

# Лабораторная работа № 7

Управление журналами событий в системе

---

Сергеев Д. О.

18 октября 2025

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Сергеев Даниил Олегович
- Студент
- Направление: Прикладная информатика
- Российский университет дружбы народов
- 1132246837@pfur.ru

## Цель работы

---

Получить навыки работы с журналами мониторинга различных событий в системе.

## Задание

---

- Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени.
- Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
- Продемонстрируйте навыки работы с `journalctl`.
- Продемонстрируйте навыки работы с `journalld`.

## Ход выполнения лабораторной работы

---



## Мониторинг журнала системных событий в реальном времени

---

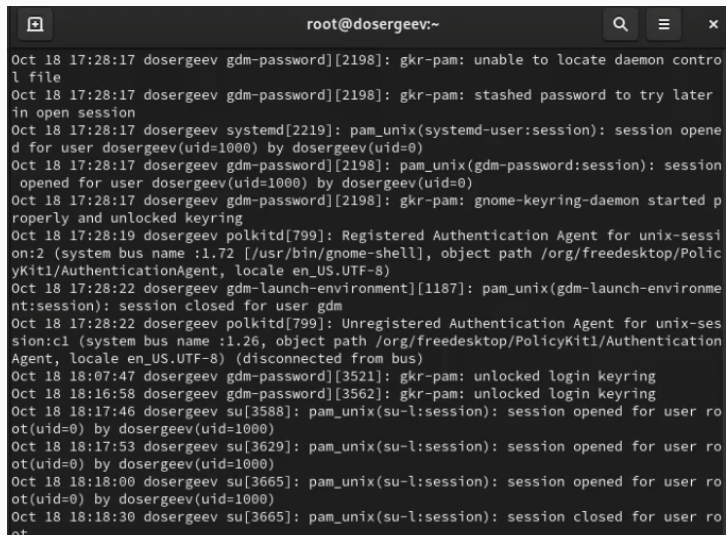
## Мониторинг журнала системных событий в реальном времени

- `tail -f /var/log/messages`
- `logger hello`

```
root@dosergeev:~  
[dosergeev@dosergeev ~]$ su -  
Password:  
[root@dosergeev ~]# tail -f /var/log/messages  
Oct 18 18:16:58 dosergeev NetworkManager[1127]: <info> [1760800618.4810] agent-manage  
r: agent[14aacb6e246c97f5,:1.72/org.gnome.Shell.NetworkAgent/1000]: agent registered  
Oct 18 18:17:27 dosergeev systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 18:17:43 dosergeev systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 18 18:17:44 dosergeev systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 18 18:17:46 dosergeev su[3588]: (to root) dosergeev on pts/0  
Oct 18 18:17:46 dosergeev systemd[1]: Starting Hostname Service...  
Oct 18 18:17:46 dosergeev systemd[1]: Started Hostname Service.  
Oct 18 18:17:53 dosergeev su[3629]: (to root) dosergeev on pts/2  
Oct 18 18:18:00 dosergeev su[3665]: (to root) dosergeev on pts/1  
Oct 18 18:18:14 dosergeev systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 18:18:30 dosergeev systemd[1]: systemd-hostnamed.service: Deactivated successf  
lly.  
Oct 18 18:18:40 dosergeev systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 18 18:18:40 dosergeev systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 18 18:18:45 dosergeev su[3716]: FAILED SU (to root) dosergeev on pts/1  
Oct 18 18:19:11 dosergeev systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 18:19:19 dosergeev dosergeev[3730]: hello  
  
dosergeev@dosergeev:~  
[dosergeev@dosergeev ~]$ su -  
Password:  
[root@dosergeev ~]#  
logout  
[dosergeev@dosergeev ~]$ su -  
Password:  
su: Authentication failure  
[dosergeev@dosergeev ~]$ logger hello  
[dosergeev@dosergeev ~]$
```

