Лабораторная работа №7

Управление журналами событий в системе

Турсунов Мухамметназар

10 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки работы с системными журналами Linux, включая настройку служб **rsyslog** и **systemd-journald**, а также анализ событий при помощи утилиты **journalctl**.

Ход выполнения работы

Мониторинг системных событий

```
root@mtursunov:/home/mtursunov# tail -f /var/log/messages
Oct 10 11:59:18 mtursunov systemd-coredump[3862]: Process 3858 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 11:59:18 mtursunov systemd[1]: Started systemd-coredump@25-3862-0.service - Process Core Dump (PI
D 3862/UID 0).
Oct 10 11:59:18 mtursunov systemd-coredump[3863]: Process 3858 (VBoxClient) of user 1000 dumped core.#01
2#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 rp
m libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012S
tack trace of thread 3861:#012#0  0x000000000041dd1b n/a (n/a + 0x0)#012#1  0x000000000041dc94 n/a (n/a
 + 0x0)#012#2  0x0000000000045041c n/a (n/a + 0x0)#012#3  0x00000000004355d0 n/a (n/a + 0x0)#012#4  0x0000
7fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#5  0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1056bc
)#012#012Stack trace of thread 3859:#012#0  0x00007fd4e17424bd syscall (libc.so.6 + 0x1034bd)#012#1  0x0
000000000434c30 n/a (n/a + 0x0)#012#2  0x0000000000450bfb n/a (n/a + 0x0)#012#3  0x000000000043566a n/a
(n/a + 0x0)#012#4  0x000000000045041c n/a (n/a + 0x0)#012#5  0x00000000004355d0 n/a (n/a + 0x0)#012#6  0
x00007fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#7  0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1
056bc)#012#012Stack trace of thread 3858:#012#0  0x00007fd4e17424bd syscall (libc.so.6 + 0x1034bd)#012#1
  0x00000000004344e2 n/a (n/a + 0x0)#012#2  0x0000000000450066 n/a (n/a + 0x0)#012#3  0x0000000000405123
 n/a (n/a + 0x0)#012#4  0x00007fd4e166930e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5  0x00007fd
4e16693c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6  0x00000000004044aa n/a (n/a + 0x0)#
012ELF object binary architecture: AMD x86-64
Oct 10 11:59:18 mtursunov systemd[1]: systemd-coredump@25-3862-0.service: Deactivated successfully.
Oct 10 11:59:21 mtursunov systemd[1]: fprintd.service: Deactivated successfully.
Oct 10 11:59:23 mtursunov kernel: traps: VBoxClient[3878] trap int3 ip:41dd1b sp:7fd4d2fb4cd0 error:0 in
 VBoxClient[1dd1b,400000+bb000]
Oct 10 11:59:23 mtursunov systemd-coredump[3879]: Process 3875 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 11:59:23 mtursunov systemd[1]: Started systemd-coredump@26-3879-0.service - Process Core Dump (PI
D 3879/UID 0).
```

Рис. 1: Мониторинг системных событий через tail -f /var/log/messages

Ошибка авторизации su -

```
0000000004344e2 n/a (n/a + 0x0)#012#2  0x0000000000450066 n/a (n/a + 0x0)#012#3  0x0000000000405123 n/a
(n/a + 0x0)#012#4  0x00007fd4e166930e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5  0x00007fd4e166
93c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6  0x00000000004044aa n/a (n/a + 0x0)#012EL
F object binary architecture: AMD x86-64
Oct 10 12:00:24 mtursunov systemd[1]: systemd-coredump@38-4013-0.service: Deactivated successfully.
Oct 10 12:00:27 mtursunov su[4000]: FAILED SU (to root) mtursunov on pts/2
Oct 10 12:00:29 mtursunov kernel: traps: VBoxClient[4024] trap int3 ip:41dd1b sp:7fd4d2fb4cd0 error:0 in
 VBoxClient[1dd1b,400000+bb000]
Oct 10 12:00:29 mtursunov systemd-coredump[4025]: Process 4021 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 12:00:29 mtursunov systemd[1]: Started systemd-coredump@39-4025-0.service - Process Core Dump (PI
D 4025/UID 0).
Oct 10 12:00:29 mtursunov systemd-coredump[4026]: Process 4021 (VBoxClient) of user 1000 dumped core.#01
```

