

# Лабораторная работа №7

Управление журналами событий в системе

---

Сидорова А.В.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Сидорова Арина Валерьевна
- студентка НПИбд-02-24
- ст.б. 1132242912
- Российский университет дружбы народов

## Вводная часть

---

Управление системными журналами (логами) является важнейшей задачей системного администратора для обеспечения мониторинга, диагностики проблем, аудита безопасности и анализа производительности операционной системы.

## Объект исследования

- Система журналирования событий в операционной системе Linux.

## Предмет исследования

- Механизмы и инструменты управления системными журналами (rsyslog, journald, journalctl).

**Цель:** Получить практические навыки работы с системой журналирования событий в Linux, включая настройку rsyslog и работу с journalctl.

**Задачи:**

1. Освоить мониторинг журналов событий в реальном времени.
2. Научиться настраивать правила фильтрации и перенаправления сообщений в rsyslog.
3. Получить навыки работы с утилитой journalctl для просмотра и фильтрации журналов systemd.
4. Настроить постоянное хранение журналов journald.

## Выполнение лабораторной работы

---





На второй вкладке терминала запустим мониторинг системных событий в реальном времени.

```
> [sudo] пароль для avsidorova:
root@avsidorova:~# tail -f /var/log/messages
Oct 11 17:08:41 avsidorova kernel: traps: VBoxClient[7864] trap int3 ip:41dc5b sp:7f3a0d577cd0 error:0 in VBoxClient[
1dc5b,400000+bb000]
Oct 11 17:08:41 avsidorova systemd-coredump[7865]: Process 7861 (VBoxClient) of user 1000 terminated abnormally with
signal 5/TRAP, processing...
Oct 11 17:08:41 avsidorova systemd[1]: Started systemd-coredump@46-7865-0.service - Process Core Dump (PID 7865/UID 0
).
Oct 11 17:08:41 avsidorova systemd-coredump[7866]: Process 7861 (VBoxClient) of user 1000 dumped core.#012#012Module
libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module
libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module
libxrandr-client.so.0 from rpm xrandr-1.22.0-2.el10.x86_64#012Stack trace of thread 7864:#012#00 000000000001d5f5
```

Рис. 1: мониторинг

В третьей вкладке терминала вернемся к учётной записи своего пользователя (достаточно нажать Ctrl + d )

попробуем получить полномочия администратора, но введем неправильный пароль.

Обратим внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username ...». Отображаемые на экране сообщения также фиксируются в файле `/var/log/messages`.

В третьей вкладке терминала из оболочки пользователя введем `logger hello`

```
[~# user] tite ...  
avsidorova@avsidorova:~$ su -  
Пароль:  
su: Сбой при проверке подлинности  
avsidorova@avsidorova:~$ logger hello  
avsidorova@avsidorova:~$
```

Рис. 2: `logger hello`

##Во второй вкладке терминала с мониторингом остановим трассировку файла сообщений мониторинга реального времени

используя `Ctrl + c`. Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов). Мы увидим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды `su`.



