Отчёт по лабораторной работе №7

Управление журналами событий в системе

Ришард Когенгар

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Ход выполнения

3 Ход выполнения

3.1 Мониторинг журнала системных событий в реальном времени

1. Для выполнения задания были открыты три вкладки терминала.
   В каждой вкладке получены полномочия администратора с помощью команды su -, что позволило выполнять действия, требующие прав суперпользователя.

2. Во второй вкладке терминала был запущен мониторинг системных сообщений в реальном времени с использованием файла /var/log/messages.
   Мониторинг позволил наблюдать появление новых системных событий непосредственно в момент их возникновения.

3. В третьей вкладке терминала выполнен выход из учётной записи администратора (Ctrl + d), после чего предпринята попытка повторного получения прав суперпользователя с вводом неверного пароля.
   В результате в журнале событий отобразилось сообщение FAILED SU (to root), свидетельствующее об ошибке аутентификации.
   Данное событие было автоматически зафиксировано в системном журнале.

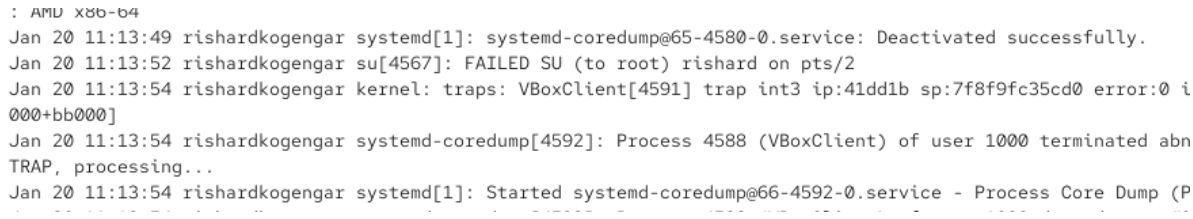

Рис. 3.1: Ошибка аутентификации su

4. В третьей вкладке терминала из пользовательской оболочки выполнена отправка сообщения в системный журнал с помощью утилиты logger.
   Во второй вкладке терминала с активным мониторингом появилось соответствующее сообщение, подтверждающее корректную работу механизма регистрации пользовательских событий.

