Отчёт по лабораторной работе №7

Управление журналами событий в системе

Амина Аджигалиева

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Ход выполнения работы

2.1 Анализ системных журналов

Сначала я просмотрела логи сбоев процессов, связанных с **VBoxClient**, и сообщения о неудачных попытках получения привилегий root.
На скриншоте видно, что при выполнении команды su вход был отклонён, а также зафиксированы ошибки в работе клиента VirtualBox.

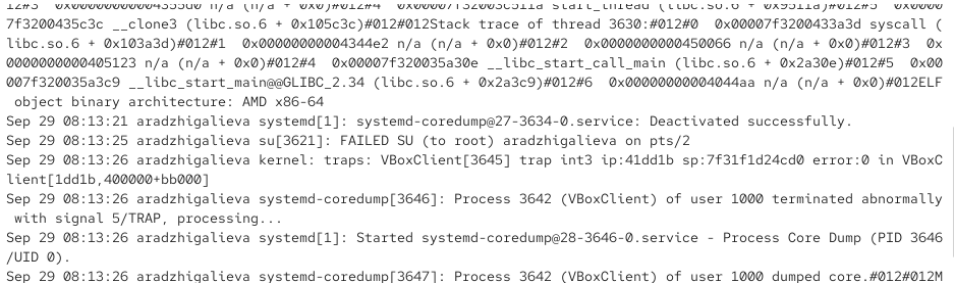


Рис. 2.1: Сообщения о сбоях VBoxClient и неудачной попытке входа под root

Далее я проанализировала системный журнал, где видно серию сообщений «hello» от пользователя **aradzhlgalieva**, а также повторяющиеся ошибки VBoxClient, сопровождающиеся завершением процессов с генерацией дампа памяти.

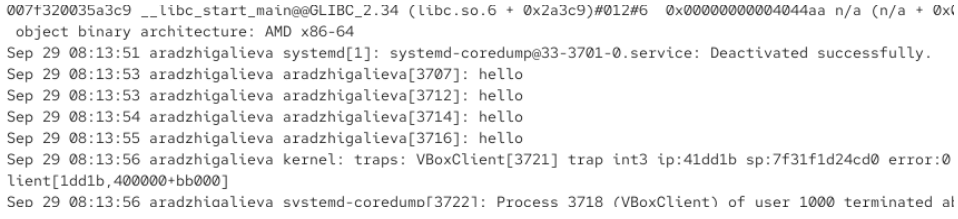


Рис. 2.2: Системные сообщения и повторные ошибки VBoxClient

Затем я обратилась к журналу **/var/log/secure**, чтобы отследить авторизации пользователей.