## В первой вкладке терминала установим Apache

```
[root@avsidorova:~]# sudo dnf -y install httpd
Последняя проверка окончания срока действия метаданных: 0:09:07 назад, Сб 11 окт 2025 17:02:14.
Зависимости разрешены.
=====
Пакет                Архитектура          Версия                Репозиторий           Размер
=====
Установка:
httpd                 x86_64                2.4.63-1.el10_0.2     appstream              52 k
Установка зависимостей:
apr                   x86_64                1.7.5-2.el10          appstream              128 k
apr-util              x86_64                1.6.3-21.el10         appstream              98 k
apr-util-ldb          x86_64                1.6.3-21.el10         appstream              14 k
httpd-core            x86_64                2.4.63-1.el10_0.2     appstream              1.5 M
httpd-filesystem      noarch                2.4.63-1.el10_0.2     appstream              13 k
httpd-tools           x86_64                2.4.63-1.el10_0.2     appstream              80 k
rocky-logos-httpd    noarch                100.4-7.el10          appstream              24 k
Установка слабых зависимостей:
apr-util-openssl      x86_64                1.6.3-21.el10         appstream              16 k
mod_http2             x86_64                2.0.29-2.el10_0.1     appstream              164 k
mod_lua               x86_64                2.4.63-1.el10_0.2     appstream              59 k

Результат транзакции
=====
Установка 11 Пакетов

Объем загрузки: 2.1 М
Объем изменений: 6.1 М
Загрузка пакетов:
(1/11): apr-util-ldb-1.6.3-21.el10.x86_64.rpm      203 kB/s | 14 kB    00:00
(2/11): apr-util-1.6.3-21.el10.x86_64.rpm         856 kB/s | 98 kB    00:00
(3/11): apr-util-openssl-1.6.3-21.el10.x86_64.rpm 309 kB/s | 16 kB    00:00
(4/11): apr-1.7.5-2.el10.x86_64.rpm               932 kB/s | 128 kB   00:00
(5/11): httpd-2.4.63-1.el10_0.2.x86_64.rpm        1.4 MB/s | 52 kB    00:00
```

Рис. 4: Apache

## После окончания процесса установки запустим веб-службу

```
Выполнено!  
root@avsidorova:~# systemctl start httpd  
root@avsidorova:~# systemctl enable httpd  
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.  
root@avsidorova:~#
```

Рис. 5: system start, enable

## Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы

```
clly~/dev/pt3/2 user-avstodorova host- user-1001
root@avstodorova:~# tail -f /var/log/httpd/error_log
[Sat Oct 11 17:13:42.740086 2025] [suexec:notice] [pid 8702:tid 8702] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fea0:fae8%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 11 17:14:12.816058 2025] [lbmethod_heartbeat:notice] [pid 8702:tid 8702] AH02282: No slotmem from mod_heartmonitor
[Sat Oct 11 17:14:12.818199 2025] [systemd:notice] [pid 8702:tid 8702] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 11 17:14:12.833395 2025] [mpm_event:notice] [pid 8702:tid 8702] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 11 17:14:12.833498 2025] [core:notice] [pid 8702:tid 8702] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 6: error\_log



В третьей вкладке терминала получим полномочия администратора и в файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавим строку

```
# # Enablement of the functionality for the various modules
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

ErrorLog syslog:local1
```

Рис. 7: 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` создадим файл мониторинга событий веб-службы:

```
[sudo] пароль для avsidorova:  
root@avsidorova:~# nano /etc/httpd/conf/httpd.conf  
root@avsidorova:~# cd /etc/rsyslog.d  
root@avsidorova:/etc/rsyslog.d# touch httpd.conf  
root@avsidorova:/etc/rsyslog.d#
```

Рис. 8: touch httpd.conf

## Открыв его на редактирование, пропишем в нём

A screenshot of the GNU nano 8.1 text editor. The title bar at the top shows 'GNU nano 8.1', 'httpd.conf', and 'ИЗМЕНЕН'. The main editing area contains the text 'local1.\* -/var/log/httpd-error.log'. A cursor is positioned at the end of this line. The editor has a simple interface with a grey vertical scrollbar on the left and a red status bar at the bottom.

```
GNU nano 8.1 httpd.conf ИЗМЕНЕН
> local1.* -/var/log/httpd-error.log
```

Рис. 9: local1.\* -/var/log/httpd-error.log

Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log.

Перейдем в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу:

```
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/li
root@avsidorova:~# systemctl restart rsyslog.service
root@avsidorova:~# systemctl restart httpd
```

Рис. 10: restart

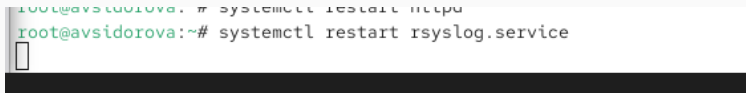
Все сообщения об ошибках веб-службы теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени, используя команду tail с соответствующими параметрами, или непосредственно просматривая указанный файл.

В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации:

