

Отчёт по лабораторной работе №7

Управление журналами событий в системе

Турсунов Мухамметназар

Содержание

1	Цель работы	5
2	Выполнение	6
2.1	Мониторинг журнала системных событий в реальном времени . .	6
2.2	Изменение правил rsyslog.conf	9
2.3	Использование journalctl	12
2.4	Постоянный журнал journald	20
3	Контрольные вопросы	22
4	Заключение	24

Список иллюстраций

2.1	Мониторинг системных событий через <code>tail -f /var/log/messages</code> . . .	7
2.2	Ошибка авторизации при попытке <code>su -</code>	8
2.3	Результат работы команды <code>logger hello</code>	8
2.4	Вывод файла <code>/var/log/secure</code>	9
2.5	Мониторинг журнала ошибок Apache	10
2.6	Изменение конфигурации <code>httpd.conf</code>	10
2.7	Создание правила для перенаправления логов Apache	11
2.8	Перезапуск служб <code>rsyslog</code> и <code>httpd</code>	11
2.9	Результат регистрации отладочного сообщения через <code>logger</code>	12
2.10	Просмотр системного журнала с момента загрузки	13
2.11	Просмотр журнала в реальном времени	14
2.12	Отображение параметров фильтрации <code>journalctl</code>	15
2.13	Вывод записей для <code>UID 0</code>	16
2.14	Отображение последних 20 строк журнала	17
2.15	Просмотр сообщений об ошибках	17
2.16	Просмотр журнала с фильтром по времени	18
2.17	Просмотр ошибок со вчерашнего дня	18
2.18	Режим подробного вывода <code>verbose</code>	19
2.19	Просмотр событий службы <code>SSHD</code>	20
2.20	Настройка постоянного журнала <code>journald</code>	21

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение

2.1 Мониторинг журнала системных событий в реальном времени

1. В трёх вкладках терминала были получены права суперпользователя с помощью команды **su -**.

Это позволило выполнять административные действия и получать доступ к системным логам.

2. Во второй вкладке запущен мониторинг системных событий в реальном времени с помощью команды **tail -f /var/log/messages**.

Команда отображает новые строки, добавляемые в журнал сообщений, что удобно для наблюдения за активностью системы в реальном времени.

```

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 abnormally with signal 5/TRAP, processing...
Oct 10 11:59:18 mtursunov systemd[1]: Started systemd-coredump@25-3862-0.service - Process Core Dump (PID 3862/UID 0).
Oct 10 11:59:18 mtursunov systemd-coredump[3863]: Process 3858 (VBoxClient) of user 1000 dumped core.#012#0Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012#1Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012#2Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012#3Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012#4Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012#5Stack trace of thread 3861:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1056bc)#012#6Stack trace of thread 3859:#012#0 0x00007fd4e17424bd syscall (libc.so.6 + 0x1034bd)#012#1 0x0000000000434c30 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 0x00007fd4e16d3b68 start_thread (libc.so.6 + 0x94b68)#012#7 0x00007fd4e17446bc __clone3 (libc.so.6 + 0x1056bc)#012#8Stack 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 0x00007fd4e16693c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012#7ELF 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 abnormally with signal 5/TRAP, processing...
Oct 10 11:59:23 mtursunov systemd[1]: Started systemd-coredump@26-3879-0.service - Process Core Dump (PID 3879/UID 0).

```

Рис. 2.1: Мониторинг системных событий через tail -f /var/log/messages

На экране фиксируются сообщения, связанные с процессами **VBoxClient**, сопровождающиеся ошибками и дампами памяти (core dump).

Это свидетельствует о сбоях в работе клиентских процессов VirtualBox.

3. В третьей вкладке произведён выход из режима суперпользователя с помощью **Ctrl + D**,

затем выполнена попытка повторного входа с использованием команды **su -**, при этом был введён неправильный пароль.

