost kernel: tsc: Detected 3686.398 MHz processor  
окт 10 12:36:43 localhost kernel: e820: update [mem 0x0000000000-0x0000ffff] usable ==> reserved  
окт 10 12:36:43 localhost kernel: e820: remove [mem 0x000a0000-0x000ffff] usable  
окт 10 12:36:43 localhost kernel: last_pfn = 0x220000 max_arch_pfn = 0x400000000  
окт 10 12:36:43 localhost kernel: MTRRs disabled by BIOS  
окт 10 12:36:43 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WP  
окт 10 12:36:43 localhost kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000  
окт 10 12:36:43 localhost kernel: found SMP MP-table at [mem 0x0009ff00-0x0009ffff]  
окт 10 12:36:43 localhost kernel: RAMDISK: [mem 0x30c7b000-0x34635fff]  
окт 10 12:36:43 localhost kernel: ACPI: Early table checksum verification disabled  
окт 10 12:36:43 localhost kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )  
окт 10 12:36:43 localhost kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX  VBOXXSDT 0)  
окт 10 12:36:43 localhost kernel: ACPI: FACP 0x00000000DFFF00F4 0000F4 (v04 VBOX  VBOXFACP 0)  
окт 10 12:36:43 localhost kernel: ACPI: DSDT 0x00000000DFFF0640 002353 (v02 VBOX  VBOXBIOS 0)  
окт 10 12:36:43 localhost kernel: ACPI: FACS 0x00000000DFFF0200 000040
```

## Просмотр содержимого журнала

Затем просмотрим содержимое журнала без использования пейджера командой journalctl -no-pager и просмотрим журнал в реальном времени journalctl -f

```
OKT 10 12:58:05 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 12:58:08 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 12:58:08 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46035" x-info="https://www.rsyslog.com"] start
OKT 10 12:58:08 localhost.localdomain rsyslogd[46035]: imjournal: journal files changed, reloading...
[v8.2412.0-1.el9 try https://www.rsyslog.com/e/0]
OKT 10 12:58:15 localhost.localdomain systemd[1]: Stopping The Apache HTTP Server...
OKT 10 12:58:16 localhost.localdomain systemd[1]: httpd.service: Deactivated successfully.
OKT 10 12:58:16 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
OKT 10 12:58:16 localhost.localdomain systemd[1]: httpd.service: Consumed 1.264s CPU time.
OKT 10 12:58:17 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
OKT 10 12:58:17 localhost.localdomain httpd[46046]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
OKT 10 12:58:17 localhost.localdomain httpd[46046]: Server configured, listening on: port 80
OKT 10 12:58:17 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
OKT 10 12:59:31 localhost.localdomain PackageKit[4923]: daemon quit
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Deactivated successfully.
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Consumed 19.543s CPU time.
OKT 10 13:00:01 localhost.localdomain gnome-shell[2391]: libinput error: client bug: timer event5 debounce short: scheduled expiry is in the past (-12ms), your system is too slow
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopping System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46035" x-info="https://www.rsyslog.com"] exiting on signal 15.
OKT 10 13:00:04 localhost.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopped System Logging Service.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46265" x-info="https://www.rsyslog.com"] start
OKT 10 13:00:04 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: imjournal: journal files changed, reloading...
[v8.2412.0-1.el9 try https://www.rsyslog.com/e/0]
OKT 10 13:00:39 localhost.localdomain root[46274]: Daemon Debug Message
OKT 10 13:01:01 localhost.localdomain CROND[46284]: (root) CMD (run-parts /etc/cron.hourly)
```

## Фильтрация просмотра

После чего используем фильтрацию просмотра конкретных параметров журнала введя команду journalctl и дважды нажав на tab

```
[root@localhost ~]# journalctl  
Display all 107 possibilities? (y or n)
```

Рис. 20: 20

## Проверка событий uid0

Пробуем просмотреть события для uid0

```
[root@localhost ~]# journalctl _UID=0
```

Рис. 21: 21

## Запуск journalctl

После чего запустим journalctl -n 20 для просмотра только сообщений об ошибке используем комаду journalctl -p err