```
root@avsidorova:/etc/rsyslog.d# nano rsyslog.conf
root@avsidorova:/etc/rsyslog.d# cd /etc/rsyslog.d
root@avsidorova:/etc/rsyslog.d# touch debug.conf
root@avsidorova:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@avsidorova:/etc/rsyslog.d#
```

Рис. 11: touch debug.conf

В первой вкладке терминала снова перезапустим rsyslogd:

A terminal window with a dark background. The prompt is root@avsidorova:~#. The command systemctl restart rsyslog.service is entered. A cursor is visible at the end of the command line.

```
root@avsidorova:~# systemctl restart rsyslog.service
```

Рис. 12: restart

Во второй вкладке терминала запустим мониторинг отладочной информации:

```
root@avsidorova:~# tail -f /var/log/messages-debug
Oct 11 17:24:00 avsidorova kernel: traps: VBoxClient[10701] trap int3 ip:41dc5b sp:7f3a0d577cd0 error:0 in VBoxClient
[1dc5b.400000+bb000]
```

Рис. 13: tail -f /var/log/messages-debug

В третьей вкладке терминала введем:

```
root@avsidorova:/etc/rsyslog.d# cat /etc/rsyslog.d/daemon.debug /etc/rsyslog.d/daemon.debug
root@avsidorova:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"
root@avsidorova:/etc/rsyslog.d#
```

Рис. 14: logger -p



В терминале с мониторингом посмотрим сообщение отладки.



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

journalctl

```
OKT 11 17:03:30 avsidorova kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.
OKT 11 17:03:30 avsidorova kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev
OKT 11 17:03:30 avsidorova kernel: BIOS-provided physical RAM map:
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000000dfff0000-0x00000000000dfffffff] ACPI data
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
OKT 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011ffffffff] usable
OKT 11 17:03:30 avsidorova kernel: NX (Execute Disable) protection: active
OKT 11 17:03:30 avsidorova kernel: APIC: Static calls initialized
OKT 11 17:03:30 avsidorova kernel: SMBIOS 2.5 present.
OKT 11 17:03:30 avsidorova kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
OKT 11 17:03:30 avsidorova kernel: DMI: Memory slots populated: 0/0
OKT 11 17:03:30 avsidorova kernel: Hypervisor detected: KVM
OKT 11 17:03:30 avsidorova kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
OKT 11 17:03:30 avsidorova kernel: kvm-clock: using sched offset of 7362847289 cycles
OKT 11 17:03:30 avsidorova kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_
OKT 11 17:03:30 avsidorova kernel: tsc: Detected 2496.010 MHz processor
OKT 11 17:03:30 avsidorova kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
OKT 11 17:03:30 avsidorova kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
OKT 11 17:03:30 avsidorova kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
OKT 11 17:03:30 avsidorova kernel: MTRR map: 3 entries (3 fixed + 0 variable; max 19), built from 8 variable MTRRs
OKT 11 17:03:30 avsidorova kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
OKT 11 17:03:30 avsidorova kernel: CPU MTRRs all blank - virtualized system.
OKT 11 17:03:30 avsidorova kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
OKT 11 17:03:30 avsidorova kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
OKT 11 17:03:30 avsidorova kernel: Incomplete global flushes, disabling PCID
OKT 11 17:03:30 avsidorova kernel: RAMDISK: [mem 0x342cd000-0x34615eff]
OKT 11 17:03:30 avsidorova kernel: ACPI: Fixed table checksum verification disabled
```

# Просмотр содержимого журнала без использования пейджера:

journalctl -no-pager

```
окт 11 17:26:43 avsidorova systemd-coredump[11064]: [?] Process 11059 (VBoxClient) of user 1000 dumped core.