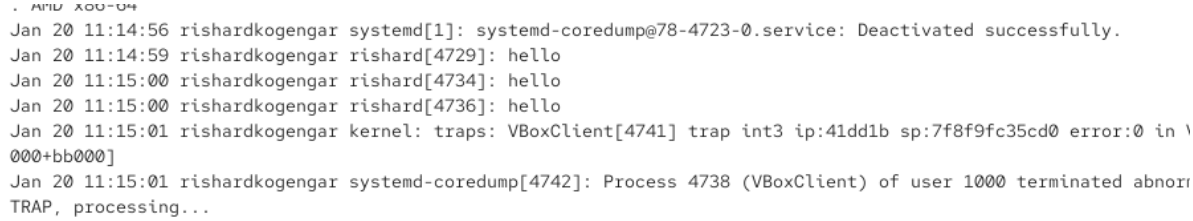

Рис. 3.2: Сообщение, отправленное командой logger

5. Мониторинг файла /var/log/messages был остановлен.
   Далее выполнен просмотр последних 20 строк журнала безопасности /var/log/secure.
   В журнале присутствуют записи, зафиксированные ранее во время неудачной попытки получения прав администратора.

```
root@rishardkogengar:/home/rishard# tail -n 20 /var/log/secure
Jan 19 14:37:37 rishardkogengar su[5408]: pam_unix(su:session): session closed for user root
Jan 19 14:38:23 rishardkogengar su[6734]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 19 14:44:04 rishardkogengar su[6734]: pam_unix(su:session): session closed for user root
Jan 20 11:07:29 rishardkogengar sshd[1432]: Server listening on 0.0.0.0 port 22.
Jan 20 11:07:29 rishardkogengar sshd[1432]: Server listening on :: port 22.
Jan 20 11:07:29 rishardkogengar (systemd)[1484]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Jan 20 11:07:29 rishardkogengar gdm-launch-environment][1476]: pam_unix(gdm-launch-environment:session): session opened for user gd
m(uid=42) by (uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: unable to locate daemon control file
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: stashed password to try later in open session
Jan 20 11:08:11 rishardkogengar (systemd)[2589]: pam_unix(systemd-user:session): session opened for user rishard(uid=1000) by risha
rd(uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: pam_unix(gdm-password:session): session opened for user rishard(uid=1000) by r
ishard(uid=0)
Jan 20 11:08:11 rishardkogengar gdm-password][2578]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Jan 20 11:08:15 rishardkogengar gdm-launch-environment][1476]: pam_unix(gdm-launch-environment:session): session closed for user gd
m
Jan 20 11:12:54 rishardkogengar (systemd)[4270]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Jan 20 11:12:55 rishardkogengar su[4245]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:00 rishardkogengar su[4360]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:06 rishardkogengar su[4434]: pam_unix(su:session): session opened for user root(uid=0) by rishard(uid=1000)
Jan 20 11:13:47 rishardkogengar su[4434]: pam_unix(su:session): session closed for user root
Jan 20 11:13:50 rishardkogengar unix_chkpwd[4586]: password check failed for user (root)
Jan 20 11:13:50 rishardkogengar su[4567]: pam_unix(su:auth): authentication failure; logname=rishard uid=1000 euid=0 tty=/dev/pts/2
 ruser=rishard rhost=  user=root
root@rishardkogengar:/home/rishard#
```

Рис. 3.3: Просмотр журнала безопасности

3.2 Изменение правил регистрации rsyslog и настройка журналирования веб-службы

6. В первой вкладке терминала выполнена установка веб-сервера Apache. После завершения установки служба была запущена и добавлена в автозагрузку, что обеспечивает её автоматический старт при загрузке системы.

```
Installed:
  apr-1.7.5-2.el10.x86_64                    apr-util-1.6.3-21.el10.x86_64            apr-util-lmdb-1.6.3-21.el10.x86_64
  apr-util-openssl-1.6.3-21.el10.x86_64      httpd-2.4.63-4.el10_1.3.x86_64           httpd-core-2.4.63-4.el10_1.3.x86_64
  httpd-filesystem-2.4.63-4.el10_1.3.noarch  httpd-tools-2.4.63-4.el10_1.3.x86_64     mod_http2-2.0.29-3.el10.x86_64
  mod_lua-2.4.63-4.el10_1.3.x86_64           rocky-logos-httpd-100.4-7.el10.noarch

Complete!
root@rishardkogengar:/home/rishard# systemctl start httpd
root@rishardkogengar:/home/rishard# systemctl enable httd
Failed to enable unit: Unit httd.service does not exist
root@rishardkogengar:/home/rishard# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@rishardkogengar:/home/rishard#
```

Рис. 3.4: Установка и запуск Apache

7. Во второй вкладке терминала выполнен просмотр журнала ошибок веб-службы, расположенного в каталоге /var/log/httpd.

В журнале отображаются сообщения о запуске службы, загрузке модулей и текущем состоянии веб-сервера.

```
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# tail -f /var/log/httpd/error_log
[Tue Jan 20 11:17:42.199161 2026] [suexec:notice] [pid 5309:tid 5309] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Jan 20 11:17:42.230172 2026] [lbmethod_heartbeat:notice] [pid 5309:tid 5309] AH02282: No slotmem from mod_heartmonitor
[Tue Jan 20 11:17:42.230682 2026] [systemd:notice] [pid 5309:tid 5309] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Tue Jan 20 11:17:42.232095 2026] [mpm_event:notice] [pid 5309:tid 5309] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Tue Jan 20 11:17:42.232103 2026] [core:notice] [pid 5309:tid 5309] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
root@rishardkogengar:/home/rishard#
```

Рис. 3.5: Журнал ошибок Apache

8. В третьей вкладке терминала выполнено редактирование файла конфигурации веб-сервера /etc/httpd/conf/httpd.conf.
   В конец файла добавлена строка, перенаправляющая сообщения об ошибках веб-службы в системный журнал syslog с использованием объекта local1.

```
# 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
```

Рис. 3.6: Изменение файла httpd.conf

9. В каталоге /etc/rsyslog.d создан файл httpd.conf, в котором задано правило регистрации всех сообщений объекта local1 в отдельный лог-файл /var/log/httpd-error.log.
   Это позволяет централизованно хранить сообщения об ошибках веб-службы.