Рис. 2: Ошибка авторизации при попытке su -

Команда logger

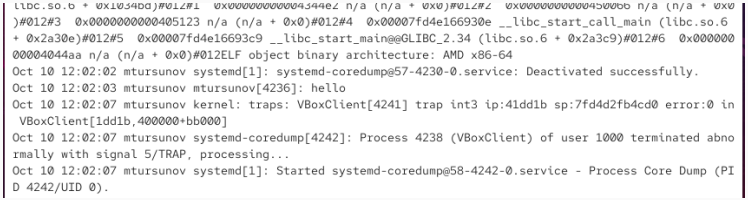

Рис. 3: Результат работы команды logger hello

Просмотр журнала безопасности

```
root@mtursunov:/home/mtursunov# tail -n 20 /var/log/secure
Oct 10 11:47:01 mtursunov su[5607]: pam_unix(su:session): session opened for user root(uid=0) by mtursun
ov(uid=1000)
Oct 10 11:51:50 mtursunov su[5607]: pam_unix(su:session): session closed for user root
Oct 10 11:51:56 mtursunov su[6299]: pam_unix(su:session): session opened for user root(uid=0) by mtursun
ov(uid=1000)
Oct 10 11:55:54 mtursunov sshd[1207]: Server listening on 0.0.0.0 port 22.
Oct 10 11:55:54 mtursunov sshd[1207]: Server listening on :: port 22.
Oct 10 11:55:55 mtursunov (systemd)[1332]: pam_unix(systemd-user:session): session opened for user gdm(u
id=42) by gdm(uid=0)
Oct 10 11:55:56 mtursunov gdm-launch-environment][1251]: pam_unix(gdm-launch-environment:session): sessi
on opened for user gdm(uid=42) by (uid=0)
Oct 10 11:57:04 mtursunov gdm-password][2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:04 mtursunov gdm-password][2342]: gkr-pam: stashed password to try later in open session
Oct 10 11:57:04 mtursunov (systemd)[2353]: pam_unix(systemd-user:session): session opened for user mturs
unov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password][2342]: pam_unix(gdm-password:session): session opened for user m
tursunov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password][2342]: gkr-pam: gnome-keyring-daemon started properly and unlock
ed keyring
Oct 10 11:57:09 mtursunov gdm-launch-environment][1251]: pam_unix(gdm-launch-environment:session): sessi
on closed for user gdm
Oct 10 11:58:53 mtursunov (systemd)[3659]: pam_unix(systemd-user:session): session opened for user root(
uid=0) by root(uid=0)
Oct 10 11:58:53 mtursunov su[3634]: pam_unix(su:session): session opened for user root(uid=0) by mtursun
ov(uid=1000)
Oct 10 11:58:59 mtursunov su[3729]: pam_unix(su:session): session opened for user root(uid=0) by mtursun
ov(uid=1000)
Oct 10 11:59:03 mtursunov su[3793]: pam_unix(su:session): session opened for user root(uid=0) by mtursun
ov(uid=1000)
Oct 10 12:00:23 mtursunov su[3793]: pam_unix(su:session): session closed for user root
Oct 10 12:00:26 mtursunov unix_chkpwd[4019]: password check failed for user (root)
```

Рис. 4: Вывод файла /var/log/secure

Настройка rsyslog для Apache

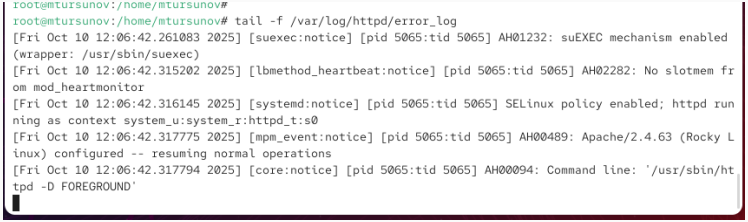

Рис. 5: Мониторинг журнала ошибок Apache

Перенаправление логов Apache в системный журнал

```
#
# 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:local1

^G Help       ^O Write Out  ^F Where Is   ^K Cut       ^T Execute    ^C Location   M
^X Exit       ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M
```

Рис. 7: Создание правила для перенаправления логов Apache

Перезапуск служб rsyslog и httpd

```
root@mtursunov:/home/mtursunov# nano /etc/httpd/conf/httpd.conf
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# cd /etc/rsyslog.d/
root@mtursunov:/etc/rsyslog.d# touch httpd.conf
root@mtursunov:/etc/rsyslog.d# nano httpd.conf
root@mtursunov:/etc/rsyslog.d#
root@mtursunov:/etc/rsyslog.d# systemctl restart rsyslog.service
root@mtursunov:/etc/rsyslog.d# systemctl restart httpd
root@mtursunov:/etc/rsyslog.d#
root@mtursunov:/etc/rsyslog.d# touch debug.conf
root@mtursunov:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > debug.conf
root@mtursunov:/etc/rsyslog.d# systemctl restart httpd
root@mtursunov:/etc/rsyslog.d# systemctl restart rsyslog.service
root@mtursunov:/etc/rsyslog.d#
```