```
[root@localhost ~]# journalctl -n 20
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Consumed 19.543s CPU time.
OKT 10 13:00:01 localhost.localdomain gnome-shell[2391]: libinput error: client bug: timer ev...
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopping System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion=>]
OKT 10 13:00:04 localhost.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopped System Logging Service.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: [origin software="rsyslogd" swVersion=>]
OKT 10 13:00:04 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: imjournal: journal files changed, reloading
OKT 10 13:00:39 localhost.localdomain root[46274]: Daemon Debug Message
OKT 10 13:01:01 localhost.localdomain CROND[46284]: (root) CMD (run-parts /etc/cron.hourly)
OKT 10 13:01:01 localhost.localdomain run-parts[46287]: (/etc/cron.hourly) starting @anacron
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Anacron started on 2025-10-10
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.daily' in 19 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.weekly' in 39 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.monthly' in 59 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Jobs will be executed sequentially
OKT 10 13:01:01 localhost.localdomain run-parts[46299]: (/etc/cron.hourly) finished @anacron
OKT 10 13:01:01 localhost.localdomain CROND[46283]: (root) CMDEND (run-parts /etc/cron.hourly)
[root@localhost ~]# journalctl -p err
OKT 10 12:36:43 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:Genuine
OKT 10 12:36:43 localhost systemd[1]: Invalid DNA field header.
OKT 10 12:36:44 localhost kernel: Warning: Unmaintained driver is detected: el1000
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported
OKT 10 12:36:51 localhost systemd[1]: Invalid DNA field header.
OKT 10 12:36:53 localhost systemd-udevd[732]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 >
OKT 10 12:36:53 localhost systemd-udevd[740]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 >
```

## Просмотр сообщений

Теперь просмотрим сообщения вчерашнего дня введя команду journalctl –since yesterday

```
[root@localhost ~]# journalctl --since yesterday
```

Рис. 23: 23

## Вывод сообщений с ошибкой

Затем выведем все сообщения с ошибкой приоритета которые были зафиксированы со вчерашнего дня

```
[root@localhost ~]# journalctl --since yesterday -p err
окт 10 12:36:43 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:Genuine>
окт 10 12:36:43 localhost systemd[1]: Invalid DMI field header.
окт 10 12:36:44 localhost kernel: Warning: Unmaintained driver is detected: el000
окт 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be runni>
окт 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is li>
окт 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a suppo>
окт 10 12:36:51 localhost systemd[1]: Invalid DMI field header.
окт 10 12:36:53 localhost systemd-udevd[732]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 >
окт 10 12:36:53 localhost systemd-udevd[740]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 >
окт 10 12:36:58 localhost alsactl[928]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: f >
окт 10 12:37:01 localhost.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
окт 10 12:39:28 localhost.localdomain gdm-password][2283]: gkr-pam: unable to locate daemon c >
окт 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by >
окт 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by >
окт 10 12:39:38 localhost.localdomain gdm-wayland-session[1318]: GLib: Source ID 2 was not fo >
окт 10 12:39:39 localhost.localdomain gdm-launch-environment][1266]: GLib-GObject: g_object_u >
[lines 1-16/16 (END)]
```

## Вывод информации

---

Затем выведем детальную информацию с помощью команды journalctl -o verbose

```
ОКТ 10 12:39:39 localhost.localdomain gdm-launcher[1144]: pam_unix(gdm-launcher:session): user not known to PAM  
[root@localhost ~]# journalctl -o verbose
```

Рис. 25: 25

## Просмотр дополнительной информации

Далее просмотрим дополнительную информацию о модуле sshd введя команду journalctl \_SYSTEMD\_UNIT=sshd.service

```
[root@localhost ~]# journalctl _SYSTEMD_UNIT=sshd.service
окт 10 12:37:02 localhost.localdomain sshd[1226]: Server listening on 0.0.0.0 port 22.
окт 10 12:37:02 localhost.localdomain sshd[1226]: Server listening on :: port 22.
[root@localhost ~]#
```

Рис. 26: 26

После чего откроем новый терминала и создадим новый каталог и скорректируем его права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию и для принятия изменений необходимо перезагрузить систему или использовать команду killall SR1 systemctl-journalctl

```
[root@localhost ~]# mkdir -p /var/log/journal  
[root@localhost ~]# chown root:systemd-journal /var/log/journal  
[root@localhost ~]# chmod 2755 /var/log/journal  
[root@localhost ~]# killall -USR1 systemd-journalctl  
[root@localhost ~]#
```

Рис. 27: 27

## Проверка журнала

Теперь журнал systemd теперь постоянный и можем проверить это командой journalctl -b