>>
86_64
Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x

Stack trace of thread 11062:
#0 0x00000000041dc5b n/a (n/a + 0x0)
#1 0x00000000041dbd4 n/a (n/a + 0x0)
#2 0x000000000450b9c n/a (n/a + 0x0)
#3 0x0000000004359a0 n/a (n/a + 0x0)
#4 0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 11060:
#0 0x00007f3a1bc8f4bd syscall (libc.so.6 + 0x1034bd)
#1 0x000000000435000 n/a (n/a + 0x0)
#2 0x00000000045137b n/a (n/a + 0x0)
#3 0x000000000435a3a n/a (n/a + 0x0)
#4 0x000000000450b9c n/a (n/a + 0x0)
#5 0x0000000004359a0 n/a (n/a + 0x0)
#6 0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
#7 0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 11059:
#0 0x00007f3a1bc8f4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000004348b2 n/a (n/a + 0x0)
#2 0x0000000004507e6 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007f3a1bbb630e __libc_start_call_main (libc.so.6 + 0x2

a30e)
#5 0x00007f3a1bbb63c9 __libc_start_main@@GLIBC_2.34 (libc.so.

6 + 0x2a3c9)
#6 0x0000000004044a n/a (n/a + 0x0)
```

journalctl -f Используем Ctrl + c для прерывания просмотра.

```
                                ELF object binary architectur
окт 11 17:27:41 avsidorova systemd[1]: systemd-coredump@262-11200-0.service: Deactiv
^Z
[1]+  Остановлен    journalctl -f
root@avsidorova:~# journalctl -f
```

A terminal window with a black background. The text is white. At the top right, there is a red error message: "ELF object binary architectur". Below it, a log entry: "окт 11 17:27:41 avsidorova systemd[1]: systemd-coredump@262-11200-0.service: Deactiv". Then a carriage return and a Z (^Z). Then a prompt "[1]+ Остановлен" followed by "journalctl -f". Then a new prompt "root@avsidorova:~#" followed by "journalctl -f". At the bottom of the terminal window, there is a taskbar with four icons: a blue square with a white swirl, a grey circle, a blue square with a white play button, and a blue square with a white document icon.

Рис. 17: journalctl -f

# Для использования фильтрации просмотра конкретных параметров журнала введем

journalctl и дважды нажмите клавишу Tab .

Посмотрим события для UID0: journalctl \_UID=0