В выводе отчётливо видно открытие сессий для пользователей `gdm`, `aradzhlgalieva` и `root`. Также зафиксированы ошибки проверки паролей и события, связанные с PAM (Pluggable Authentication Modules).

```
root@aradzhigalieva:/home/aradzhigalieva# tail -n 20 /var/log/secure
Sep 29 08:10:34 aradzhigalieva sshd[1193]: Server listening on :: port 22.
Sep 29 08:10:34 aradzhigalieva (systemd)[1258]: pam_unix(systemd-user:session): session opened for user gdm(uid=42)
 by gdm(uid=0)
Sep 29 08:10:34 aradzhigalieva gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session ope
ned for user gdm(uid=42) by (uid=0)
Sep 29 08:10:40 aradzhigalieva unix_chkpwd[1980]: password check failed for user (aradzhigalieva)
Sep 29 08:10:40 aradzhigalieva gdm-password][1973]: pam_unix(gdm-password:auth): authentication failure; logname= u
id=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=aradzhigalieva
Sep 29 08:10:40 aradzhigalieva gdm-password][1973]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:40 aradzhigalieva gdm-password][1973]: gkr-pam: stashed password to try later in open session
Sep 29 08:10:52 aradzhigalieva gdm-password][1992]: gkr-pam: unable to locate daemon control file
Sep 29 08:10:52 aradzhigalieva gdm-password][1992]: gkr-pam: stashed password to try later in open session
Sep 29 08:10:52 aradzhigalieva (systemd)[2004]: pam_unix(systemd-user:session): session opened for user aradzhigali
eva(uid=1000) by aradzhigalieva(uid=0)
Sep 29 08:10:52 aradzhigalieva gdm-password][1992]: pam_unix(gdm-password:session): session opened for user aradzhi
galieva(uid=1000) by aradzhigalieva(uid=0)
Sep 29 08:10:52 aradzhigalieva gdm-password][1992]: gkr-pam: gnome-keyring-daemon started properly and unlocked key
ring
Sep 29 08:11:02 aradzhigalieva gdm-launch-environment][1237]: pam_unix(gdm-launch-environment:session): session clo
sed for user gdm
Sep 29 08:12:33 aradzhigalieva (systemd)[3365]: pam_unix(systemd-user:session): session opened for user root(uid=0)
 by root(uid=0)
Sep 29 08:12:33 aradzhigalieva su[3350]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigaliev
a(uid=1000)
Sep 29 08:12:42 aradzhigalieva su[3445]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigaliev
a(uid=1000)
Sep 29 08:12:47 aradzhigalieva su[3508]: pam_unix(su:session): session opened for user root(uid=0) by aradzhigaliev
a(uid=1000)
Sep 29 08:13:19 aradzhigalieva su[3508]: pam_unix(su:session): session closed for user root
Sep 29 08:13:22 aradzhigalieva unix_chkpwd[3640]: password check failed for user (root)
```

Рис. 2.3: Просмотр журнала /var/log/secure

2.2 Настройка регистрации сообщений через rsyslog

Сначала я установила веб-сервер Apache и запустила его службу. Также я настроила автоматический запуск `httpd` при старте 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-2.4.63-1.el10_0.2.x86_64                   httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch        httpd-tools-2.4.63-1.el10_0.2.x86_64
  mod_http2-2.0.29-2.el10_0.1.x86_64               mod_lua-2.4.63-1.el10_0.2.x86_64
  rocky-logos-httpd-100.4-7.el10.noarch

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

Рис. 2.4: Установка и запуск Apache

Затем я просмотрела журнал ошибок веб-службы, чтобы убедиться в корректности её работы.

На скриншоте видно сообщения о запуске Apache и успешной конфигурации.

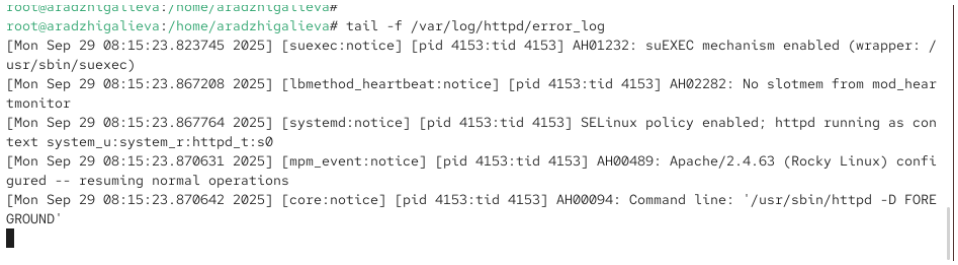


Рис. 2.5: Просмотр error_log веб-сервера

После этого я изменила конфигурацию веб-сервера, добавив в файл `/etc/httpd/conf/httpd.conf` строку:

`ErrorLog syslog:local1`.

Эта настройка позволяет перенаправлять сообщения об ошибках Apache в системный журнал.