Во второй вкладке с активным мониторингом отобразилось сообщение об ошибке авторизации:

FAILED SU (to root) mtursunov on pts/2.

```

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:41ddb1b sp:7fd4d2fb4cd0 error:0 in
VBoxClient[1ddb1b,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. 2.2: Ошибка авторизации при попытке su -

4. Далее в пользовательской оболочке выполнена команда **logger hello**.

Она предназначена для записи произвольных сообщений в системный жур-
нал.

После выполнения во второй вкладке с мониторингом появилось сообще-
ние с текстом **hello**,

подтверждающее успешную запись в файл **/var/log/messages**.

```

libc.so.6 + 0x10340d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x00000000004050bb 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 0x00007fd4e16693c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x000000
00004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct 10 12:02:02 mtursunov systemd[1]: systemd-coredump@57-4230-0.service: Deactivated successfully.
Oct 10 12:02:03 mtursunov mtursunov[4236]: hello
Oct 10 12:02:07 mtursunov kernel: traps: VBoxClient[4241] trap int3 ip:41ddb1b sp:7fd4d2fb4cd0 error:0 in
VBoxClient[1ddb1b,400000+bb000]
Oct 10 12:02:07 mtursunov systemd-coredump[4242]: Process 4238 (VBoxClient) of user 1000 terminated abno
rmally with signal 5/TRAP, processing...
Oct 10 12:02:07 mtursunov systemd[1]: Started systemd-coredump@58-4242-0.service - Process Core Dump (PI
D 4242/UID 0).

```

Рис. 2.3: Результат работы команды logger hello

5. После завершения наблюдения за системными событиями процесс мони- торинга был остановлен сочетанием **Ctrl + C**.

Затем выполнен просмотр последних двадцати строк журнала безопасно-
сти с помощью команды **tail -n 20 /var/log/secure**.

В выводе зафиксированы события входа в систему, в том числе успешные и
неудачные попытки авторизации через **su**, **sshd** и **gdm**.

Также видны записи о неудачных попытках ввода пароля при повышении
привилегий пользователя **mtursunov**.


```

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 mtursunov(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 mtursunov(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(uid=42) by gdm(uid=0)
Oct 10 11:55:56 mtursunov gdm-launch-environment[1251]: pam_unix(gdm-launch-environment:session): session 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 mtursunov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password[2342]: pam_unix(gdm-password:session): session opened for user mtursunov(uid=1000) by mtursunov(uid=0)
Oct 10 11:57:04 mtursunov gdm-password[2342]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 11:57:09 mtursunov gdm-launch-environment[1251]: pam_unix(gdm-launch-environment:session): session 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 mtursunov(uid=1000)
Oct 10 11:58:59 mtursunov su[3729]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 11:59:03 mtursunov su[3793]: pam_unix(su:session): session opened for user root(uid=0) by mtursunov(uid=1000)
Oct 10 12:00:23 mtursunov su[3793]: pam_unix(su:session): session closed for user root
Oct 10 12:00:25 mtursunov su[3793]: password check failed for user (root)

```

Рис. 2.4: Вывод файла /var/log/secure

2.2 Изменение правил rsyslog.conf

1. В первой вкладке терминала был установлен и запущен веб-сервер Apache. Для этого выполнены команды установки и запуска службы **httpd**, а также её автоматического запуска при загрузке системы.
2. После установки веб-службы выполнено наблюдение за журналом ошибок Apache:

tail -f /var/log/httpd/error_log.

В выводе фиксировались стандартные служебные сообщения о запуске и настройке Apache, включая уведомления SELinux и конфигурацию модулей.

```
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# tail -f /var/log/httpd/error_log
[Fri Oct 10 12:06:42.261083 2025] [suexec:notice] [pid 5065:tid 5065] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 10 12:06:42.315202 2025] [lbmethod_heartbeat:notice] [pid 5065:tid 5065] AH02282: No slotmem from mod_heartbeat
[Fri Oct 10 12:06:42.316145 2025] [systemd:notice] [pid 5065:tid 5065] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 10 12:06:42.317775 2025] [mpm_event:notice] [pid 5065:tid 5065] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 10 12:06:42.317794 2025] [core:notice] [pid 5065:tid 5065] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.5: Мониторинг журнала ошибок Apache

3. В конфигурационном файле **/etc/httpd/conf/httpd.conf** была добавлена строка:

ErrorLog syslog:local1.

