

# Лабораторная работа №7

Управление журналами событий в системе

---

Тукаев Тимур

9 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить навыки работы с журналами мониторинга различных событий в системе Linux, освоить использование служб `rsyslogd` и `journald`, а также методы фильтрации и анализа сообщений.

## Ход выполнения работы

---

[illegible]

Рис. 1: Мониторинг системных сообщений

Запуск `tail -f /var/log/messages` для просмотра событий ядра и служб в реальном времени.



## Отправка пользовательского сообщения

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# tail -n 20 /var/log/secure  
Oct 9 13:49:03 titukaev gdm-password[1994]: gkr-pam: stashed password to try later in open session  
Oct 9 13:49:03 titukaev (systemd)[2005]: pam_unix(systemd-user:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)  
Oct 9 13:49:03 titukaev gdm-password[1994]: pam_unix(gdm-password:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)  
Oct 9 13:49:03 titukaev gdm-password[1994]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring  
Oct 9 13:49:09 titukaev gdm-launch-environment[1247]: pam_unix(gdm-launch-environment:session): session closed for user gdm  
Oct 9 13:49:41 titukaev (systemd)[3216]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)  
Oct 9 13:49:41 titukaev su[3183]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 13:57:39 titukaev su[3183]: pam_unix(su:session): session closed for user root  
Oct 9 13:58:16 titukaev (systemd)[4644]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)  
Oct 9 13:58:16 titukaev su[4619]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 14:05:19 titukaev su[4619]: pam_unix(su:session): session closed for user root  
Oct 9 14:05:25 titukaev su[5649]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 14:10:14 titukaev su[5649]: pam_unix(su:session): session closed for user root  
Oct 9 14:15:22 titukaev gdm-password[6995]: gkr-pam: unlocked login keyring  
Oct 9 14:18:10 titukaev su[7376]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 14:18:17 titukaev su[7443]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 14:18:22 titukaev su[7503]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)  
Oct 9 14:18:36 titukaev su[7503]: pam_unix(su:session): session closed for user root  
Oct 9 14:18:40 titukaev unix_chkpwd[7589]: password check failed for user (root)  
Oct 9 14:18:40 titukaev su[7574]: pam_unix(su:auth): authentication failure; logname=titukaev uid=1000 euid=0 tty=/dev/pts/1 ruser=titukaev rhost= user=root  
root@titukaev:/home/titukaev#
```

Рис. 3: Регистрация пользовательского сообщения

Команда `logger hello` добавляет сообщение в `/var/log/messages`.

# Настройка rsyslog для Apache

```
##### 2023-03-21 10:00:00 #####

Installed:
apr-1.7.5-2.el10.x86_64                apr-util-1.6.3-21.el10.x86_64        apr-util-ldap-1.6.3-21.el10.x86_64
apr-util-openssl-1.6.3-21.el10.x86_64  httpd-2.4.63-1.el10_0.2.x86_64        httpd-core-2.4.63-1.el10_0.2.x86_64
httpd-filesystem-2.4.63-1.el10_0.2.noarch  httpd-tools-2.4.63-1.el10_0.2.x86_64  mod_http2-2.0.29-2.el10_0.1.x86_64
mod_lua-2.4.63-1.el10_0.2.x86_64        rocky-logos-httpd-100.4-7.el10.noarch

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

Рис. 4: Настройка передачи логов Apache в rsyslog

Добавлена строка **ErrorLog syslog:local1** в **/etc/httpd/conf/httpd.conf**.



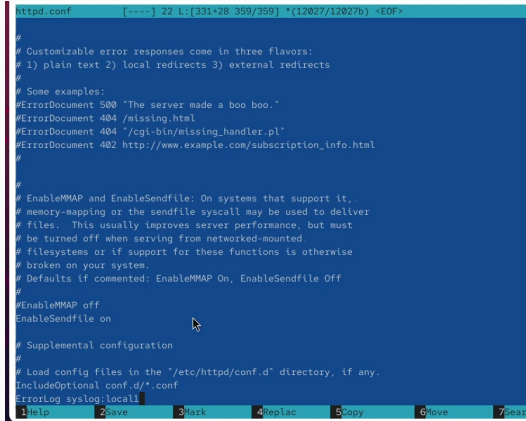
## Создание отдельного файла для логов Apache