# Мониторинг журнала системных событий в реальном времени

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

A terminal window titled 'root@dosergeev:~' with search, menu, and close icons in the title bar. It displays the output of the 'tail -n 20 /var/log/secure' command, showing a series of system events from October 18th. The logs include messages from gdm-password, systemd, polkitd, and su, detailing session openings, closings, and keyring operations for various users like dosergeev and root.

```
Oct 18 17:28:17 dosergeev gdm-password[2198]: gkr-pam: unable to locate daemon contro
l file
Oct 18 17:28:17 dosergeev gdm-password[2198]: gkr-pam: stashed password to try later
in open session
Oct 18 17:28:17 dosergeev systemd[2219]: pam_unix(systemd-user:session): session opene
d for user dosergeev(uid=1000) by dosergeev(uid=0)
Oct 18 17:28:17 dosergeev gdm-password[2198]: pam_unix(gdm-password:session): session
opened for user dosergeev(uid=1000) by dosergeev(uid=0)
Oct 18 17:28:17 dosergeev gdm-password[2198]: gkr-pam: gnome-keyring-daemon started p
roperly and unlocked keyring
Oct 18 17:28:19 dosergeev polkitd[799]: Registered Authentication Agent for unix-sessi
on:2 (system bus name :1.72 [/usr/bin/gnome-shell], object path /org/freedesktop/Polic
yKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 18 17:28:22 dosergeev gdm-launch-environment[1187]: pam_unix(gdm-launch-environe
nt:session): session closed for user gdm
Oct 18 17:28:22 dosergeev polkitd[799]: Unregistered Authentication Agent for unix-ses
sion:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/Authentication
Agent, locale en_US.UTF-8) (disconnected from bus)
Oct 18 18:07:47 dosergeev gdm-password[3521]: gkr-pam: unlocked login keyring
Oct 18 18:16:58 dosergeev gdm-password[3562]: gkr-pam: unlocked login keyring
Oct 18 18:17:46 dosergeev su[3588]: pam_unix(su-l:session): session opened for user ro
ot(uid=0) by dosergeev(uid=1000)
Oct 18 18:17:53 dosergeev su[3629]: pam_unix(su-l:session): session opened for user ro
ot(uid=0) by dosergeev(uid=1000)
Oct 18 18:18:00 dosergeev su[3665]: pam_unix(su-l:session): session opened for user ro
ot(uid=0) by dosergeev(uid=1000)
Oct 18 18:18:30 dosergeev su[3665]: pam_unix(su-l:session): session closed for user ro
ot
```

## Изменение правил rsyslog.conf

---

В первой вкладке терминала установим Apache (пакет httpd). После окончания процесса установки запустим службу командами `systemctl start httpd` и `systemctl enable httpd`

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

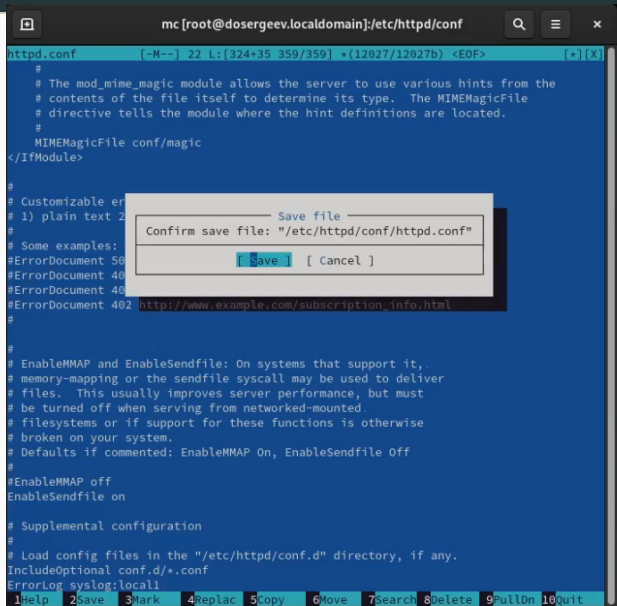
Рис. 3: Запуск службы httpd

```
[root@dosergeev ~]# tail -f /var/log/httpd/error_log
[Sat Oct 18 18:24:15.968333 2025] [core:notice] [pid 13685:tid 13685] SELinux policy e
nabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 18:24:15.972969 2025] [suexec:notice] [pid 13685:tid 13685] AH01232: suEXE
C mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 18 18:24:16.025883 2025] [lbmethod_heartbeat:notice] [pid 13685:tid 13685] AH
02282: No slotmem from mod_heartbeat
[Sat Oct 18 18:24:16.037896 2025] [mpm_event:notice] [pid 13685:tid 13685] AH00489: Ap
ache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 18:24:16.037940 2025] [core:notice] [pid 13685:tid 13685] AH00094: Command
line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4: Журнал ошибок httpd

# Изменение правил rsyslog.conf

- ErrorLog syslog:local1.



The screenshot shows a terminal window with the title bar "mc [root@dosergeev.localdomain]:/etc/httpd/conf". The terminal displays the contents of the `httpd.conf` file, which includes comments about the `mod_mime_magic` module and the `MIMEMagicFile` directive. A modal dialog box titled "Save file" is overlaid on the terminal, asking to confirm saving the file `"/etc/httpd/conf/httpd.conf"`. The dialog has two buttons: "Save" and "Cancel". At the bottom of the terminal window, there is a status bar with navigation shortcuts: 1Help, 2Save, 3Mark, 4Replac, 5Copy, 6Move, 7Search, 8Delete, 9PullDn, 10Quit.