```
о́кт 11 17:03:31 avsidorova systemd[1]: systemd-ask-password-console.path - Dispatch Password Requests to Console Directory Watch
о́кт 11 17:03:31 avsidorova systemd[1]: Started systemd-ask-password-plymouth.path - Forward Password Requests to Plymouth
о́кт 11 17:03:31 avsidorova systemd[1]: Reached target paths.target - Path Units.
о́кт 11 17:03:31 avsidorova systemd[1]: Mounting sys-kernel-config.mount - Kernel Configuration File System...
о́кт 11 17:03:31 avsidorova systemd[1]: Mounted sys-kernel-config.mount - Kernel Configuration File System.
о́кт 11 17:03:31 avsidorova systemd[1]: systemd-vconsole-setup.service: Deactivated successfully.
о́кт 11 17:03:31 avsidorova systemd[1]: Stopped systemd-vconsole-setup.service - Virtual Console Setup.
о́кт 11 17:03:31 avsidorova systemd[1]: Stopping systemd-vconsole-setup.service - Virtual Console Setup...
о́кт 11 17:03:31 avsidorova systemd[1]: Starting systemd-vconsole-setup.service - Virtual Console Setup...
о́кт 11 17:03:31 avsidorova systemd-vconsole-setup[444]: setfont: ERROR kdfontop.c:183 put_font_kdfontop: Unable to load font
о́кт 11 17:03:31 avsidorova systemd-vconsole-setup[441]: /usr/bin/setfont failed with a "system error" (EX_OSERR), ignoring
о́кт 11 17:03:31 avsidorova systemd[1]: systemd-vconsole-setup.service: Deactivated successfully.
о́кт 11 17:03:31 avsidorova systemd[1]: Stopped systemd-vconsole-setup.service - Virtual Console Setup.
о́кт 11 17:03:31 avsidorova systemd[1]: Starting systemd-vconsole-setup.service - Virtual Console Setup...
о́кт 11 17:03:31 avsidorova systemd[1]: systemd-vconsole-setup.service: Deactivated successfully.
о́кт 11 17:03:31 avsidorova systemd[1]: Stopped systemd-vconsole-setup.service - Virtual Console Setup.
о́кт 11 17:03:31 avsidorova systemd[1]: Starting systemd-vconsole-setup.service - Virtual Console Setup...
о́кт 11 17:03:31 avsidorova systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
о́кт 11 17:03:32 avsidorova dracut-initqueue[504]: Scanning devices sda3 for LVM logical volumes rl/root rl/swap
о́кт 11 17:03:32 avsidorova dracut-initqueue[504]:   rl/root linear
о́кт 11 17:03:32 avsidorova dracut-initqueue[504]:   rl/swap linear
о́кт 11 17:03:32 avsidorova systemd[1]: Found device dev-mapper-rl\x2droot.device - /dev/mapper/rl-root.
о́кт 11 17:03:32 avsidorova systemd[1]: Reached target initrd-root-device.target - Initrd Root Device.
о́кт 11 17:03:32 avsidorova systemd[1]: Found device dev-disk-by\x2duuid-8fd659be\x2d727b\x2d4081\x2db4d7\x2d7ee53b8e\x2d5a.device - /dev/disk/by-uuid/8fd659be727b4081b4d77ee53b8e5a
о́кт 11 17:03:32 avsidorova systemd[1]: Starting systemd-hibernate-resume.service - Resume from hibernation...
о́кт 11 17:03:32 avsidorova systemd[1]: systemd-hibernate-resume.service: Deactivated successfully.
о́кт 11 17:03:32 avsidorova systemd[1]: Finished systemd-hibernate-resume.service - Resume from hibernation.
о́кт 11 17:03:32 avsidorova systemd[1]: Reached target local-fs-pre.target - Preparation for Local File Systems.
о́кт 11 17:03:32 avsidorova systemd[1]: Reached target local-fs.target - Local File Systems.
о́кт 11 17:03:32 avsidorova systemd[1]: Starting systemd-tmpfiles-setup.service - Create System Files and Directories
о́кт 11 17:03:32 avsidorova systemd[1]: Finished dracut-initqueue.service - dracut initqueue hook.
```

## Для отображения последних 20 строк журнала введем

journalctl -n 20

```
ОКТ 11 17:29:10 avsidorova kernel: traps: VBoxClient[11394] trap int3 ip:41dc5b sp:7f3a0d577cd0 error:0 in VBoxClient[11394]
ОКТ 11 17:29:10 avsidorova systemd-coredump[11395]: Process 11391 (VBoxClient) of user 1000 terminated abnormally with core dump (PID 11395/UB
ОКТ 11 17:29:10 avsidorova systemd[1]: Started systemd-coredump@279-11395-0.service - Process Core Dump (PID 11395/UB
ОКТ 11 17:29:10 avsidorova systemd-coredump[11396]: [ ] Process 11391 (VBoxClient) of user 1000 dumped core.

                                Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
                                Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64
                                Stack trace of thread 11394:
                                #0 0x0000000041dc5b n/a (n/a + 0x0)
                                #1 0x00000000041dbd4 n/a (n/a + 0x0)
                                #2 0x000000000450b9c n/a (n/a + 0x0)
                                #3 0x0000000004359a0 n/a (n/a + 0x0)
                                #4 0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
                                #5 0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

                                Stack trace of thread 11391:
                                #0 0x00007f3a1bc8f4bd syscall (libc.so.6 + 0x1034bd)
                                #1 0x0000000004348b2 n/a (n/a + 0x0)
                                #2 0x0000000004507e6 n/a (n/a + 0x0)
                                #3 0x000000000405123 n/a (n/a + 0x0)
                                #4 0x00007f3a1bbb630e __libc_start_call_main (libc.so.6 + 0x1034bd)
                                #5 0x00007f3a1bbb63c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x1034bd)
                                #6 0x0000000004044aa n/a (n/a + 0x0)
                                ELF object binary architecture: AMD x86-64