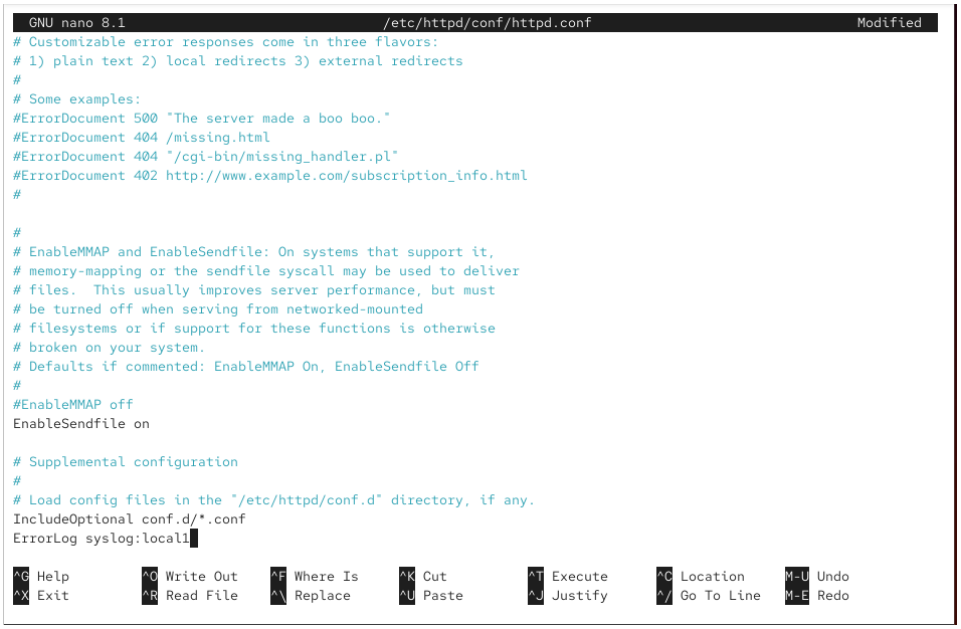


Рис. 2.6: Редактирование httpd.conf

В каталоге `/etc/rsyslog.d` я создала новый файл конфигурации и добавила пра-

вило, которое направляет все сообщения объекта `local1` в файл `/var/log/httpd-error.log`.

Рис. 2.7: Создание правила для регистрации ошибок Apache

Затем я создала отдельный файл `debug.conf` для регистрации отладочных сообщений и указала в нём правило:
`*.debug /var/log/messages-debug`.

Рис. 2.8: Создание файла debug.conf

После перезапуска служб `rsyslog` и `httpd` я проверила работу конфигурации. Для этого выполнила команду `logger -p daemon.debug "Daemon Debug Message"`. На скриншоте видно, что отладочные сообщения корректно записываются в файл `/var/log/messages-debug`, а ошибки VBoxClient продолжают фиксироваться.

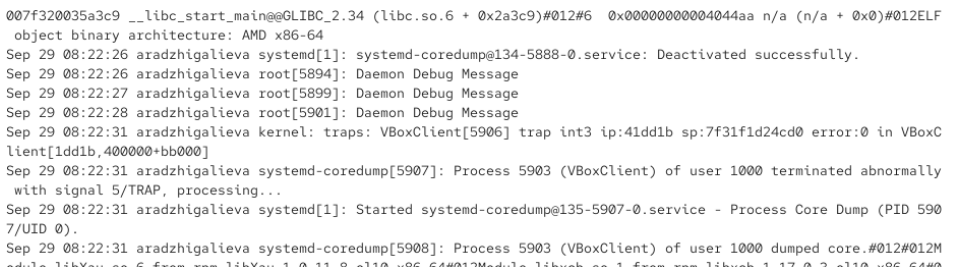


Рис. 2.9: Проверка работы отладочного логирования

2.3 Использование journalctl

Сначала я просмотрела журнал системы, чтобы получить список событий, начиная с последней загрузки.

Команда `journalctl` показала записи ядра и системных служб, включая параметры запуска и информацию о виртуальной машине.