Рис. 3.7: Создание правила rsyslog для Apache

10. После внесения изменений выполнена перезагрузка службы rsyslog и веб-сервера Apache.
    С этого момента все сообщения об ошибках веб-службы записываются в файл /var/log/httpd-error.log.

3.3 Настройка регистрации отладочных сообщений

11. В каталоге /etc/rsyslog.d создан файл debug.conf, содержащий правило регистрации всех отладочных сообщений в отдельный файл /var/log/messages-debug.
    Это позволяет изолировать отладочную информацию от основного системного журнала.

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

Рис. 3.8: Файл debug.conf

12. После изменения конфигурации выполнена перезагрузка службы rsyslog для применения новых правил.

13. Во второй вкладке терминала запущен мониторинг файла /var/log/messages-debug, что позволило наблюдать поступление отладочных сообщений в реальном времени.

14. В третьей вкладке терминала выполнена отправка отладочного сообщения уровня daemon.debug.
    Сообщение успешно отобразилось в окне мониторинга, что подтверждает корректность настройки маршрутизации событий и работы rsyslog.

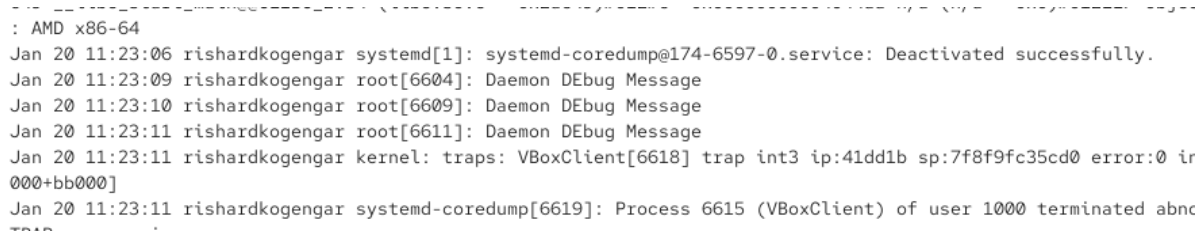

Рис. 3.9: Отладочное сообщение в messages-debug

3.4 Использование journalctl

1. Во второй вкладке терминала выполнен просмотр журнала событий с момента последнего запуска системы.
   Отображены сообщения ядра Linux, сведения о загрузке системы, инициализации оборудования, обнаружении гипервизора и настройке подсистем памяти.
   Для навигации по журналу использовались стандартные средства постраничного и построчного просмотра.

Рис. 3.10: Просмотр журнала systemd с момента загрузки системы

2. Выполнен просмотр содержимого журнала без использования пейджера. В результате весь журнал был выведен непосредственно в терминал без возможности прокрутки, что удобно при перенаправлении вывода или быстром анализе.

Рис. 3.11: Просмотр журнала без пейджера

3. Активирован режим просмотра журнала в реальном времени.

   В этом режиме в терминале отображались новые сообщения systemd по мере их появления.

   Просмотр был остановлен вручную после завершения наблюдения.