```
httpd.conf [-M--] 22 L:[324+35 359/359] *(12027/12027b) <E0F> [*][X]
#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
MIMEMagicFile conf/magic
</IfModule>
#
# Customizable error documents:
# 1) plain text 2) HTML
#
# Some examples:
#ErrorDocument 500 "The server has a problem."
#ErrorDocument 403 "The requested URL is not allowed."
#ErrorDocument 402 "http://www.example.com/subscription_info.html"
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# 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
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Теперь перейдем в каталог `/etc/rsyslog.d` и создадим файл мониторинга событий веб-службы.

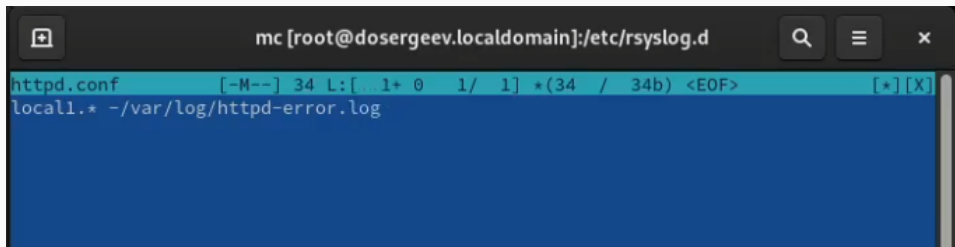
```
[root@dosergeev conf]#  
[root@dosergeev conf]# cd /etc/rsyslog.d  
[root@dosergeev rsyslog.d]# touch httpd.conf  
[root@dosergeev rsyslog.d]#
```

Рис. 6: Создание `httpd.conf` в `/etc/rsyslog.d`



## Изменение правил rsyslog.conf

Пропишем в нем строку, которая позволит нам отправлять все сообщения, получаемые для local1, в файл /var/log/httpd-error.log



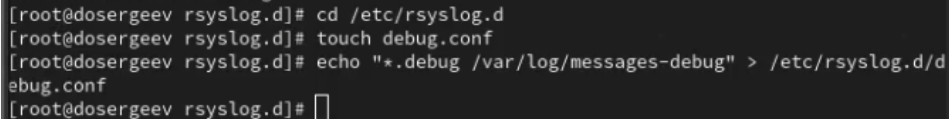
The screenshot shows a terminal window with the title bar "mc [root@dosergeev.localdomain]:/etc/rsyslog.d". The terminal content shows the file "httpd.conf" being edited. The first line of the file is highlighted in blue and contains the text: "local1.\* -/var/log/httpd-error.log". The second line of the file is highlighted in light blue and contains the text: "[\*] [X]".

Рис. 7: Модификация файла мониторинга httpd.conf

Перейдем обратно в первый терминал и перезагрузим rsyslogd и httpd:

- systemctl restart rsyslog.service
- systemctl restart httpd

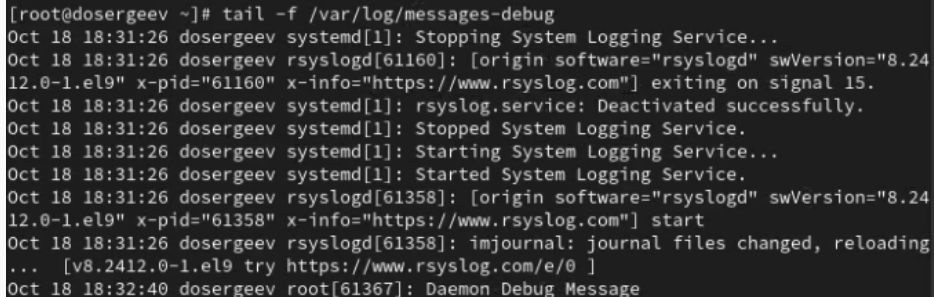
В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации.



```
[root@dosergeev rsyslog.d]# cd /etc/rsyslog.d
[root@dosergeev rsyslog.d]# touch debug.conf
[root@dosergeev rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/d
ebug.conf
[root@dosergeev rsyslog.d]#
```

