

Лабораторная работа №7

Управление журналами событий в системе

Максат Хемраев

2 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе Linux.

Ход выполнения работы

- Запуск мониторинга через `tail -f /var/log/messages`
- Проверка ошибок при вводе неверного пароля
- Использование команды `logger` для записи сообщений

```
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for cups-fsfilesystem
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for cmake-fsfilesystem
Sep 30 11:02:38 mhemraev packagekitd[1351]: Failed to get cache filename for kernel
Sep 30 11:02:40 mhemraev su[3412]: FAILED SU (to root) mhemraev on pts/2
Sep 30 11:02:42 mhemraev kernel: traps: VBoxClient[3441] trap int3 ip:41dd1b sp:7eff4cbb4cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 30 11:02:42 mhemraev systemd-coredump[3442]: Process 3438 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 30 11:02:42 mhemraev systemd[1]: Started systemd-coredump@18-3442-0.service - Process Core Dump (PID 3442/UID 0).
Sep 30 11:02:42 mhemraev systemd-coredump[3443]: Process 3438 (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 libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3441:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000045041
```

Рис. 1: Мониторинг системных сообщений

Проверка безопасности

- Анализ файла /var/log/secure
- Отображение сообщений об ошибках авторизации

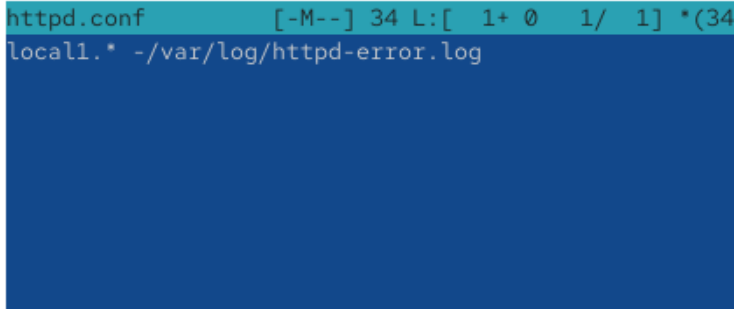
```
root@mhemraev:/home/mhemraev# tail -n 20 /var/log/secure
Sep 30 11:00:20 mhemraev sshd[1152]: Server listening on 0.0.0.0 port 22.
Sep 30 11:00:20 mhemraev sshd[1152]: Server listening on :: port 22.
Sep 30 11:00:20 mhemraev (systemd)[1225]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm
(uid=0)
Sep 30 11:00:20 mhemraev gdm-launch-environment[1196]: pam_unix(gdm-launch-environment:session): session opened for
user gdm(uid=42) by (uid=0)
Sep 30 11:00:54 mhemraev unix_chkpwd[1923]: password check failed for user (mhemraev)
Sep 30 11:00:54 mhemraev gdm-password[1906]: pam_unix(gdm-password:auth): authentication failure; logname= uid=0 eu
id=0 tty=/dev/tty1 ruser= rhost= user=mhemraev
Sep 30 11:00:54 mhemraev gdm-password[1906]: gkr-pam: unable to locate daemon control file
Sep 30 11:00:54 mhemraev gdm-password[1906]: gkr-pam: stashed password to try later in open session
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: unable to locate daemon control file
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: stashed password to try later in open session
Sep 30 11:00:59 mhemraev (systemd)[1936]: pam_unix(systemd-user:session): session opened for user mhemraev(uid=1000)
by mhemraev(uid=0)
Sep 30 11:00:59 mhemraev gdm-password[1926]: pam_unix(gdm-password:session): session opened for user mhemraev(uid=1
000) by mhemraev(uid=0)
Sep 30 11:00:59 mhemraev gdm-password[1926]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep 30 11:01:10 mhemraev gdm-launch-environment[1196]: pam_unix(gdm-launch-environment:session): session closed for
user gdm
Sep 30 11:01:24 mhemraev (systemd)[3042]: pam_unix(systemd-user:session): session opened for user root(uid=0) by roo
t(uid=0)
Sep 30 11:01:24 mhemraev su[3011]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:01:35 mhemraev su[3130]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:01:45 mhemraev su[3213]: pam_unix(su:session): session opened for user root(uid=0) by mhemraev(uid=1000)
Sep 30 11:02:35 mhemraev su[3213]: pam_unix(su:session): session closed for user root
Sep 30 11:02:38 mhemraev su[3412]: pam_unix(su:auth): authentication failure; logname=mhemraev uid=1000 euid=0 tty=/
dev/pts/2 ruser=mhemraev rhost= user=root
root@mhemraev:/home/mhemraev#
```

- Установка и запуск Apache
- Перенаправление ошибок httpd через syslog
- Создание правила `local1.*` для `/var/log/httpd-error.log`

```
httpd.conf [----] 22 L:[331+28 359/359] *(12027/12027b)
#
# 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
```

mhemraev@m
httpd.conf

- Перезапуск служб rsyslog и httpd
- Создание отдельного файла для ошибок Apache
- Проверка записи в /var/log/httpd-error.log

A screenshot of a terminal window showing the configuration for the httpd.conf file in rsyslog. The first line is highlighted in teal and contains the text 'httpd.conf' followed by some status information in brackets. The second line is on a dark blue background and shows the rule definition: 'local1.* -/var/log/httpd-error.log'.

```
httpd.conf      [-M--] 34 L:[ 1+ 0  1/ 1] *(34  
local1.* -/var/log/httpd-error.log
```