Эта запись перенаправляет сообщения об ошибках веб-сервера в системный журнал, используя объект **local1**, предназначенный для пользовательских приложений.

```
#
# 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
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify	^_ Go To Line

Рис. 2.6: Изменение конфигурации httpd.conf

4. В каталоге **/etc/rsyslog.d** был создан новый файл **httpd.conf**, в который до-

бавлена строка:

local1.* -/var/log/httpd-error.log.

Таким образом, все сообщения, поступающие в объект **local1**, будут записываться в отдельный лог-файл **/var/log/httpd-error.log**.



Рис. 2.7: Создание правила для перенаправления логов Apache

- После изменения конфигураций службы журналирования и веб-сервера выполнена их перезагрузка:

systemctl restart rsyslog.service и **systemctl restart httpd**.

Это позволило применить новые параметры без перезагрузки системы.



Рис. 2.8: Перезапуск служб rsyslog и httpd

- Для регистрации отладочных сообщений был создан дополнительный файл **debug.conf** в каталоге **/etc/rsyslog.d**.

В него добавлена строка ***.debug /var/log/messages-debug**, направляющая

все сообщения с уровнем debug в отдельный журнал **/var/log/messages-debug**.

- После перезапуска службы rsyslog был запущен мониторинг этого файла командой **tail -f /var/log/messages-debug**.

Затем в другой вкладке терминала была выполнена команда **logger -p daemon.debug "Daemon Debug Message"**,

которая отправила тестовое отладочное сообщение в системный журнал.

В окне мониторинга отображается переданное сообщение, что подтверждает корректную настройку фильтрации и маршрутизации логов.

```
VBoxClient[1dd1b,400000+bb000]
Oct 10 12:13:16 mtursunov systemd-coredump[6880]: Process 6876 (VBoxClient) of user 1000 terminated abnor-
mally with signal 5/TRAP, processing...
Oct 10 12:13:16 mtursunov systemd[1]: Started systemd-coredump@189-6880-0.service - Process Core Dump (P
ID 6880/UID 0).
Oct 10 12:13:16 mtursunov root[6883]: Daemon Debug Message
Oct 10 12:13:16 mtursunov systemd-coredump[6881]: Process 6876 (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 6879:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a
+ 0x0)#012#2 0x00000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x0000
7f44-1623f69 start thread (libc.so.6 + 0x04560) #012#5 0x00007f44-17445b _dl_start (libc.so.6 + 0x1055b)
```

Рис. 2.9: Результат регистрации отладочного сообщения через logger

2.3 Использование journalctl

- Во второй вкладке терминала был запущен просмотр системного журнала с момента последней загрузки системы с помощью команды **journalctl**.

На экране отобразились записи ядра Linux, включая сведения о версии, параметрах загрузки, структуре памяти и активности BIOS.

Управление просмотром осуществлялось клавишами **Enter** (построчно), **пробел** (постранично) и **q** (выход).

```
root@mtursunov: /home/mtursunov# journalctl
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-6.12.0-55.37.1>
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 0x0000000001000000-0x000000000dffff] us>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dfffffff] AC>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] re>
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] 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
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: using sched offset of 4573410790 cycles
Oct 10 11:55:42 mtursunov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycl>
Oct 10 11:55:42 mtursunov.localdomain kernel: tsc: Detected 3187.206 MHz processor
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reser>
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 10 11:55:42 mtursunov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 11:55:42 mtursunov.localdomain kernel: total RAM covered: 4096M
Oct 10 11:55:42 mtursunov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 10 11:55:42 mtursunov.localdomain kernel: page size: 64K chunk size: 10M num pages: 256
```

Рис. 2.10: Просмотр системного журнала с момента загрузки

2. Для получения журналов без использования пейджера применена команда **journalctl –no-pager**, что позволило вывести все записи сразу, без постраничной навигации.
3. Команда **journalctl -f** запустила отображение событий в реальном времени, аналогично действию утилиты **tail -f** для обычных логов. После появления новых сообщений (например, об ошибках VBoxClient) информация сразу же выводилась в консоль. Прекращение режима выполнено с помощью **Ctrl + C**.