ОКТ 11 17:29:10 avsidorova systemd[1]: systemd-coredump@279-11395-0.service: Deactivated successfully.
ОКТ 11 17:29:15 avsidorova kernel: traps: VBoxClient[11404] trap int3 ip:41dc5b sp:7f3a0d577cd0 error:0 in VBoxClient[11404]
ОКТ 11 17:29:15 avsidorova systemd-coredump[11405]: Process 11401 (VBoxClient) of user 1000 terminated abnormally with core dump (PID 11405/UB
ОКТ 11 17:29:15 avsidorova systemd[1]: Started systemd-coredump@280-11405-0.service - Process Core Dump (PID 11405/UB
ОКТ 11 17:29:15 avsidorova systemd-coredump[11406]: [ ] Process 11401 (VBoxClient) of user 1000 dumped core.

                                Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
                                Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64
                                Stack trace of thread 11404:
```

# Для просмотра только сообщений об ошибках введем

journalctl -p err

```
root@avsidorova:~# sudo -i x root@avsidorova:~# sudo -i root@avsidorova:/etc/rsyslog.d# sudo -i

OCT 11 17:03:30 avsidorova systemd-udevd[386]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignoring.
OCT 11 17:03:30 avsidorova systemd-udevd[386]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignoring.
OCT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported h
OCT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
OCT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to
OCT 11 17:03:39 avsidorova kernel: Warning: Unmaintained driver is detected: e1000
OCT 11 17:03:41 avsidorova alsactl[889]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 u
OCT 11 17:04:17 avsidorova gdm-password[3431]: gkr-pam: unable to locate daemon control file
OCT 11 17:04:22 avsidorova systemd[5453]: Failed to start app-gnome-xdg\x2duser\x2ddirs-5580.scope - Application laun
OCT 11 17:04:38 avsidorova systemd-coredump[6316]: [.] Process 6296 (VBoxClient) of user 1000 dumped core.

                                Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
                                Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x
Stack trace of thread 6306:
#0 0x000000000041dc5b n/a (n/a + 0x0)
#1 0x000000000041dbd4 n/a (n/a + 0x0)
#2 0x0000000000450b9c n/a (n/a + 0x0)
#3 0x00000000004359a0 n/a (n/a + 0x0)
#4 0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 6298:
#0 0x00007f3a1bc8f4bd syscall (libc.so.6 + 0x1034bd)
#1 0x00000000004348b2 n/a (n/a + 0x0)
#2 0x00000000004507e6 n/a (n/a + 0x0)
#3 0x0000000000416559 n/a (n/a + 0x0)
#4 0x00000000004182da n/a (n/a + 0x0)
#5 0x0000000000417d6a n/a (n/a + 0x0)
#6 0x0000000000404860 n/a (n/a + 0x0)
#7 0x0000000000450b9c n/a (n/a + 0x0)
#8 0x00000000004359a0 n/a (n/a + 0x0)
```



# Для просмотра всех сообщений со вчерашнего дня введем

journalctl -since yesterday