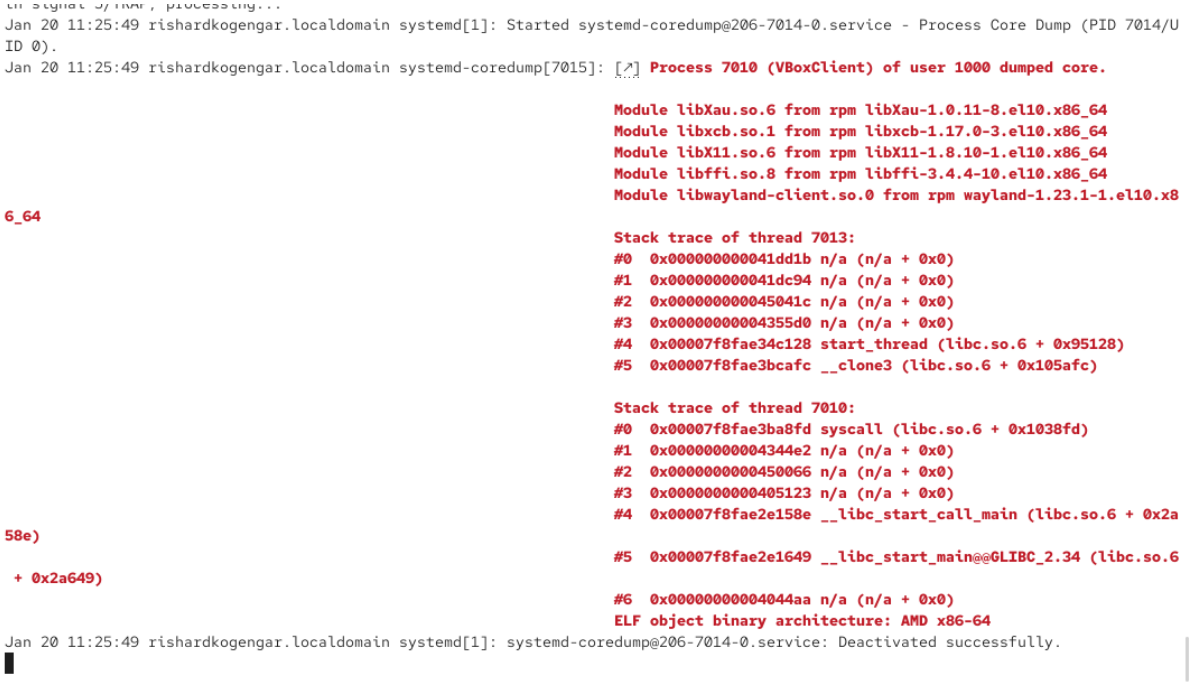

Рис. 3.12: Просмотр журнала в реальном времени

4. Для изучения возможностей фильтрации выполнен вызов journalctl с автодополнением параметров.