```
Oct 10 12:16:20 mtursunov.localdomain kernel: traps: VBoxClient[7331] trap int3 ip:41dd1b sp:7fd4d2fb4cd
0 error:0 in VBoxClient[1dd1b,400000+bb000]
Oct 10 12:16:20 mtursunov.localdomain systemd-coredump[7332]: Process 7328 (VBoxClient) of user 1000 ter
minated abnormally with signal 5/TRAP, processing...
Oct 10 12:16:20 mtursunov.localdomain systemd[1]: Started systemd-coredump@225-7332-0.service - Process
Core Dump (PID 7332/UID 0).
Oct 10 12:16:20 mtursunov.localdomain systemd-coredump[7333]: [^] Process 7328 (VBoxClient) of user 1000
dumped core.

8.e110.x86_64 Module libXau.so.6 from rpm libXau-1.0.11-
3.e110.x86_64 Module libxcb.so.1 from rpm libxcb-1.17.0-
1.e110.x86_64 Module libX11.so.6 from rpm libX11-1.8.10-
.e110.x86_64 Module libffi.so.8 from rpm libffi-3.4.4-9
land-1.23.0-2.e110.x86_64 Module libwayland-client.so.0 from rpm way

Stack trace of thread 7331:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007fd4e16d3b68 start_thread (libc.
so.6 + 0x94b68)
#5 0x00007fd4e17446bc __clone3 (libc.so.6
+ 0x1056bc)

Stack trace of thread 7330:
#0 0x00007fd4e17424bd syscall (libc.so.6
```

Рис. 2.11: Просмотр журнала в реальном времени

4. При двойном нажатии клавиши **Tab** после ввода команды **journalctl** был выведен список доступных параметров для фильтрации.

Это позволило увидеть все возможные поля фильтрации, такие как **_UID**, **_SYSTEMD_UNIT**, **_EXE**, **_PID** и другие.

```
Oct 10 12:17:26 mtursunov.localdomain systemd-coredump[7471]: Process 7466 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct 10 12:17:26 mtursunov.localdomain systemd[1]: Started systemd-coredump@238-7470-0.service - Process Core Dump (PID 7470/UID 0).
Oct 10 12:17:26 mtursunov.localdomain systemd-coredump[7471]: [...] Process 7466 (VBoxClient) of user 1000 dumped core.

                                     Module libXau.so.6 from rpm libXau-1.0.11-
8.el10.x86_64
                                     Module libxcb.so.1 from rpm libxcb-1.17.0-
3.el10.x86_64
                                     Module libX11.so.6 from rpm libX11-1.8.10-
1.el10.x86_64
                                     Module libffi.so.8 from rpm libffi-3.4.4-9
.el10.x86_64
                                     Module libwayland-client.so.0 from rpm way
land-1.23.0-2.el10.x86_64

                                     Stack trace of thread 7469:
                                     #0  0x00000000041dd1b n/a (n/a + 0x0)
                                     #1  0x00000000041dc94 n/a (n/a + 0x0)
                                     #2  0x00000000045041c n/a (n/a + 0x0)
                                     #3  0x0000000004355d0 n/a (n/a + 0x0)
                                     #4  0x00007fd4e16d3b68 start_thread (libc.
so.6 + 0x94b68)
                                     #5  0x00007fd4e17446bc __clone3 (libc.so.6
+ 0x1056bc)

                                     Stack trace of thread 7466:
                                     #0  0x00007fd4e17424bd syscall (libc.so.6
+ 0x1034bd)
                                     #1  0x0000000004344e2 n/a (n/a + 0x0)
```

Рис. 2.12: Отображение параметров фильтрации journalctl

5. Для отображения записей, созданных пользователем с идентификатором UID 0 (root), была использована команда `**journalctl _UID=0**`.

В результате выведены системные события, инициированные пользователем root во время запуска служб и модулей.

