

# Лабораторная работа №7

Управление журналами событий в системе

---

Юсупова К. Р.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Юсупова Ксения Равиловна
- Российский университет дружбы народов
- Номер студенческого билета- 1132247531
- [1132247531@pfur.ru]

## Вводная часть

---

Получить навыки работы с журналами мониторинга различных событий в системе.

## Выполнение лабораторной работы

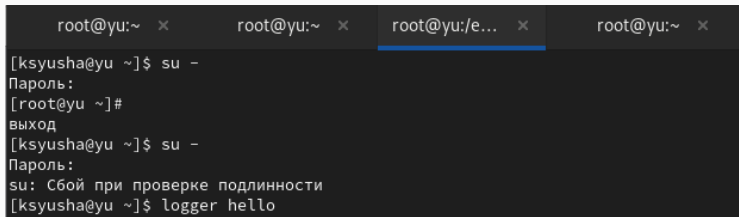
---

## Выполнение лабораторной работы

Запустили три вкладки терминала с правами администратора. Во второй вкладке начали мониторинг системных событий, затем остановили его Ctrl+C и запустили просмотр сообщений безопасности

```
root@yu:~ x root@yu:~ x root@yu/e... x root@yu:~ x
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# tail -f /var/log/messages
Oct 17 21:28:49 yu systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 21:28:49 yu systemd[1]: Started Fingerprint Authentication Daemon.
Oct 17 21:28:52 yu su[2833]: (to root) ksyusha on pts/0
Oct 17 21:28:52 yu systemd[1]: Starting Hostname Service...
Oct 17 21:28:52 yu systemd[1]: Started Hostname Service.
Oct 17 21:28:54 yu systemd[1475]: Started VTE child process 2876 launched by gno
me-terminal-server process 2172.
Oct 17 21:28:56 yu systemd[1475]: Started VTE child process 2903 launched by gno
me-terminal-server process 2172.
Oct 17 21:29:02 yu su[2929]: (to root) ksyusha on pts/1
Oct 17 21:29:13 yu su[2964]: (to root) ksyusha on pts/2
Oct 17 21:29:20 yu systemd[1]: fprintd.service: Deactivated successfully.
Oct 17 21:29:43 yu systemd[1]: systemd-hostnamed.service: Deactivated successf
ly.
Oct 17 21:30:08 yu systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 21:30:08 yu systemd[1]: Started Fingerprint Authentication Daemon.
Oct 17 21:30:13 yu su[3019]: FAILED SU (to root) ksyusha on pts/2
Oct 17 21:30:30 yu ksyusha[3042]: hello
Oct 17 21:30:38 yu systemd[1]: fprintd.service: Deactivated successfully.
^C
[root@yu ~]# tail -n 20 /var/log/secure
Oct 17 21:20:10 yu polkitd[776]: Acquired the name org.freedesktop.PolicyKit1 on
```

В третьей вкладке вернулись к учётной записи пользователя и ввели неверный пароль root.  
Во второй вкладке появилось сообщение о failed su, затем ввели logger hello



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

Рис. 2: Логирование событий аутентификации



## Выполнение лабораторной работы

В первой вкладке установили и запустили веб-сервер Apache

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

Установлен:

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

Выполнено !

Во второй вкладке просмотрели журнал ошибок веб-службы

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

Рис. 4: Журнал ошибок Apache

В третьей вкладке настроили логирование ошибок Apache через syslog, создали конфигурационные файлы для мониторинга и отладки

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

Рис. 5: Настройка логирования Apache

В первой вкладке перезагрузили конфигурацию rsyslogd и веб-службы

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

Рис. 6: Перезагрузка служб

Во второй вкладке запустили мониторинг отладочной информации и просмотрели debug-сообщения

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

Рис. 7: Мониторинг отладочной информации

## Выполнение лабораторной работы

Просмотрели журнал событий с последнего запуска системы и содержимое журнала без пейджера

```
окт 17 21:19:52 yu.k.r kernel: VFS: Disk quotas dquot_6.6.0
окт 17 21:19:52 yu.k.r kernel: VFS: Dquot-cache hash table entries: 512 (order
окт 17 21:19:52 yu.k.r kernel: pnp: PnP ACPI init
окт 17 21:19:52 yu.k.r kernel: pnp: PnP ACPI: found 2 devices
окт 17 21:19:52 yu.k.r kernel: clocksource: acpi_pm: mask: 0xffffffff max_cycles:
окт 17 21:19:52 yu.k.r kernel: NET: Registered PF_INET protocol family
окт 17 21:19:52 yu.k.r kernel: IP idents hash table entries: 131072 (order: 8,
окт 17 21:19:52 yu.k.r kernel: tcp_listen_portaddr_hash hash table entries: 409
окт 17 21:19:52 yu.k.r kernel: Table-perturb hash table entries: 65536 (order:
окт 17 21:19:52 yu.k.r kernel: TCP established hash table entries: 65536 (order
окт 17 21:19:52 yu.k.r kernel: TCP bind hash table entries: 65536 (order: 8, 10
окт 17 21:19:52 yu.k.r kernel: TCP: Hash tables configured (established 65536 b
окт 17 21:19:52 yu.k.r kernel: MPTCP token hash table entries: 8192 (order: 5,
окт 17 21:19:52 yu.k.r kernel: UDP hash table entries: 4096 (order: 5, 131072 b
окт 17 21:19:52 yu.k.r kernel: UDP-Lite hash table entries: 4096 (order: 5, 131
окт 17 21:19:52 yu.k.r kernel: NET: Registered PF_UNIX/PF_LOCAL protocol family
окт 17 21:19:52 yu.k.r kernel: NET: Registered PF_XDP protocol family
окт 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 4 [io 0x0000-0x0cf7 w
окт 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 5 [io 0x0d00-0xffff w
окт 17 21:19:52 yu.k.r kernel: pci_bus 0000:00: resource 6 [mem 0x000a0000-0x00
[root@yu ~]# journalctl --no-pager
окт 17 21:19:52 yu.k.r kernel: Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockb
uild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red
Hat 11.5.0-5), GNU ld version 2.35.2-63.el9) #1 SMP PREEMPT_DYNAMIC Fri May 23 2
2:47:01 UTC 2025
окт 17 21:19:52 yu.k.r kernel: The list of certified hardware and cloud instance
s for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https/
```