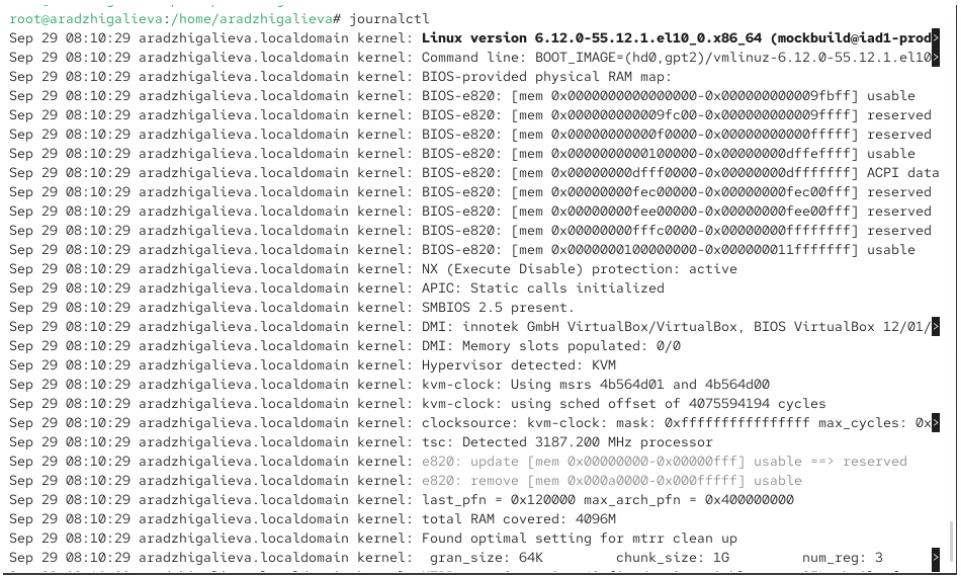
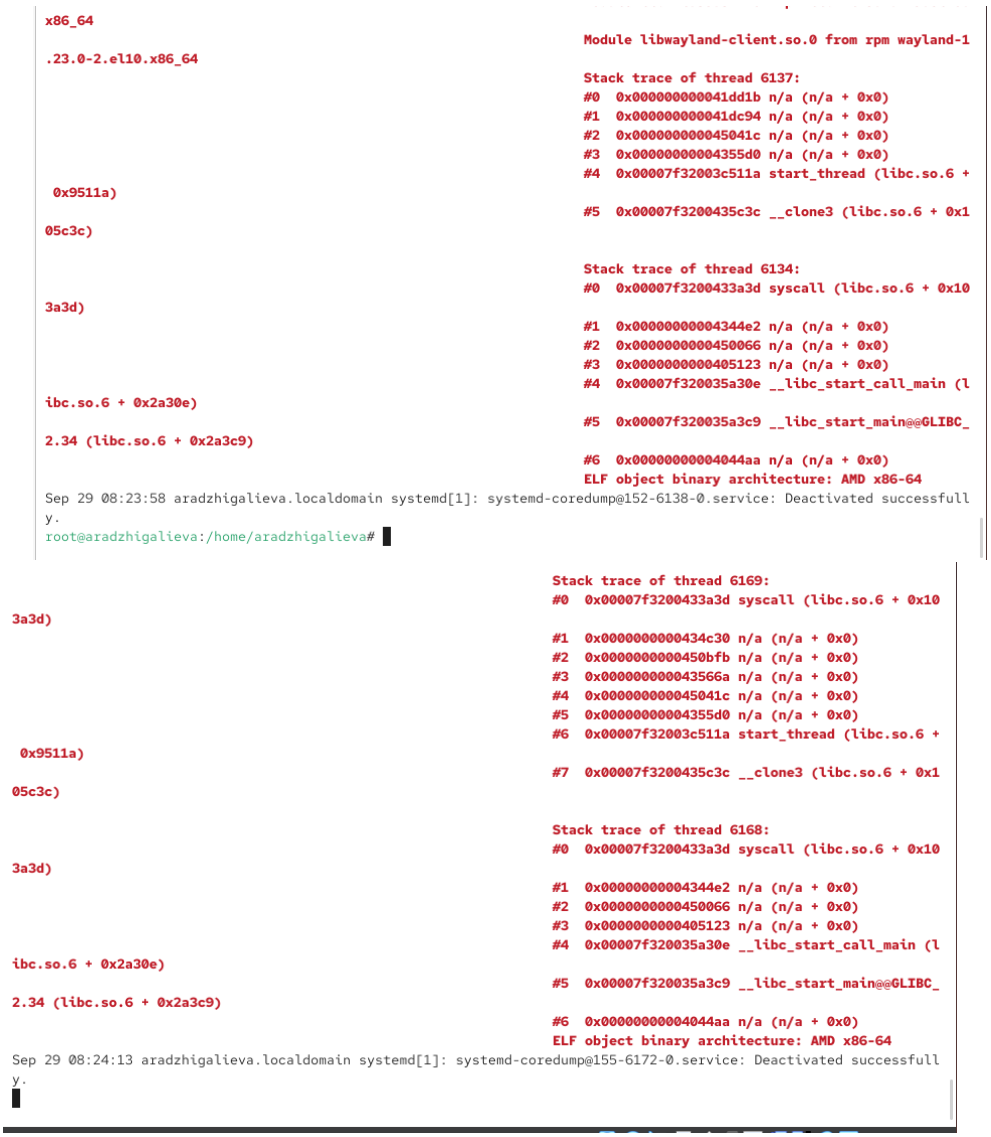