```

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=
COREDUMP_PROC_CGROUP=   SEAT_ID=

```

Рис. 2.13: Вывод записей для UID 0

6. Команда **journalctl -n 20** отобразила последние двадцать строк журнала. В них зафиксированы сообщения ядра и службы systemd, включая сведения о процессах и ошибках приложений.


```

root@mtursunov:/home/mtursunov# journalctl _UID=0
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Collecting audit messages is disabled.
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Journal started
Oct 10 11:55:42 mtursunov.localdomain systemd-journald[280]: Runtime Journal (/run/log/journal/a055ff80)
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'msr' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Inserted module 'fuse'
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_alua' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_emc' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd-modules-load[281]: Module 'scsi_dh_rdac' is built in
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'nobody' with GID 65534.
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'users' with GID 100.
Oct 10 11:55:42 mtursunov.localdomain systemd-sysusers[296]: Creating group 'systemd-journal' with GID 100.
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create and Update
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional kernel
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook
Oct 10 11:55:42 mtursunov.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Oct 10 11:55:42 mtursunov.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOOT=
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create and Update
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook
Oct 10 11:55:42 mtursunov.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook

```

Рис. 2.14: Отображение последних 20 строк журнала

- Для вывода только сообщений с уровнем приоритета “ошибка” использовалась команда **journalctl -p err**.

На экран были выведены критические сообщения ядра и системных служб, включая ошибки видеодрайвера `vmwgfx` и библиотеки `alsa-lib`.

```

root@mtursunov:/home/mtursunov# journalctl -n 20
Oct 10 12:18:53 mtursunov.localdomain kernel: traps: VBoxClient[7660] trap int3 ip:41ddb sp:7fd4d2fb4c
Oct 10 12:18:53 mtursunov.localdomain systemd-coredump[7661]: Process 7657 (VBoxClient) of user 1000 te
Oct 10 12:18:53 mtursunov.localdomain systemd[1]: Started systemd-coredump@255-7661-0.service - Process
Oct 10 12:18:53 mtursunov.localdomain systemd-coredump[7664]: [core] Process 7657 (VBoxClient) of user 1000

Module libXau.so.6 from rpm libXau-1.0.11
Module libxcb.so.1 from rpm libxcb-1.17.0
Module libX11.so.6 from rpm libX11-1.8.10
Module libffi.so.8 from rpm libffi-3.4.4
Module libwayland-client.so.0 from rpm wayland-1.20.0
Stack trace of thread 7660:
#0  0x00000000041ddb n/a (n/a + 0x0)
#1  0x00000000041dc94 n/a (n/a + 0x0)
#2  0x00000000045041c n/a (n/a + 0x0)
#3  0x0000000004355d0 n/a (n/a + 0x0)
#4  0x00007fd4e16d3b68 start_thread (libc.so.2)
#5  0x00007fd4e17446bc __clone3 (libc.so.2)

Stack trace of thread 7658:
#0  0x00007fd4e17424bd syscall (libc.so.6)
#1  0x000000000434c30 n/a (n/a + 0x0)
#2  0x000000000450bfb n/a (n/a + 0x0)
#3  0x00000000043566a n/a (n/a + 0x0)
#4  0x00000000045041c n/a (n/a + 0x0)

```

Рис. 2.15: Просмотр сообщений об ошибках

- Для анализа событий, произошедших со вчерашнего дня, применена команда **journalctl -since yesterday**,

которая вывела все сообщения, начиная с предыдущих суток.