Рис. 8: Файл мониторинга отладочной информации

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

A terminal window with a dark background and light gray text. The prompt is [root@dosergeev ~]#. The command tail -f /var/log/messages-debug is entered. The output shows the rsyslog service being stopped and started, with version and PID information. Finally, a debug message "Daemon Debug Message" is received from root.

```
[root@dosergeev ~]# tail -f /var/log/messages-debug
Oct 18 18:31:26 dosergeev systemd[1]: Stopping System Logging Service...
Oct 18 18:31:26 dosergeev rsyslogd[61160]: [origin software="rsyslogd" swVersion="8.24
12.0-1.el9" x-pid="61160" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 18:31:26 dosergeev systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 18:31:26 dosergeev systemd[1]: Stopped System Logging Service.
Oct 18 18:31:26 dosergeev systemd[1]: Starting System Logging Service...
Oct 18 18:31:26 dosergeev systemd[1]: Started System Logging Service.
Oct 18 18:31:26 dosergeev rsyslogd[61358]: [origin software="rsyslogd" swVersion="8.24
12.0-1.el9" x-pid="61358" x-info="https://www.rsyslog.com"] start
Oct 18 18:31:26 dosergeev rsyslogd[61358]: imjournal: journal files changed, reloading
... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 18:32:40 dosergeev root[61367]: Daemon Debug Message
```

Рис. 9: Проверка мониторинга отладки rsyslog

## Использование journalctl

---

# Использование journalctl

- Посмотрим содержимое журнала с событиями с момента последнего запуска системы:  
journalctl

```
root@dosergeev:~
Oct 18 16:48:09 dosergeev.localdomain kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.
Oct 18 16:48:09 dosergeev.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9
Oct 18 16:48:09 dosergeev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.39.1.el9_6.x86_6
Oct 18 16:48:09 dosergeev.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-provided physical RAM map:
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000dff0000-0x0000000000dfffffff] ACPI data
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000041ffffffff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: NX (Execute Disable) protection: active
Oct 18 16:48:09 dosergeev.localdomain kernel: APIC: Static calls initialized
Oct 18 16:48:09 dosergeev.localdomain kernel: SMBIOS 2.5 present.
Oct 18 16:48:09 dosergeev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 18 16:48:09 dosergeev.localdomain kernel: Hypervisor detected: KVM
Oct 18 16:48:09 dosergeev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 18 16:48:09 dosergeev.localdomain kernel: kvm-clock: using sched offset of 9001186731 cycles
Oct 18 16:48:09 dosergeev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dfff
Oct 18 16:48:09 dosergeev.localdomain kernel: tsc: Detected 3399.994 MHz processor
Oct 18 16:48:09 dosergeev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: iact pfn = 0x420000, max arch pfn = 0x400000000
```

- Посмотрим содержимое журнала без использования пейджера: `journalctl -no-pager`

```
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Stopping System Logging Service...
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61160]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="61160" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Stopped System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Starting System Logging Service...
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Started System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="61358" x-info="https://www.rsyslog.com"] start
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 18:32:40 dosergeev.localdomain root[61367]: Daemon Debug Message
[root@dosergeev ~]#
```

Рис. 11: Вывод `journalctl -no-pager`

- Включим режим просмотра в реальном времени: `journalctl -f`

```
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Stopped System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Starting System Logging Service...
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Started System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pi
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: imjournal: journal files changed, reloading... [v8.2412.0-
Oct 18 18:32:40 dosergeev.localdomain root[61367]: Daemon Debug Message
Oct 18 18:35:15 dosergeev.localdomain root[61373]: debug
^C
[root@dosergeev ~]#
```