Рис. 4: Создание правила для httpd

- Создание debug.conf с правилом *.debug
- Просмотр отладочных сообщений в messages-debug
- Отправка тестового сообщения через logger

```
x103a3d)#012#1 0x000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000004500b6 n/a (n/a + 0x0)#012#3 0x0000000000041b559 n/a (n/a + 0x0)#012#4 0x0000000000041838a n/a (n/a + 0x0)#012#5 0x00000000000417d6a n/a (n/a + 0x0)#012#6 0x00000000000404860 n/a (n/a + 0x0)#012#7 0x0000000000045041c n/a (n/a + 0x0)#012#8 0x000000000004355d0 n/a (n/a + 0x0)#012#9 0x000007eff5b27111a start_thread (libc.so.6 + 0x9511a)#012#10 0x000007eff5b2e1c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 5674:#012#0 0x000007eff5b2dfa3d syscall (libc.so.6 + 0x103a3d)#012#1 0x000000000004344e2 n/a (n/a + 0x0)#012#2 0x00000000000450066 n/a (n/a + 0x0)#012#3 0x00000000000405123 n/a (n/a + 0x0)#012#4 0x000007eff5b20630e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007eff5b2063c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 30 11:12:51 mhemraev systemd[1]: systemd-coredump@138-5678-0.service: Deactivated successfully.
Sep 30 11:12:53 mhemraev root[5684]: Daemon Debug Message
```

Рис. 5: Проверка отладочного сообщения

Использование journalctl

- Просмотр журналов после загрузки системы
- Режим реального времени через `journalctl -f`
- Фильтрация по UID, приоритету и диапазону времени

```
root@mhemraev:/home/mhemraev# journalctl
Sep 30 11:00:15 mhemraev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0)
Sep 30 11:00:15 mhemraev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009bfff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000001000000-0x00000000007ffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000007ffff0000-0x00000000007ffff] ACPI data
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000fec000000-0x00000000fec00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000fee000000-0x00000000fee00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000ffff00000-0x00000000ffffffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 11:00:15 mhemraev.localdomain kernel: APIC: Static calls initialized
Sep 30 11:00:15 mhemraev.localdomain kernel: SMBIOS 2.5 present.
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 11:00:15 mhemraev.localdomain kernel: Hypervisor detected: KVM
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: using sched offset of 4365313689 cycles
Sep 30 11:00:15 mhemraev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e40
Sep 30 11:00:15 mhemraev.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: e820: remove [mem 0x0000a0000-0x0000ffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: last_pfn = 0x80000 max_arch_pfn = 0x400000000
Sep 30 11:00:15 mhemraev.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35) built from 16 vari
```

Рис. 6: Просмотр журнала systemd

- Вывод в режиме verbose
- Анализ событий службы sshd

```

Tue 2025-09-30 11:00:15.734488 MSK [s=88cff91ce96e4368bd3belaca512d1eb;i=2;b=1d5ee01a6db1475ca697b01ca33b4470;m=bbc>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=1d5ee01a6db1475ca697b01ca33b4470
_MACHINE_ID=c69c609d0a8742be8f2a1e4538ef6441
_HOSTNAME=mhemraev.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mapper/rl_vbox-root >
Tue 2025-09-30 11:00:15.734497 MSK [s=88cff91ce96e4368bd3belaca512d1eb;i=3;b=1d5ee01a6db1475ca697b01ca33b4470;m=bbc>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
root@mhemraev:/home/mhemraev# journalctl _SYSTEMD_UNIT=sshd.service
Sep 30 11:00:20 mhemraev.localdomain (sshd)[1152]: sshd.service: Referenced but unset environment variable evaluat>
Sep 30 11:00:20 mhemraev.localdomain sshd[1152]: Server listening on 0.0.0.0 port 22.
Sep 30 11:00:20 mhemraev.localdomain sshd[1152]: Server listening on :: port 22.
root@mhemraev:/home/mhemraev#
```

Рис. 7: Фильтрация по sshd

Постоянный журнал journald

- Создание каталога /var/log/journal
- Настройка прав доступа
- Перезапуск journald для активации

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

Sep 30 11:00:15 mhemraev.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build0)
Sep 30 11:00:15 mhemraev.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-provided physical RAM map:
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000007ffff000-0x00000000007fffff] ACPI data
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 30 11:00:15 mhemraev.localdomain kernel: NX (Execute Disable) protection: active
Sep 30 11:00:15 mhemraev.localdomain kernel: APIC: Static calls initialized
Sep 30 11:00:15 mhemraev.localdomain kernel: SMBIOS 2.5 present.
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 30 11:00:15 mhemraev.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 30 11:00:15 mhemraev.localdomain kernel: Hypervisor detected: KVM
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 30 11:00:15 mhemraev.localdomain kernel: kvm-clock: using sched offset of 4365313689 cycles
Sep 30 11:00:15 mhemraev.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4d
Sep 30 11:00:15 mhemraev.localdomain kernel: tsc: Detected 3187.202 MHz processor
```

Рис. 8: Просмотр постоянного журнала

Итоги работы

В ходе работы были изучены: - Основы журналирования в Linux - Методы настройки rsyslog и journald - Фильтрация и просмотр системных сообщений - Создание постоянного журнала и разделение логов по уровням важности