```
root@avsidorova:~ - sudo -i  X root@avsidorova:~ - sudo -i root@avsidorova:/etc/rsyslog.d - sudo -i
ОКТ 11 17:03:30 avsidorova kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.)
ОКТ 11 17:03:30 avsidorova kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev
ОКТ 11 17:03:30 avsidorova kernel: BIOS-provided physical RAM map:
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000fffff] reserved
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000000dfff0000-0x00000000000dffffff] ACPI data
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
ОКТ 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000100000000-0x0000000011ffffff] usable
ОКТ 11 17:03:30 avsidorova kernel: NX (Execute Disable) protection: active
ОКТ 11 17:03:30 avsidorova kernel: APIC: Static calls initialized
ОКТ 11 17:03:30 avsidorova kernel: SMBIOS 2.5 present.
ОКТ 11 17:03:30 avsidorova kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
ОКТ 11 17:03:30 avsidorova kernel: DMI: Memory slots populated: 0/0
ОКТ 11 17:03:30 avsidorova kernel: Hypervisor detected: KVM
ОКТ 11 17:03:30 avsidorova kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
ОКТ 11 17:03:30 avsidorova kernel: kvm-clock: using sched offset of 7362847289 cycles
ОКТ 11 17:03:30 avsidorova kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_
ОКТ 11 17:03:30 avsidorova kernel: tsc: Detected 2496.010 MHz processor
ОКТ 11 17:03:30 avsidorova kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> reserved
ОКТ 11 17:03:30 avsidorova kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
ОКТ 11 17:03:30 avsidorova kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
ОКТ 11 17:03:30 avsidorova kernel: MTRR map: 3 entries (3 fixed + 0 variable; max 19), built from 8 variable MTRRs
ОКТ 11 17:03:30 avsidorova kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
ОКТ 11 17:03:30 avsidorova kernel: CPU MTRRs all blank - virtualized system.
ОКТ 11 17:03:30 avsidorova kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
ОКТ 11 17:03:30 avsidorova kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
ОКТ 11 17:03:30 avsidorova kernel: Incomplete global flushes, disabling PCID
ОКТ 11 17:03:30 avsidorova kernel: RAMDISK: [mem 0x342cd000-0x3615efff]
ОКТ 11 17:03:30 avsidorova kernel: ACPI: Early table checksum verification disabled
ОКТ 11 17:03:30 avsidorova kernel: ACPI: RSDP 0x000000000000E0000 000024 (v02 VBOX )
ОКТ 11 17:03:30 avsidorova kernel: ACPI: XSDT 0x000000000000FF030 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
ОКТ 11 17:03:30 avsidorova kernel: ACPI: FACP 0x000000000000FF0F0 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
```

journalctl -since yesterday -p err

```
root@avsidorova:~ -- sudo -i x root@avsidorova:~ -- sudo -i root@avsidorova:/etc/rsyslog.d -- sudo -i

OKT 11 17:03:30 avsidorova systemd-udevd[386]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignoring.
OKT 11 17:03:30 avsidorova systemd-udevd[386]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignoring.
OKT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported h
OKT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
OKT 11 17:03:31 avsidorova kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device t
OKT 11 17:03:39 avsidorova kernel: Warning: Unmaintained driver is detected: e1000
OKT 11 17:03:41 avsidorova alsactl[889]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 u
OKT 11 17:04:17 avsidorova gdm-password[3431]: gkr-pam: unable to locate daemon control file
OKT 11 17:04:22 avsidorova systemd[5453]: Failed to start app-gnome-xdg/x2duser/x2ddirs-5580.scope - Application laun
OKT 11 17:04:38 avsidorova systemd-coredump[6316]: [^] Process 6296 (VBoxClient) of user 1000 dumped core.

                                Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
                                Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
                                Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
                                Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
                                Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x
Stack trace of thread 6306:
#0  0x000000000041dc5b n/a (n/a + 0x0)
#1  0x000000000041dbd4 n/a (n/a + 0x0)
#2  0x0000000000450b9c n/a (n/a + 0x0)
#3  0x00000000004359a0 n/a (n/a + 0x0)
#4  0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
#5  0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 6298:
#0  0x00007f3a1bc8f4bd syscall (libc.so.6 + 0x1034bd)
#1  0x00000000004348b2 n/a (n/a + 0x0)
#2  0x00000000004507e6 n/a (n/a + 0x0)
#3  0x0000000000416559 n/a (n/a + 0x0)
#4  0x00000000004182da n/a (n/a + 0x0)
#5  0x0000000000417d6a n/a (n/a + 0x0)
#6  0x0000000000404860 n/a (n/a + 0x0)
#7  0x0000000000450b9c n/a (n/a + 0x0)
#8  0x00000000004359a0 n/a (n/a + 0x0)
#9  0x00007f3a1bc20b68 start_thread (libc.so.6 + 0x94b68)
#10 0x00007f3a1bc916bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 6297:
```

# Для детальной информации используем

journalctl -o verbose