Рис. 8: Перезапуск служб rsyslog и httpd

Запись отладочного сообщения

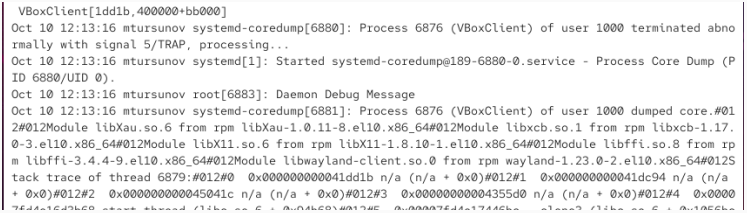

Рис. 9: Результат регистрации отладочного сообщения через logger

Работа с journalctl

Общий просмотр журнала

Рис. 10: Просмотр системного журнала с момента загрузки

Просмотр журнала в реальном времени

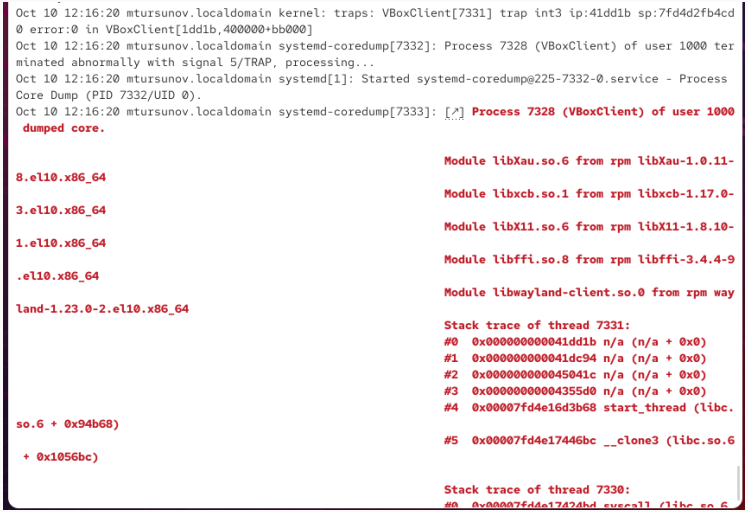

Рис. 11: Просмотр журнала в реальном времени

Параметры фильтрации journalctl

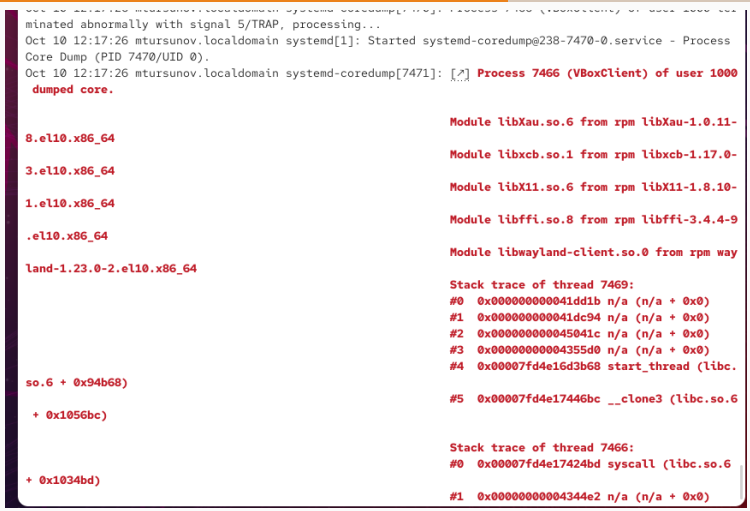

Рис. 12: Отображение параметров фильтрации journalctl

Сообщения UID 0

```
root@mtursunov:/home/mtursunov# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=                    JOB_TYPE=
_AUDIT_SESSION=                     JOURNAL_NAME=
AVAILABLE=                          JOURNAL_PATH=
AVAILABLE_PRETTY=                   _KERNEL_DEVICE=
_BOOT_ID=                           _KERNEL_SUBSYSTEM=
_CAP_EFFECTIVE=                     KERNEL_USEC=
_CMDLINE=                           LEADER=
CODE_FILE=                          LIMIT=
CODE_FUNC=                          LIMIT_PRETTY=
CODE_LINE=                          _LINE_BREAK=
_COMM=                              _MACHINE_ID=
CONFIG_FILE=                        MAX_USE=
CONFIG_LINE=                        MAX_USE_PRETTY=
COREDUMP_CGROUP=                    MEMORY_PEAK=
COREDUMP_CMDLINE=                   MEMORY_SWAP_PEAK=
COREDUMP_COMM=                      MESSAGE=
COREDUMP_CWD=                       MESSAGE_ID=
COREDUMP_ENVIRON=                   NM_DEVICE=
COREDUMP_EXE=                       NM_LOG_DOMAINS=
COREDUMP_FILENAME=                  NM_LOG_LEVEL=
COREDUMP_GID=                       _PID=
COREDUMP_HOSTNAME=                  PODMAN_EVENT=
COREDUMP_OPEN_FDS=                  PODMAN_TIME=
COREDUMP_OWNER_UID=                 PODMAN_TYPE=
COREDUMP_PACKAGE_JSON=              PRIORITY=
COREDUMP_PID=                       REALMD_OPERATION=
COREDUMP_PROC_AUXV=                 _RUNTIME_SCOPE=
```