Рис. 2.10: Просмотр системного журнала

Затем я проанализировала ошибки, связанные с библиотеками и аварийным завершением процессов.

Скриншоты фиксируют трассировки стека (stack trace), полученные при падении процессов.



Для фильтрации событий я использовала встроенные параметры. При вводе команды `journalctl` и двойном нажатии Tab был отображён список доступных фильтров.

```
root@aradzhigalieva:/home/aradzhigalieva# 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=
```

Рис. 2.11: Отображение доступных фильтров journalctl

Затем я просмотрела только те события, которые связаны с пользователем root (`UID=0`).

В журнале отображаются действия системных служб и процессы, запускаемые от имени суперпользователя.

```
root@aradzhigalieva:/home/aradzhigalieva#
root@aradzhigalieva:/home/aradzhigalieva# journalctl _UID=0
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Collecting audit messages is disabled.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Journal started
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-journald[281]: Runtime Journal (/run/log/journal/343a350182dc42>
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'msr' is built in
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Inserted module 'fuse'
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_alua' is built in
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_emc' is built in
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-modules-load[282]: Module 'scsi_dh_rdac' is built in
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console S>
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdl>
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'nobody' with GID 65534.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'users' with GID 100.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd-sysusers[295]: Creating group 'systemd-journal' with GID 190.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static>
Sep 29 08:10:29 aradzhigalieva.localdomain dracut-cmdline[304]: dracut-105-4.el10_0
Sep 29 08:10:29 aradzhigalieva.localdomain dracut-cmdline[304]: Using kernel command line parameters:    BOOT_IMAG>
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static>
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Sep 29 08:10:29 aradzhigalieva.localdomain systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Dev>
```

Рис. 2.12: Просмотр событий для UID=0

Для анализа последних записей я вывела последние 20 строк журнала с помощью команды `journalctl -n 20`.

В сообщениях видны ошибки клиента VirtualBox и созданные дампы процессов.