```
[KT 10 12:36:43 localhost kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iadi-prod-build001.bld.equinor.no)
[KT 10 12:36:43 localhost kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be vi...
[KT 10 12:36:43 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev...
[KT 10 12:36:43 localhost kernel: BIOS-provided physical RAM map:
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009ffff] usable
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000000ff0000-0x00000000000fffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffffff] usable
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000ffff00-0x00000000dffffff] ACPI data
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000fec0000-0x00000000fec00fff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000ffec0000-0x00000000feec00ff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000fffc0000-0x00000000ffffffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000021fffff] usable
[KT 10 12:36:43 localhost kernel: NX (Execute Disable) protection: active
[KT 10 12:36:43 localhost kernel: APIC: Static calls initialized
[KT 10 12:36:43 localhost kernel: SMBIOS 2.5 present.
[KT 10 12:36:43 localhost kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[KT 10 12:36:43 localhost kernel: Hypervisor detected: KVM
[KT 10 12:36:43 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
[KT 10 12:36:43 localhost kernel: kvm-clock: using sched offset of 622553352 cycles
[KT 10 12:36:43 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dfffb, max_idl...
[KT 10 12:36:43 localhost kernel: tsc: Detected 3686.398 MHz processor
[KT 10 12:36:43 localhost kernel: e820: update [mem 0x00000000-0x000000ff] usable ==> reserved
[KT 10 12:36:43 localhost kernel: e820: remove [mem 0x0000a000-0x000fffff] usable
[KT 10 12:36:43 localhost kernel: last_pfn = 0x220000 max_arch_pfn = 0x400000000
[KT 10 12:36:43 localhost kernel: HTRRs disabled by BIOS
[KT 10 12:36:43 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
[KT 10 12:36:43 localhost kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
[KT 10 12:36:43 localhost kernel: found SMP MP-table at [mem 0x0000ffff-0x0009ffff]
[KT 10 12:36:43 localhost kernel: RAMDISK: [mem 0x30c7b000-0x34635fff]
[KT 10 12:36:43 localhost kernel: ACPI: Early table checksum verification disabled
[KT 10 12:36:43 localhost kernel: ACPI: RSDP 0x000000000000E00000 000024 {v02 VBOX }
[KT 10 12:36:43 localhost kernel: ACPI: XSDT 0x00000000FFFF0030 00003C {v01 VBOX VBOXXSDT 00000001 ASL 00000061}
[KT 10 12:36:43 localhost kernel: ACPI: FACP 0x00000000FFFF00F0 0000F4 {v04 VBOX VBOXFACP 00000001 ASL 00000061}
[KT 10 12:36:43 localhost kernel: DSDT 0x00000000FFFF0040 002353 {v02 VBOX VBOXBIOS 00000002 INTL 20100528}
[KT 10 12:36:43 localhost kernel: FACS 0x00000000FFFF0020 000040
[KT 10 12:36:43 localhost kernel: FACS 0x00000000FFFF00200 000040
[KT 10 12:36:43 localhost kernel: ACPI: APIC 0x00000000FFFF0240 00008C {v02 VBOX VBOXAPIC 00000001 ASL 00000061}
[KT 10 12:36:43 localhost kernel: SSDT 0x00000000FFFF02D0 00003C {v01 VBOX VBOXCPU 00000002 INTL 20100528}
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACP table memory at [mem 0xdfff0f00-0xdfff101e3]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving DSDT table memory at [mem 0xdfff0640-0xdfff2992]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02cb]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving SSDT table memory at [mem 0xdfff02d0-0xdfff063b]
[KT 10 12:36:43 localhost kernel: No NUMA configuration found
[KT 10 12:36:43 localhost kernel: Faking a node at [mem 0x0000000000000000-0x0000000021fffff]
[KT 10 12:36:43 localhost kernel: NODE_DATA(0) allocated [mem 0x21ffd1000-0x21ffffbfff]
[KT 10 12:36:43 localhost kernel: sschbctrl_maxsize=0x0000000000000000 0x0000000000000000 (256 MB)
```

## Контрольный вопрос 1

---

1. Какой файл используется для настройки rsyslogd?

Ответ - файл /etc/rsyslog.conf

## Контрольный вопрос 2

---

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

Ответ - файл журнала айнтефекации /var/log/auth.log

## Контрольный вопрос 3

---

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

Ответ - период ротации журналов по умолчанию раз в неделю

## Контрольный вопрос 4

---

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

Ответ - строку /var/log/message.info

## Контрольный вопрос 5

---

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

Ответ - команда `tail -f /var/log/syslog`

## Контрольный вопрос 6

---

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

Ответ - команда journalctl \_PID=1 –since “9:00” –until “15:00”

## Контрольный вопрос 7

---

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

Ответ - команда journalctl -b

## Контрольный вопрос 8

---

8. Какая процедура позволяет сделать журнал journald постоянным?

Ответ - команда создать каталог и перезапустить службу  
`mkdir -p /var/log/journal`  
`systemctl restart systemd-journald`

## Вывод

---

В результате выполнения лабораторной работы я получил навыки работы с журналами мониторинга различных событий в системе