   В результате были отображены доступные поля журнала, такие как идентификаторы процессов, приоритеты, идентификаторы пользователей, модули и службы systemd.

```
root@rishardkogengar:/home/rishard# journalctl
Display all 128 possibilities? (y or n)
_AUDIT_LOGINUID=                      CURRENT_USE_PRETTY=                   PODMAN_TIME=
_AUDIT_SESSION=                       DBUS_BROKER_LOG_DROPPED=              PODMAN_TYPE=
AVAILABLE=                            DBUS_BROKER_METRICS_DISPATCH_AVG=     PRIORITY=
AVAILABLE_PRETTY=                     DBUS_BROKER_METRICS_DISPATCH_COUNT=   REALMD_OPERATION=
_BOOT_ID=                             DBUS_BROKER_METRICS_DISPATCH_MAX=     _RUNTIME_SCOPE=
_CAP_EFFECTIVE=                       DBUS_BROKER_METRICS_DISPATCH_MIN=     SEAT_ID=
_CMDLINE=                             DBUS_BROKER_METRICS_DISPATCH_STDDEV=  _SELINUX_CONTEXT=
CODE_FILE=                            DISK_AVAILABLE=                       SESSION_ID=
CODE_FUNC=                            DISK_AVAILABLE_PRETTY=                _SOURCE_BOOTTIME_TIMESTAMP=
CODE_LINE=                            DISK_KEEP_FREE=                       _SOURCE_MONOTONIC_TIMESTAMP=
_COMM=                                DISK_KEEP_FREE_PRETTY=                _SOURCE_REALTIME_TIMESTAMP=
CONFIG_FILE=                          ERRNO=                                SSSD_DOMAIN=
CONFIG_LINE=                          _EXE=                                 SSSD_PRG_NAME=
COREDUMP_CGROUP=                      _GID=                                 _STREAM_ID=
COREDUMP_CMDLINE=                     GLIB_DOMAIN=                          SYSLOG_FACILITY=
COREDUMP_COMM=                        GLIB_OLD_LOG_API=                     SYSLOG_IDENTIFIER=
COREDUMP_CWD=                         _HOSTNAME=                            SYSLOG_PID=
COREDUMP_ENVIRON=                     INITRD_USEC=                          SYSLOG_RAW=
COREDUMP_EXE=                         INVOCATION_ID=                        SYSLOG_TIMESTAMP=
COREDUMP_FILENAME=                    JOB_ID=                               _SYSTEMD_CGROUP=
COREDUMP_GID=                         JOB_RESULT=                           _SYSTEMD_INVOCATION_ID=
COREDUMP_HOSTNAME=                    JOB_TYPE=                             _SYSTEMD_OWNER_UID=
COREDUMP_OPEN_FDS=                    JOURNAL_NAME=                         _SYSTEMD_SESSION=
COREDUMP_OWNER_UID=                   JOURNAL_PATH=                         _SYSTEMD_SLICE=
COREDUMP_PACKAGE_JSON=                _KERNEL_DEVICE=                       _SYSTEMD_UNIT=
COREDUMP_PID=                         _KERNEL_SUBSYSTEM=                    _SYSTEMD_USER_SLICE=
COREDUMP_PROC_AUXV=                   KERNEL_USEC=                          _SYSTEMD_USER_UNIT=
COREDUMP_PROC_CGROUP=                 LEADER=                               THREAD_ID=
COREDUMP_PROC_LIMITS=                 LIMIT=                                TID=
COREDUMP_PROC_MAPS=                   LIMIT_PRETTY=                         TIMESTAMP_BOOTTIME=
COREDUMP_PROC_MOUNTINFO=              _LINE_BREAK=                          TIMESTAMP_MONOTONIC=
COREDUMP_PROC_STATUS=                 _MACHINE_ID=                          TOPIC=
COREDUMP_RLIMIT=                      MAX_USE=                              _TRANSPORT=
```

Рис. 3.13: Список доступных параметров journalctl

5. Выполнен просмотр событий, относящихся к пользователю с UID 0.

   В журнале отображены системные сообщения, связанные с запуском служб, инициализацией systemd и действиями суперпользователя.

```
root@rishardkogengar:/home/rishard# journalctl _UID=0
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Collecting audit messages is disabled.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Journal started
Jan 20 11:07:24 rishardkogengar.localdomain systemd-journald[287]: Runtime Journal (/run/log/journal/d90867af7659402b989cb6f4b1bca>
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'msr' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Inserted module 'fuse'
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_alua' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_emc' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-modules-load[288]: Module 'scsi_dh_rdac' is built in
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'nobody' with GID 65534.
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'users' with GID 100.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'systemd-journal' with GID 190.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'dbus' with GID 81.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating user 'dbus' (System Message Bus) with UID 81 and GID 8>
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating group 'tss' with GID 59.
Jan 20 11:07:24 rishardkogengar.localdomain systemd-sysusers[298]: Creating user 'tss' (Account used for TPM access) with UID 59 a>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes i>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Starting systemd-tmpfiles-setup.service - Create System Files and Director>
Jan 20 11:07:24 rishardkogengar.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
```

Рис. 3.14: Журнал событий для UID 0

6. Отображены последние 20 записей журнала.