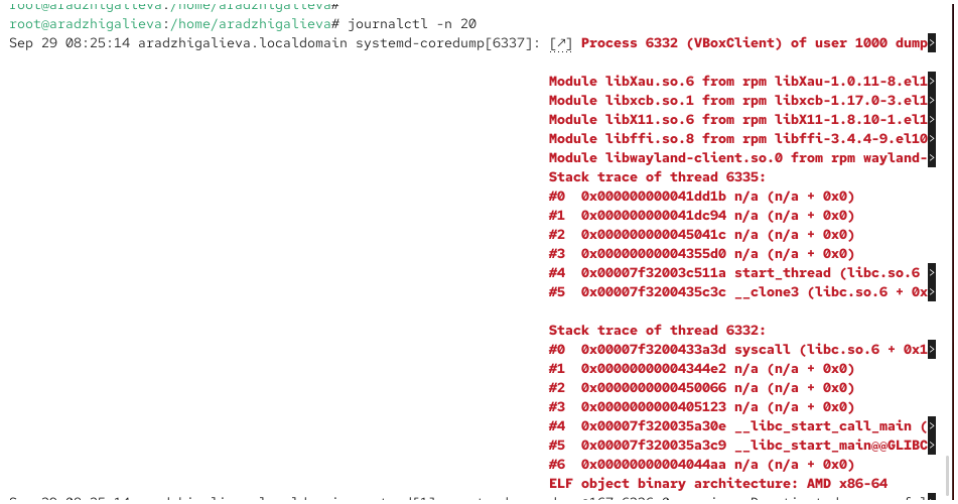


Рис. 2.13: Вывод последних строк журнала

Далее я просмотрела только сообщения уровня ошибок с помощью команды `journalctl -p err`.

В выводе содержатся ошибки графического драйвера `vmwgfx`, предупреждения ядра и сбои процессов VBoxClient.

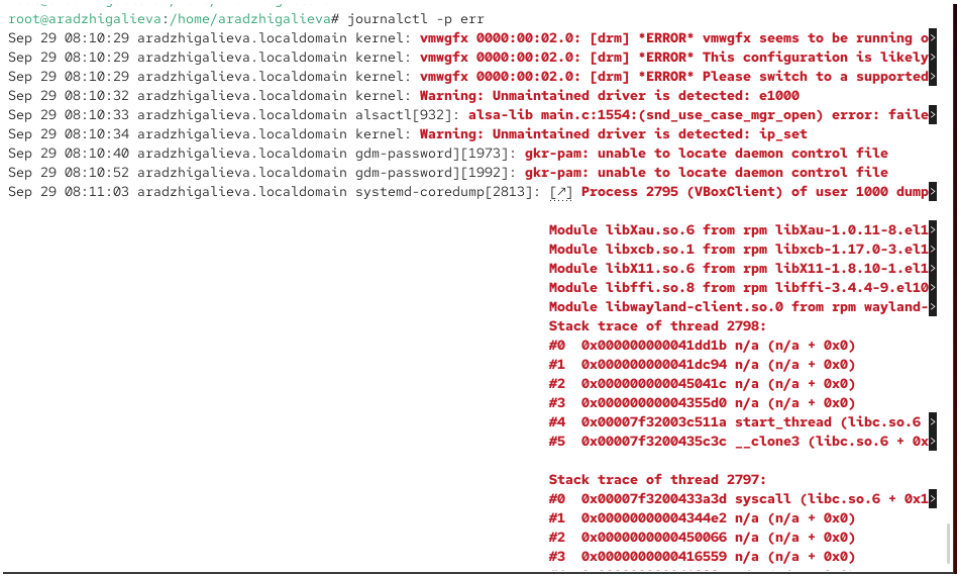


Рис. 2.14: Фильтрация сообщений по приоритету ошибок

Используя параметр `--since yesterday`, я просмотрела все события, начиная со вчерашнего дня.

Журнал снова показал последовательность загрузки системы и параметры ядра.