Последние строки журнала

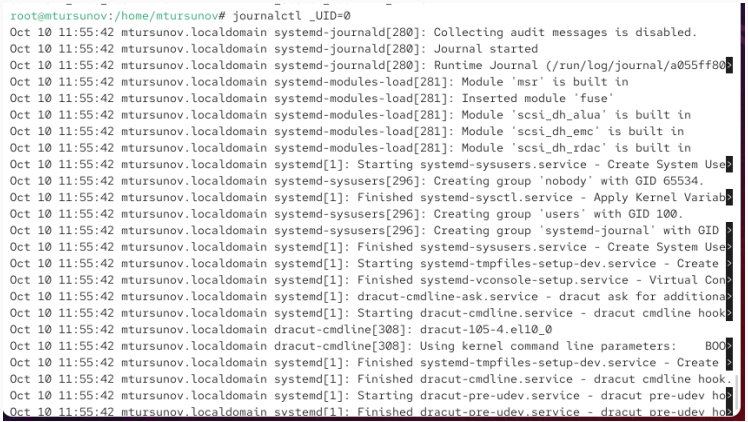

Рис. 14: Отображение последних 20 строк журнала

Сообщения об ошибках

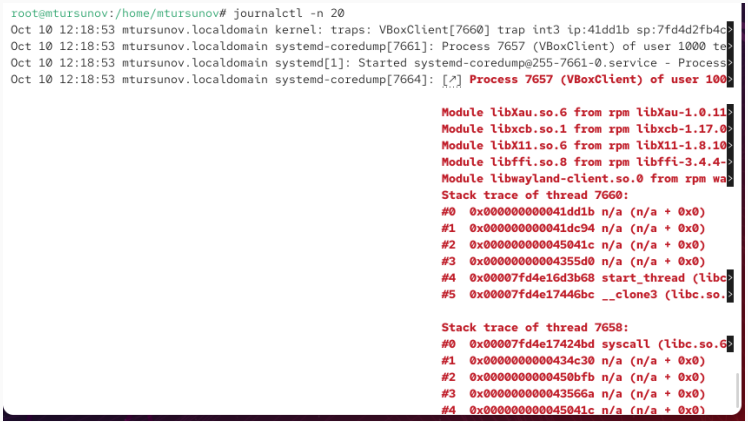

Рис. 15: Просмотр сообщений об ошибках

Просмотр по времени

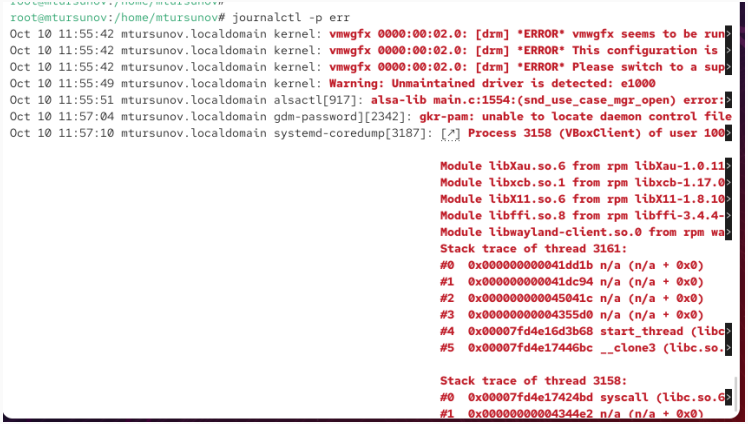

Рис. 16: Просмотр журнала с фильтром по времени

Ошибки со вчерашнего дня

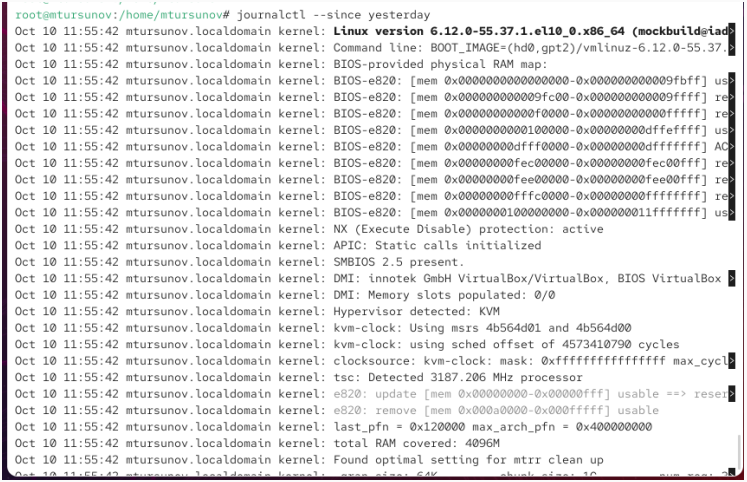

Рис. 17: Просмотр ошибок со вчерашнего дня

Подробный вывод (verbose)

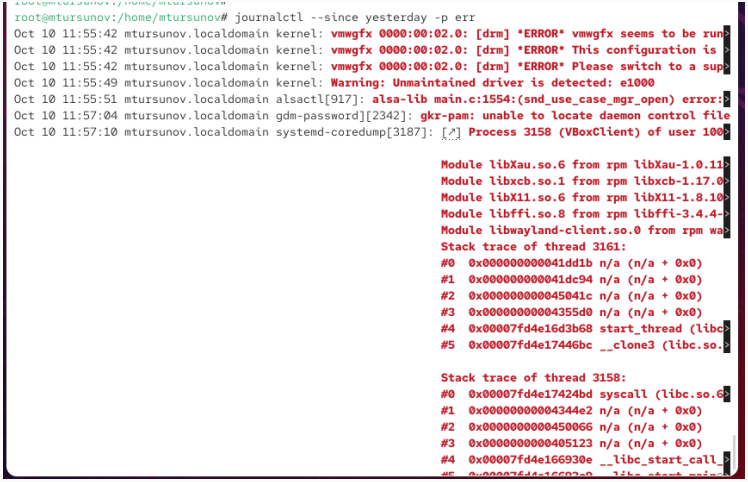

Рис. 18: Режим подробного вывода verbose

Рис. 19: Просмотр событий службы SSHD

Постоянный журнал journald

Создание постоянного журнала

```
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# mkdir -p /var/log/journal
root@mtursunov:/home/mtursunov# chown root:systemd-journal /var/log/journal/
root@mtursunov:/home/mtursunov# chmod 2755 /var/log/journal/
root@mtursunov:/home/mtursunov# killall -USR1 systemd-journald
root@mtursunov:/home/mtursunov# journalctl -b
Oct 10 11:55:42 mtursunov.localdomain kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad>
Oct 10 11:55:42 mtursunov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-provided physical RAM map:
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] AC>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: NX (Execute Disable) protection: active
Oct 10 11:55:42 mtursunov.localdomain kernel: APIC: Static calls initialized
Oct 10 11:55:42 mtursunov.localdomain kernel: SMBIOS 2.5 present.
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox >
Oct 10 11:55:42 mtursunov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 10 11:55:42 mtursunov.localdomain kernel: Hypervisor detected: KVM
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

Рис. 20: Настройка постоянного журнала journald

Итоги работы

Вывод

В ходе работы были изучены механизмы регистрации и хранения системных событий в Linux. Были освоены приёмы настройки **rsyslog**, перенаправления логов веб-службы Apache и фильтрации сообщений по уровням приоритета.
Также исследованы возможности **journalctl** по просмотру, фильтрации и анализу событий, а система журналирования **journald** была настроена на постоянное хранение логов.