   В выводе присутствуют сообщения об ошибках приложений, завершении процессов и создании дампов памяти.

```
root@rishardkogengar:/home/rishard# journalctl -n 20
Jan 20 11:27:00 rishardkogengar.localdomain kernel: traps: VBoxClient[7180] trap int3 ip:41dd1b sp:7f8f9fc35cd0 error:0 in VBoxCli>
Jan 20 11:27:00 rishardkogengar.localdomain systemd-coredump[7181]: Process 7177 (VBoxClient) of user 1000 terminated abnormally w>
Jan 20 11:27:00 rishardkogengar.localdomain systemd[1]: Started systemd-coredump@220-7181-0.service - Process Core Dump (PID 7181/>
Jan 20 11:27:00 rishardkogengar.localdomain systemd-coredump[7182]: [↗] Process 7177 (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-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x>
                                                                    Stack trace of thread 7180:
                                                                    #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  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #5  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

                                                                    Stack trace of thread 7178:
                                                                    #0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
                                                                    #1  0x0000000000434c30 n/a (n/a + 0x0)
                                                                    #2  0x0000000000450bfb n/a (n/a + 0x0)
                                                                    #3  0x000000000043566a n/a (n/a + 0x0)
                                                                    #4  0x000000000045041c n/a (n/a + 0x0)
                                                                    #5  0x00000000004355d0 n/a (n/a + 0x0)
                                                                    #6  0x00007f8fae34c128 start_thread (libc.so.6 + 0x95128)
                                                                    #7  0x00007f8fae3bcafc __clone3 (libc.so.6 + 0x105afc)

                                                                    Stack trace of thread 7179:
                                                                    #0  0x00007f8fae3ba8fd syscall (libc.so.6 + 0x1038fd)
```

Рис. 3.15: Последние 20 строк журнала systemd

7. Выполнена фильтрация журнала по приоритету ошибок.

   В журнале зафиксированы предупреждения ядра, ошибки графического

драйвера, сообщения udev и события аварийного завершения процессов VBoxClient.

Рис. 3.16: Сообщения журнала с приоритетом error

8. Выполнен просмотр всех сообщений журнала, зафиксированных со вчерашнего дня.
   В журнале представлены события загрузки системы, инициализации оборудования и работы служб.

```
root@rishardkogengar:/home/rishard# journalctl --since yesterday
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Linux version 6.12.0-124.27.1.el10_1.x86_64 (mockbuild@iad1-prod-build001.bld.>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.27.1.el10_1.x86_64 root>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-provided physical RAM map:
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jan 20 11:07:24 rishardkogengar.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Jan 20 11:07:24 rishardkogengar.localdomain kernel: NX (Execute Disable) protection: active
Jan 20 11:07:24 rishardkogengar.localdomain kernel: APIC: Static calls initialized
Jan 20 11:07:24 rishardkogengar.localdomain kernel: SMBIOS 2.5 present.
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 20 11:07:24 rishardkogengar.localdomain kernel: DMI: Memory slots populated: 0/0
Jan 20 11:07:24 rishardkogengar.localdomain kernel: Hypervisor detected: KVM
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jan 20 11:07:24 rishardkogengar.localdomain kernel: kvm-clock: using sched offset of 4165280846 cycles
Jan 20 11:07:24 rishardkogengar.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, ma>
Jan 20 11:07:24 rishardkogengar.localdomain kernel: tsc: Detected 3187.204 MHz processor
Jan 20 11:07:24 rishardkogengar.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

Рис. 3.17: Журнал событий со вчерашнего дня

9. Выполнен просмотр только сообщений с приоритетом ошибки, зарегистрированных со вчерашнего дня.

   Это позволило быстро выделить критические и проблемные события за выбранный период времени.