Рис. 12: Вывод `journalctl -f`

- Посмотрим события для UID=0: journalctl \_UID=0

```
[root@dosergeev ~]# journalctl _UID=0
Oct 18 16:48:10 dosergeev.localdomain systemd-journald[243]: Journal started
Oct 18 16:48:10 dosergeev.localdomain systemd-journald[243]: Runtime Journal (/run/log/journal/30fa918ba5df4b1f8dee15f25a4580d7) is 8.0M, max 314.6M, 306.6M free.
Oct 18 16:48:09 dosergeev.localdomain systemd-sysusers[246]: Creating group 'nobody' with GID 65534.
Oct 18 16:48:09 dosergeev.localdomain systemd-sysusers[246]: Creating group 'users' with GID 100.
Oct 18 16:48:09 dosergeev.localdomain systemd-sysusers[246]: Creating group 'dbus' with GID 81.
Oct 18 16:48:09 dosergeev.localdomain systemd-sysusers[246]: Creating user 'dbus' (System Message Bus) with UID 81 and GID 81.
Oct 18 16:48:10 dosergeev.localdomain systemd-modules-load[245]: Inserted module 'fuse'
Oct 18 16:48:10 dosergeev.localdomain systemd-modules-load[245]: Module 'msr' is built in
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Finished Load Kernel Modules.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Starting Apply Kernel Variables...
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Starting Create Volatile Files and Directories...
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Finished Apply Kernel Variables.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Finished Create Static Device Nodes in /dev.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Finished Create Volatile Files and Directories.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Finished Setup Virtual Console.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: dracut ask for additional cmdline parameters was skipped because no trigger condition checks were met.
Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Starting dracut cmdline hook...
```

Рис. 13: Вывод journalctl \_UID=0



- Отобразим последние 20 строк журнала: `journalctl -n 20`

```
([root@dosergeev ~]# journalctl -n 20
Oct 18 18:29:25 dosergeev.localdomain systemd[1]: Stopping The Apache HTTP Server...
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: httpd.service: Deactivated successfully.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: Stopped The Apache HTTP Server.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: httpd.service: Consumed 1.508s CPU time.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 18 18:29:27 dosergeev.localdomain httpd[61171]: Server configured, listening on: port 80
Oct 18 18:29:27 dosergeev.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 18 18:29:50 dosergeev.localdomain PackageKit[4769]: daemon quit
Oct 18 18:29:50 dosergeev.localdomain systemd[1]: packagekit.service: Deactivated successfully.
Oct 18 18:29:50 dosergeev.localdomain systemd[1]: packagekit.service: Consumed 18.713s CPU time.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Stopping System Logging Service...
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61160]: [origin software="rsyslogd" swVersion="8.2412.0
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Stopped System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Starting System Logging Service...
Oct 18 18:31:26 dosergeev.localdomain systemd[1]: Started System Logging Service.
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: [origin software="rsyslogd" swVersion="8.2412.0
Oct 18 18:31:26 dosergeev.localdomain rsyslogd[61358]: imjournal: journal files changed, reloading...
Oct 18 18:32:40 dosergeev.localdomain root[61367]: Daemon Debug Message
Oct 18 18:35:15 dosergeev.localdomain root[61373]: debug
lines 1-20/20 (END)
```

- Просмотрим только сообщения об ошибках: `journalctl -p err`

```
[[root@dosergeev ~]# journalctl -p err
(Oct 18 16:48:09 dosergeev.localdomain kernel: Warning: Deprecated Hardware is detected: x86_64-v2:AuthenticAMD:AMD Ryzen 5 2600 Six-Core Pro
(Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Invalid DMI field header.
(Oct 18 16:48:11 dosergeev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] «ERROR» vmwgfx seems to be running on an unsupported hypervisor.
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] «ERROR» This configuration is likely broken.
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] «ERROR» Please switch to a supported graphics device to avoid probl
(Oct 18 16:48:16 dosergeev.localdomain systemd[1]: Invalid DMI field header.
Oct 18 16:48:17 dosergeev.localdomain systemd-udevd[668]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:1 Only network interfaces can be renam
Oct 18 16:48:17 dosergeev.localdomain systemd-udevd[689]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only network interfaces can be ren
Oct 18 16:48:19 dosergeev.localdomain alsactl[827]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use case confi
Oct 18 16:48:21 dosergeev.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 18 17:05:42 dosergeev.localdomain systemd[1]: Failed to start dnf makecache.
Oct 18 17:28:17 dosergeev.localdomain gdm-password[2198]: gkr-pam: unable to locate daemon control file
Oct 18 17:28:18 dosergeev.localdomain systemd[2219]: Failed to start Application launched by gnome-session-binary.
Oct 18 17:28:20 dosergeev.localdomain systemd[2219]: Failed to start Application launched by gnome-session-binary.
Oct 18 17:28:22 dosergeev.localdomain gdm-wayland-session[1245]: GLib: Source ID 2 was not found when attempting to remove it
Oct 18 17:28:22 dosergeev.localdomain gdm-launch-environment[1187]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT(object)' failed
lines 1-17/17 (END)
```