```
root@mtursunov:/home/mtursunov# journalctl -p err
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup
Oct 10 11:55:49 mtursunov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 10 11:55:51 mtursunov.localdomain alsactl[917]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:
Oct 10 11:57:04 mtursunov.localdomain gdm-password[2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:10 mtursunov.localdomain systemd-coredump[3187]: [Process 3158 (VBoxClient) of user 100]

Module libXau.so.6 from rpm libXau-1.0.11
Module libxcb.so.1 from rpm libxcb-1.17.0
Module libX11.so.6 from rpm libX11-1.8.10
Module libffi.so.8 from rpm libffi-3.4.4
Module libwayland-client.so.0 from rpm wa
Stack trace of thread 3161:
#0 0x00000000041dd1b n/a (n/a + 0x0)
#1 0x00000000041dc94 n/a (n/a + 0x0)
#2 0x00000000045041c n/a (n/a + 0x0)
#3 0x0000000004355d0 n/a (n/a + 0x0)
#4 0x00007fd4e16d3b68 start_thread (libc
#5 0x00007fd4e17446bc __clone3 (libc.so.
Stack trace of thread 3158:
#0 0x00007fd4e17424bd syscall (libc.so.6
#1 0x0000000004344e2 n/a (n/a + 0x0)
```

Рис. 2.16: Просмотр журнала с фильтром по времени

9. Команда **journalctl --since yesterday -p err** отобразила только сообщения об ошибках, зафиксированные со вчерашнего дня.

Среди них присутствовали системные ошибки, предупреждения драйверов и сбои процессов VBoxClient.

```
root@mtursunov:/home/mtursunov# journalctl --since yesterday
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 0x0000000000000000-0x0000000000009bfff] us
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000009bfff-0x0000000000009ffff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000009ffff-0x000000000000ffff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000ffff-0x000000000000dffff] us
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000dffff-0x000000000000ffff] AC
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000ffff-0x000000000000fec0fff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000fec0fff-0x000000000000fee0fff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000fee0fff-0x000000000000fee0fff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000fee0fff-0x000000000000ffffff] re
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x000000000000ffffff-0x00000000000011ffff] 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
Oct 10 11:55:42 mtursunov.localdomain kernel: kvm-clock: using sched offset of 4573410790 cycles
Oct 10 11:55:42 mtursunov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycl
Oct 10 11:55:42 mtursunov.localdomain kernel: tsc: Detected 3187.206 MHz processor
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserv
Oct 10 11:55:42 mtursunov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Oct 10 11:55:42 mtursunov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 11:55:42 mtursunov.localdomain kernel: total RAM covered: 4096M
Oct 10 11:55:42 mtursunov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 10 11:55:42 mtursunov.localdomain kernel: page size: 64K chunk size: 1G sum pages: 25
```

Рис. 2.17: Просмотр ошибок со вчерашнего дня

10. Для получения расширенной информации о каждом событии была использована команда **journalctl -o verbose**.

В этом режиме журнал отображает полные метаданные записей: дату, источник, уровень приоритета, идентификатор процесса, контекст и сообщение.

```
root@mtursunov:/home/mtursunov# journalctl --since yesterday -p err
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run>
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is >
Oct 10 11:55:42 mtursunov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup>
Oct 10 11:55:49 mtursunov.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 10 11:55:51 mtursunov.localdomain alsactl[917]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:>
Oct 10 11:57:04 mtursunov.localdomain gdm-password[2342]: gkr-pam: unable to locate daemon control file
Oct 10 11:57:10 mtursunov.localdomain systemd-coredump[3187]: [..] Process 3158 (VBoxClient) of user 100>

Module libXau.so.6 from rpm libXau-1.0.11>
Module libxcb.so.1 from rpm libxcb-1.17.0>
Module libX11.so.6 from rpm libX11-1.8.10>
Module libffi.so.8 from rpm libffi-3.4.4->
Module libwayland-client.so.0 from rpm wa>
Stack trace of thread 3161:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007fd4e16d3b68 start_thread (libc>
#5 0x00007fd4e17446bc __clone3 (libc.so.>

Stack trace of thread 3158:
#0 0x00007fd4e17424bd syscall (libc.so.6>
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007fd4e166930e __libc_start_call>
#5 0x00007fd4e16602c0 libc_start_main
```

Рис. 2.18: Режим подробного вывода verbose

11. Для просмотра дополнительной информации о модуле SSHD использовалась команда ****journalctl _SYSTEMD_UNIT=sshd.service****.

В результате были показаны сообщения, связанные с запуском службы sshd, включая прослушивание портов и предупреждения окружения.