```
root@rishardkogengar:/home/rishard# journalctl --since yesterday -p err
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: cnic_init
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: bnx2i_mod_init
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain systemd-udevd[528]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignor>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Jan 20 11:07:25 rishardkogengar.localdomain kernel: Warning: Unmaintained driver is detected: e1000_init_module
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupporte>
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Jan 20 11:07:25 rishardkogengar.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics devic>
Jan 20 11:07:28 rishardkogengar.localdomain alsactl[1130]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw>
Jan 20 11:08:11 rishardkogengar.localdomain gdm-password][2578]: gkr-pam: unable to locate daemon control file
Jan 20 11:08:16 rishardkogengar.localdomain systemd-coredump[3412]: [↗] Process 3387 (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-3.4.4-10.el10.x86_64
                                                                    Module libwayland-client.so.0 from rpm wayland-1.23.1-1.el10.x>
```

Рис. 3.18: Ошибки журнала со вчерашнего дня

10. Включён расширенный режим отображения журнала.

    Для каждого события были выведены дополнительные поля, включая идентификаторы загрузки, временные метки, источник сообщения, приоритет и контекст выполнения.

Рис. 3.19: Подробный вывод journalctl

11. Выполнен просмотр сообщений, относящихся к службе sshd.

    В журнале отображены сведения о запуске службы и состоянии прослушивания сетевых портов, что подтверждает корректную работу SSH-сервера.

3.5 Настройка постоянного журнала journald

1. Для выполнения настройки был запущен терминал и получены полномочия администратора, что позволило вносить изменения в системные каталоги и управлять службами systemd.

2. Создан каталог `/var/log/journal`, предназначенный для постоянного хранения журнала systemd.

   Наличие данного каталога указывает службе journald на необходимость сохранения записей на диске, а не только в оперативной памяти.

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

Рис. 3.20: Создание каталога /var/log/journal

3. Выполнена корректировка прав доступа к каталогу `/var/log/journal`.
   Владельцем каталога назначен пользователь root и группа systemd-journal, а также установлен режим доступа, позволяющий службе journald корректно записывать журнальные данные.
   Дополнительно установлен бит SGID, обеспечивающий наследование группы для создаваемых файлов.

4. Для применения изменений без перезагрузки системы отправлен сигнал службе systemd-journald.
   После получения сигнала служба пересчитала конфигурацию и начала запись журнала в постоянное хранилище.

5. Таким образом, журнал systemd был переведён в режим постоянного хранения.
   Все события теперь сохраняются на диске и доступны после перезагрузки системы.

6. Для просмотра сообщений журнала, зафиксированных с момента последней загрузки системы, может использоваться просмотр журнала текущей загрузочной сессии.
   Это позволяет анализировать события, произошедшие после последнего запуска операционной системы.

3.6 Вывод

В ходе работы были изучены механизмы журналирования в системе Linux. Освоены способы мониторинга системных и пользовательских событий в реальном времени, анализ журналов безопасности и ошибок, а также фильтрация и детализация сообщений с использованием journalctl. Выполнена настройка постоянного хранения журнала journald и централизованной регистрации событий служб. Полученные навыки позволяют эффективно контролировать состояние системы, выявлять ошибки и анализировать работу сервисов.

4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Основной файл конфигурации службы rsyslog — `/etc/rsyslog.conf`. Дополнительные и пользовательские правила регистрации событий размещаются в виде отдельных файлов в каталоге `/etc/rsyslog.d/`, что позволяет удобно структурировать конфигурацию и избегать изменений основного файла.

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

Сообщения, связанные с аутентификацией пользователей, попытками входа в систему, использованием команды su и работой PAM, записываются в файл журнала `/var/log/secure`.

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

По умолчанию ротация файлов журналов в системе Linux выполняется с использованием утилиты logrotate и осуществляется один раз в сутки.
Конкретные параметры ротации (периодичность, количество хранимых файлов, сжатие) задаются в файлах конфигурации `/etc/logrotate.conf` и `/etc/logrotate.d/`.

4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?

Для записи всех сообщений с приоритетом info в отдельный файл необходимо добавить следующую строку в конфигурацию rsyslog:

```
*.info /var/log/messages.info
```

Данная строка указывает службе rsyslog сохранять все сообщения уровня info и выше в указанный файл.

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

Для просмотра сообщений системного журнала в режиме реального времени используется команда:

```
journalctl -f
```

Она позволяет отслеживать появление новых записей по мере их регистрации в journald.

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

Для просмотра сообщений, относящихся к процессу с PID 1 за указанный промежуток времени, используется команда:

```
journalctl _PID=1 --since "09:00" --until "15:00"
```

Данная команда фильтрует журнал по идентификатору процесса и временному интервалу.

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?

Для просмотра сообщений журнала, записанных после последней загрузки системы, используется команда:

```
journalctl -b
```

Она отображает события текущей загрузочной сессии.

8. Какая процедура позволяет сделать журнал journald постоянным?

Для перевода journald в режим постоянного хранения необходимо создать каталог `/var/log/journal`, задать ему корректные права доступа и применить изменения.

После этого служба journald начинает сохранять журнальные данные на диск, и они остаются доступными после перезагрузки системы.