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# tail -f /var/log/httpd/error_log
[Thu Oct 09 14:20:32.679626 2025] [suexec:notice] [pid 8057:tid 8057] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Thu Oct 09 14:20:32.711112 2025] [lbmethod_heartbeat:notice] [pid 8057:tid 8057] AH02282: No slotmem from mod_heartbeat
[Thu Oct 09 14:20:32.711595 2025] [systemd:notice] [pid 8057:tid 8057] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 09 14:20:32.712671 2025] [npm_event:notice] [pid 8057:tid 8057] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Thu Oct 09 14:20:32.712680 2025] [core:notice] [pid 8057:tid 8057] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 5: Создание конфигурации rsyslog

Создан файл `/etc/rsyslog.d/httpd.conf` с правилом `local1.*  
-/var/log/httpd-error.log`.

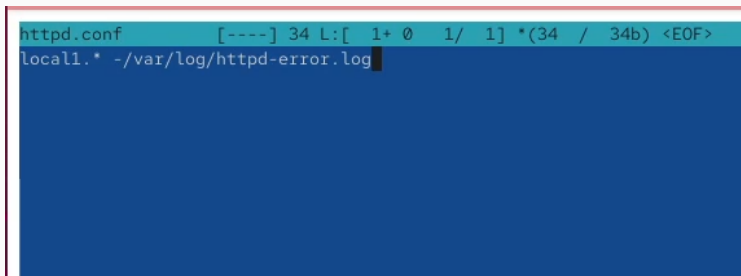
## Настройка отладочного журнала



```
httpd.conf [-----] 22 L:[331+28 359/359] *(12027/12027b) <EOF>
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#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:local
```

Рис. 6: Создание debug.conf для отладки

Добавлено правило \*.debug /var/log/messages-debug для регистрации отладочной



```
httpd.conf [----] 34 L:[ 1+ 0 1/ 1] *(34 / 34b) <EOF>
local1.* -/var/log/httpd-error.log
```

Рис. 7: Регистрация отладочного сообщения

Сообщение **Daemon Debug Message** успешно зафиксировано в `/var/log/messages-debug`.

# Использование journalctl

```
Oct 09 13:48:22 titukaev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rocky)
Oct 09 13:48:22 titukaev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mapper:
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-provided physical RAM map:
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000000ffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] ACPI data
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 09 13:48:22 titukaev.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: NX (Execute Disable) protection: active
Oct 09 13:48:22 titukaev.localdomain kernel: APIC: Static calls initialized
Oct 09 13:48:22 titukaev.localdomain kernel: SMBIOS 2.5 present.
Oct 09 13:48:22 titukaev.localdomain kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 09 13:48:22 titukaev.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 09 13:48:22 titukaev.localdomain kernel: Hypervisor detected: KVM
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 09 13:48:22 titukaev.localdomain kernel: kvm-clock: using sched offset of 4612772641 cycles
Oct 09 13:48:22 titukaev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_n
Oct 09 13:48:22 titukaev.localdomain kernel: tsc: Detected 3187.202 MHz processor
Oct 09 13:48:22 titukaev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 09 13:48:22 titukaev.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 09 13:48:22 titukaev.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 09 13:48:22 titukaev.localdomain kernel: total RAM covered: 4096M
Oct 09 13:48:22 titukaev.localdomain kernel: Found optimal setting for mtrr clean up
Oct 09 13:48:22 titukaev.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RAM: 0G
Oct 09 13:48:22 titukaev.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
```

lines 1-29

Рис. 8: Просмотр журнала через journalctl

Просмотр системных сообщений, фильтрация по UID и модулю `sshd.service`.

```
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev#  
root@titukaev:/home/titukaev# mkdir -p /var/log/journal  
root@titukaev:/home/titukaev# chown root:systemd-journal /var/log/journal/  
root@titukaev:/home/titukaev# chmod 2755 /var/log/journal/  
root@titukaev:/home/titukaev# killall -USR1 systemd-journald  
root@titukaev:/home/titukaev#
```

Рис. 9: Создание каталога для постоянного хранения журнала

Создан каталог `/var/log/journal` и настроены права для обеспечения постоянного хранения логов.

## Итоги работы

---

В результате лабораторной работы изучены инструменты системного журналирования Linux. Настроено взаимодействие служб **rsyslogd** и **journald**, реализовано хранение логов в постоянном режиме.

Получены навыки фильтрации, анализа и управления системными событиями.