Рис. 15: Вывод `journalctl -p err`

- Отфильтруем вывод журнала по точному времени: `journalctl --since "2025-10-18 18:28:00"`

```
[root@dosergeev ~]# journalctl --since "2025-10-18 18:28:00"
Oct 18 18:29:19 dosergeev.localdomain systemd[1]: Stopping System Logging Service...
Oct 18 18:29:19 dosergeev.localdomain rsyslogd[1267]: [origin software="rsyslogd" swVersion="8.2412.0-1
=Oct 18 18:29:19 dosergeev.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 18:29:19 dosergeev.localdomain systemd[1]: Stopped System Logging Service.
Oct 18 18:29:19 dosergeev.localdomain systemd[1]: rsyslog.service: Consumed 1.538s CPU time.
Oct 18 18:29:19 dosergeev.localdomain systemd[1]: Starting System Logging Service...
Oct 18 18:29:19 dosergeev.localdomain rsyslogd[61160]: [origin software="rsyslogd" swVersion="8.2412.0-
Oct 18 18:29:19 dosergeev.localdomain systemd[1]: Started System Logging Service.
Oct 18 18:29:19 dosergeev.localdomain rsyslogd[61160]: imjournal: journal files changed, reloading...
Oct 18 18:29:25 dosergeev.localdomain systemd[1]: Stopping The Apache HTTP Server...
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: httpd.service: Deactivated successfully.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: Stopped The Apache HTTP Server.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: httpd.service: Consumed 1.508s CPU time.
Oct 18 18:29:26 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
```

Рис. 16: Вывод `journalctl --since "2025-10-18 18:28:00"`

- Отфильтруем вывод журнала по относительно времени с выводом сообщений с ошибкой приоритета: `journalctl --since yesterday -p err`

```
[root@dosergeev ~]# journalctl --since yesterday -p err
(Oct 18 16:48:09 dosergeev.localdomain kernel: Warning: Deprecated Hardware is detected: x86_64-v
(Oct 18 16:48:10 dosergeev.localdomain systemd[1]: Invalid DMI field header.
(Oct 18 16:48:11 dosergeev.localdomain kernel: Warning: Unmaintained driver is detected: e1000
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configurat
(Oct 18 16:48:12 dosergeev.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch t
(Oct 18 16:48:16 dosergeev.localdomain systemd[1]: Invalid DMI field header.
Oct 18 16:48:17 dosergeev.localdomain systemd-udevd[668]: vboxuser: /etc/udev/rules.d/60-vboxadd
Oct 18 16:48:17 dosergeev.localdomain systemd-udevd[689]: vboxguest: /etc/udev/rules.d/60-vboxad
Oct 18 16:48:19 dosergeev.localdomain alsactl[827]: alsa-lib main.c:1554:(snd_use_case_mgr_open)
Oct 18 16:48:21 dosergeev.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 18 17:05:42 dosergeev.localdomain systemd[1]: Failed to start dnf makecache.
```

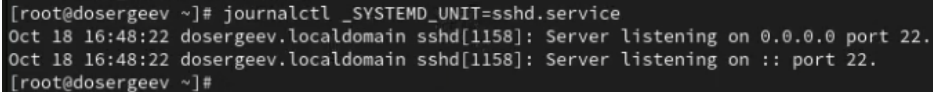
Рис. 17: Вывод `journalctl --since yesterday -p err`

- Выведем детальную информацию: journalctl -o verbose

```
([root@dosergeev ~]# journalctl -o verbose
(Sat 2025-10-18 16:48:09.946291 MSK [s=4892d18aa0e341aeb28f3c2ac661e87e;i=1;b=de39c2d0148e42a6800e95af590a8a59
(
  _SOURCE_MONOTONIC_TIMESTAMP=0
(
  _TRANSPORT=kernel
(
  PRIORITY=5
(
  SYSLOG_FACILITY=0
(
  SYSLOG_IDENTIFIER=kernel
(
  MESSAGE=Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org)
(
  _BOOT_ID=de39c2d0148e42a6800e95af590a8a59
(
  _MACHINE_ID=30fa918ba5df4b1f8dee15f25a4580d7
(
  _HOSTNAME=dosergeev.localdomain
(
  _RUNTIME_SCOPE=initrd
```