```
_RUNTIME_SCOPE=initrd
Fri 2025-10-10 11:55:42.723607 MSK [s=18507d14dc3449e39968f5c00a0bf2de;i=2;b=e5d51ff71c3049c58f1cdc5764b
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=e5d51ff71c3049c58f1cdc5764919953
_MACHINE_ID=a055ff809d5a4a55b89dacba4a93a2a5
_HOSTNAME=mtursunov.localdomain
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/mapper/r
Fri 2025-10-10 11:55:42.723613 MSK [s=18507d14dc3449e39968f5c00a0bf2de;i=3;b=e5d51ff71c3049c58f1cdc5764b
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
root@mtursunov:/home/mtursunov# journalctl _SYSTEMD_UNIT=sshd.service
Oct 10 11:55:54 mtursunov.localdomain (sshd)[1207]: sshd.service: Referenced but unset environment vari
Oct 10 11:55:54 mtursunov.localdomain sshd[1207]: Server listening on 0.0.0.0 port 22.
Oct 10 11:55:54 mtursunov.localdomain sshd[1207]: Server listening on :: port 22.
root@mtursunov:/home/mtursunov#
```

Рис. 2.19: Просмотр событий службы SSHD

2.4 Постоянный журнал journald

1. Для начала был получен доступ с правами суперпользователя.
Это необходимо, так как изменение параметров системного журнала требует административных прав.
2. Создан каталог **/var/log/journal**, предназначенный для хранения постоянных записей журнала.
Каталог создаётся с помощью команды **mkdir -p /var/log/journal**, которая создаёт директорию, если она отсутствует, включая промежуточные пути.
3. Для корректной работы службы **systemd-journald** настроены права доступа к каталогу:
 - командой **chown root:systemd-journal /var/log/journal** назначена владельцем группа *systemd-journal*,
 - командой **chmod 2755 /var/log/journal** заданы права доступа, позволяющие записи и чтение журналов службой journald.

4. Чтобы применить изменения без перезагрузки системы, была выполнена команда

killall -USR1 systemd-journald, которая посылает процессу **journald** сигнал на перезапуск с перечитыванием конфигурации.

5. После этого журнал **systemd-journald** стал постоянным — все новые сообщения теперь сохраняются в каталоге **/var/log/journal** и не теряются после перезагрузки.

Проверка осуществлена командой **journalctl -b**, которая выводит сообщения с момента последней загрузки системы.

```
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 755 /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-6.12.0-55.37.2  
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] res  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] res  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] us  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff000-0x00000000dfffffff] AC  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] res  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] res  
Oct 10 11:55:42 mtursunov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] res  
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. 2.20: Настройка постоянного журнала **journald**

3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

`/etc/rsyslog.conf`

а также дополнительные файлы конфигурации, расположенные в каталоге

`/etc/rsyslog.d/`

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 ротация файлов журналов выполняется **еженедельно (weekly)** — один раз в неделю, согласно настройкам файла `/etc/logrotate.conf`.

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?

`journalctl -f`

или для системных логов, управляемых rsyslog:

`tail -f /var/log/messages`

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
```

- 8. Какая процедура позволяет сделать журнал journald постоянным?**

1. Создать каталог **/var/log/journal**

2. Назначить права и владельца:

```
chown root:systemd-journal /var/log/journal
```

```
chmod 2755 /var/log/journal
```

3. Отправить сигнал службе journald для применения изменений:

```
killall -USR1 systemd-journald
```

После этого журнал journald становится постоянным и сохраняется после перезагрузки.

4 Заключение

В ходе выполнения работы были изучены принципы и механизмы регистрации системных событий в Linux с использованием служб **rsyslog** и **systemd-journald**. Были выполнены практические действия по настройке журналов, фильтрации сообщений, перенаправлению логов веб-службы Apache, а также организации отдельного файла для отладочной информации.

Освоены приёмы работы с утилитой **journalctl**, включая поиск, фильтрацию, просмотр сообщений за определённые периоды и в режиме реального времени.