```
root@avsidorova:~ -- sudo -i x root@avsidorova:~ -- sudo -i root@avsidorova:/etc/rsyslog.d -- sudo -i

Sat 2025-10-11 17:03:30.138653 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=1;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
  _SOURCE_BOOTTIME_TIMESTAMP=0
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (G
  _BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
  _MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
  _HOSTNAME=avsidorova
  _RUNTIME_SCOPE=initrd
Sat 2025-10-11 17:03:30.138685 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=2;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
  _SOURCE_BOOTTIME_TIMESTAMP=0
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
  _MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
  _HOSTNAME=avsidorova
  _RUNTIME_SCOPE=initrd
  PRIORITY=6
  MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/mapper/rl-root ro res
Sat 2025-10-11 17:03:30.138704 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=3;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
  _SOURCE_BOOTTIME_TIMESTAMP=0
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
  _MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
  _HOSTNAME=avsidorova
  _RUNTIME_SCOPE=initrd
  PRIORITY=6
  MESSAGE=BIOS-provided physical RAM map:
```

# Для просмотра дополнительной информации о модуле sshd введем

journalctl \_SYSTEMD\_UNIT=sshd.service

```
root@avsidorova:~ - sudo -i x root@avsidorova:~ - sudo -i root@avsidorova:/etc/rsyslog.d - sudo -i

SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (G
_BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
_MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
_HOSTNAME=avsidorova
_RUNTIME_SCOPE=initrd
Sat 2025-10-11 17:03:30.138685 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=2;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
_MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
_HOSTNAME=avsidorova
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/mapper/rl-root ro res
Sat 2025-10-11 17:03:30.138704 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=3;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=ce1c48ae5a6c43e1a0eef05931f81551
_MACHINE_ID=4a8a2b25645d419c8162f90f3884eb68
_HOSTNAME=avsidorova
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=BIOS-provided physical RAM map:
Sat 2025-10-11 17:03:30.138709 MSK [s=76a53f364631459d8a3b2b24e1166ea7;i=4;b=ce1c48ae5a6c43e1a0eef05931f81551;m=1f71b
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
```

## Постоянный журнал journald

Запустим терминал и получим полномочия администратора. Создадим каталог для хранения записей журнала. Скорректируем права доступа для каталога `/var/log/journal`, чтобы `journald` смог записывать в него информацию. Для принятия изменений необходимо или перезагрузить систему. Журнал `systemd` теперь постоянный. Мы хотим видеть сообщения журнала с момента последней перезагрузки, используем `journalctl -b`.

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# mkdir -p /var/log/journal
root@avsidorova:~# chown root:systemd-journal /var/log/journal
root@avsidorova:~# chmod 775 /var/log/journal
root@avsidorova:~# killall -USR1 systemd-journald
root@avsidorova:~# journalctl -b
окт 11 17:03:30 avsidorova kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.)
окт 11 17:03:30 avsidorova kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev
окт 11 17:03:30 avsidorova kernel: BIOS-provided physical RAM map:
окт 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
окт 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
окт 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
окт 11 17:03:30 avsidorova kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000000fffff] usable
```

Рис. 25: Постоянный журнал journald

## Результаты

---

- Освоены команды `tail -f`, `logger` для мониторинга и генерации логов.
- Настроен перенос логов веб-сервиса Apache в отдельный файл через `rsyslog`.
- Созданы пользовательские правила фильтрации для `rsyslog`.
- Освоена работа с `journalctl` для просмотра, фильтрации и анализа журналов.
- Настроено постоянное хранение журналов `systemd-journald`.

...