Рис. 18: Вывод journalctl -o verbose

- Просмотрим дополнительную информацию о службе, напмрм о sshd: `journalctl _SYSTEMD_UNIT=sshd.service`

A terminal window with a dark background and light text. The prompt is [root@dosergeev ~]#. The command journalctl \_SYSTEMD\_UNIT=sshd.service has been executed. The output shows two log entries for the sshd service on October 18 at 16:48:22, both from dosergeev.localdomain. The first entry shows the server listening on 0.0.0.0 port 22, and the second entry shows it listening on :: port 22. The prompt [root@dosergeev ~]# is visible at the bottom.

```
[root@dosergeev ~]# journalctl _SYSTEMD_UNIT=sshd.service
Oct 18 16:48:22 dosergeev.localdomain sshd[1158]: Server listening on 0.0.0.0 port 22.
Oct 18 16:48:22 dosergeev.localdomain sshd[1158]: Server listening on :: port 22.
[root@dosergeev ~]#
```

Рис. 19: Вывод `journalctl _SYSTEMD_UNIT=sshd.service`

Постоянный журнал journald

---

```
[root@dosergeev ~]# mkdir -p /var/log/journal
[root@dosergeev ~]# chown root:systemd-journal /var/log/journal
[root@dosergeev ~]# chmod 2755 /var/log/journal
[root@dosergeev ~]# ls -l /var/log/ | grep journal
drwxr-sr-x. 3 root    systemd-journal    46 Oct 18 18:44 journal
[root@dosergeev ~]#
```

Рис. 20: Настройка прав для /var/log/journal



Журнал systemd теперь стал постоянным. Посмотрим сообщения журнала с момента загрузки: `journalctl -b`.

```
[root@dosergeev ~]# journalctl -b
Oct 18 16:48:09 dosergeev.localdomain kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux
Oct 18 16:48:09 dosergeev.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at
Oct 18 16:48:09 dosergeev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.39.1.el9_6.x86_64 root=/dev/mapper
Oct 18 16:48:09 dosergeev.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-provided physical RAM map:
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dffff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffff] ACPI data
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 18 16:48:09 dosergeev.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000041ffffff] usable
Oct 18 16:48:09 dosergeev.localdomain kernel: NX (Execute Disable) protection: active
Oct 18 16:48:09 dosergeev.localdomain kernel: APIC: Static calls initialized
Oct 18 16:48:09 dosergeev.localdomain kernel: SMBIOS 2.5 present.
Oct 18 16:48:09 dosergeev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 18 16:48:09 dosergeev.localdomain kernel: Hypervisor detected: KVM
```

Рис. 21: Вывод сообщений журнала

## Ответы на контрольные вопросы

---

1. Какой файл используется для настройки rsyslogd?
  - `/etc/rsyslog.conf`
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?
  - `/var/log/secure`

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?
  - По умолчанию в дистрибутиве Rocky Linux установлена утилита logrotate, которая автоматически ротирует журналы. Чтобы узнать период ротации, можно посмотреть файл `/etc/logrotate.conf`

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

- Для ротации файлов журналов потребуется одна неделя (weekly)

```
[root@dosergeev ~]# cat /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
[root@dosergeev ~]#
```

Рис. 22: Файл конфигурации logrotate

4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл `/var/log/messages.info`?
  - `*.info /var/log/messages.info`
5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?
  - `tail -f <Журнал>`
6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?
  - `journalctl _PID=1 -since="09:00" -until "15:00"`

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

- `journalctl -b(-boot)`

8. Какая процедура позволяет сделать журнал journald постоянным?

- Создать директорию для хранения журналов: `mkdir -p /var/log/journal`
- Настроить права директории: `chown root:systemd-journal /var/log/journal; chmod 2775 /var/log/journal.`
- Перезапустить систему или службу: `reboot` или `killall -USR1 systemd-journal`

## Вывод

---



В результате выполнения лабораторной работы я получил навыки работы с утилитой `journalctl` и мониторинга событий в системе Linux.