## Выполнение лабораторной работы

Запустили просмотр журнала в реальном времени и изучили доступные параметры фильтрации

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

# Выполнение лабораторной работы

Просмотрели события для UID 0, последние 20 строк журнала и сообщения об ошибках

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



# Выполнение лабораторной работы

Просмотрели сообщения со вчерашнего дня, ошибки за этот период, детальную информацию и логи sshd

```
окт 17 21:19:52 yu.k.r kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
окт 17 21:19:52 yu.k.r kernel: RAMDISK: [mem 0x30aa5000-0x3454afff]
окт 17 21:19:52 yu.k.r kernel: ACPI: Early table checksum verification disabled
окт 17 21:19:52 yu.k.r kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
окт 17 21:19:52 yu.k.r kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX )
[root@yu ~]# journalctl --since yesterday -p err
окт 17 21:19:52 yu.k.r kernel: Warning: Deprecated Hardware is detected: x86_64
окт 17 21:19:52 yu.k.r systemd[1]: Invalid DMI field header.
окт 17 21:19:53 yu.k.r kernel: Warning: Unmaintained driver is detected: e1000
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configur
окт 17 21:19:54 yu.k.r kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch
окт 17 21:20:01 yu.k.r systemd[1]: Invalid DMI field header.
окт 17 21:20:08 yu.k.r alsactl[806]: alsa-lib main.c:1554:(snd_use_case_mgr_ope
окт 17 21:20:15 yu.k.r kernel: Warning: Unmaintained driver is detected: ip_set
окт 17 21:20:27 yu.k.r setroubleshoot[823]: SELinux запущен /usr/bin/lsmd до
окт 17 21:20:54 yu.k.r systemd[1475]: Failed to start Application launched by g
окт 17 21:21:01 yu.k.r gdm-wayland-session[1023]: GLib: Source ID 2 was not fou
окт 17 21:21:01 yu.k.r gdm-launch-environment[960]: GLib-GObject: g_object_unr
[root@yu ~]# journalctl -o verbose
Fri 2025-10-17 21:19:52.950551 MSK [s=ce6273bddcf5474ba775f0e3c93e99b3;i=1;b=98
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockbuild@iad1-prod-bui
_BOOT_ID=984507a3bf2645daaec282806b0eb29d
_MACHINE_ID=fea32d02ff8b4e2695eb396f08cec4f5
_HOSTNAME=yu.k.r
_RUNTIME_SCOPE=initrd
```

## Выполнение лабораторной работы

Создали каталог для постоянного хранения журналов, настроили права и активировали постоянное хранение journald

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# mkdir -p /var/log/journal
[root@yu ~]# chown root:systemd-journal /var/log/journal
[root@yu ~]# chmod 2755 /var/log/journal
[root@yu ~]# killall -USR1 systemd-journald
[root@yu ~]# journalctl -b
окт 17 21:19:52 yu.k.r kernel: Linux version 5.14.0-570.17.1.el9_6.x86_64 (mock>
окт 17 21:19:52 yu.k.r kernel: The list of certified hardware and cloud instance>
окт 17 21:19:52 yu.k.r kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.>
окт 17 21:19:52 yu.k.r kernel: [Firmware Bug]: TSC doesn't count with P0 frequen>
окт 17 21:19:52 yu.k.r kernel: BIOS-provided physical RAM map:
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x0000000000009fc00-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfff>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dfff>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fff>
окт 17 21:19:52 yu.k.r kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000021fff>
окт 17 21:19:52 yu.k.r kernel: NX (Execute Disable) protection: active
окт 17 21:19:52 yu.k.r kernel: APIC: Static calls initialized
окт 17 21:19:52 yu.k.r kernel: SMBIOS 2.5 present.
окт 17 21:19:52 yu.k.r kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vio>
окт 17 21:19:52 yu.k.r kernel: Hypervisor detected: KVM
окт 17 21:19:52 yu.k.r kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
окт 17 21:19:52 yu.k.r kernel: kvm-clock: using sched offset of 8008313700 cycl>
окт 17 21:19:52 yu.k.r kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff>
```

## Выводы

---

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