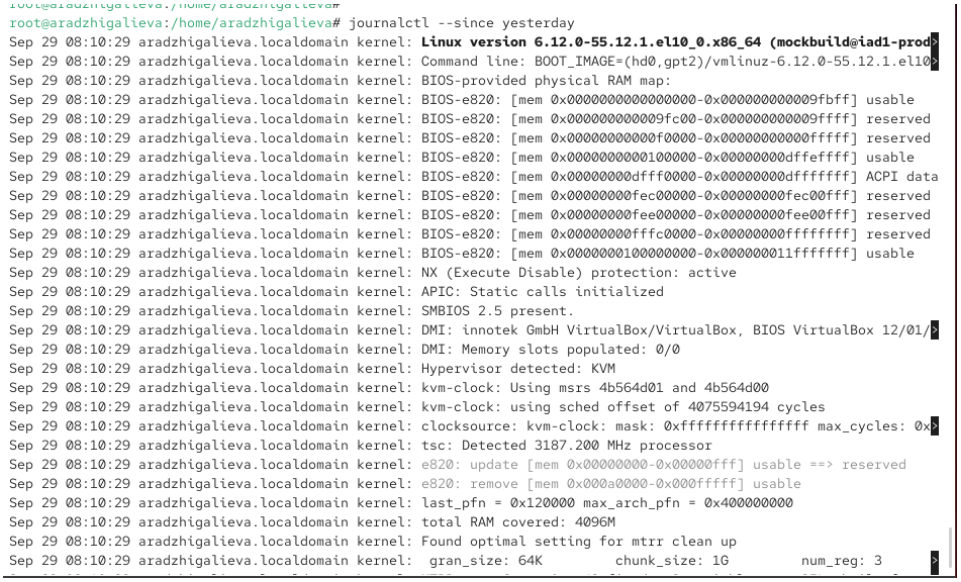


Рис. 2.15: События со вчерашнего дня

Затем я объединила фильтры и вывела только ошибки, зафиксированные со вчерашнего дня: `journalctl --since yesterday -p err`.
Результат включает сообщения о проблемах с драйвером `vmwgfx`, PAM-авторизацией и сбоями VBoxClient.

Рис. 2.16: Ошибки со вчерашнего дня

Для получения более подробных сведений я использовала режим `journalctl`

`-o verbose`.

На скриншоте видно, что каждая запись сопровождается расширенными атрибутами: временем, хостом, идентификатором процесса и приоритетом.

Рис. 2.17: Подробный вывод журнала

Я использовала команду `journalctl _SYSTEMD_UNIT=sshd.service`, чтобы просмотреть сообщения, относящиеся к службе `sshd`.

В выводе отразились предупреждение об unset-переменной окружения, а также информация о том, что сервер слушает порт 22.

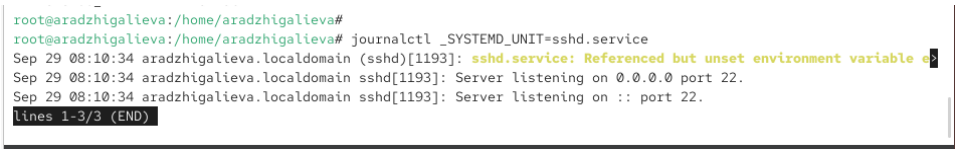


Рис. 2.18: Просмотр журнала sshd

2.4 Настройка постоянного журнала journald

По умолчанию система хранит журнал journald во временном каталоге `/run/log/journal`, и после перезагрузки записи теряются.

Чтобы сделать журнал постоянным, я создала каталог `/var/log/journal`, назначила владельца и права доступа, а затем отправила сигнал `USR1` процессу `systemd-journald`.

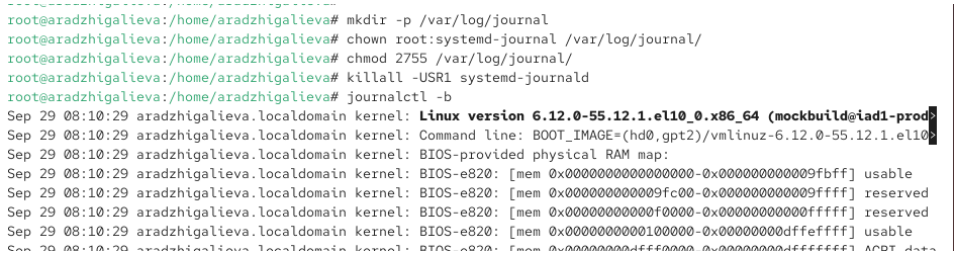


Рис. 2.19: Создание постоянного журнала journald

После этого я выполнила команду `journalctl -b`, чтобы убедиться, что журнал сохраняет записи с момента последней загрузки системы.
В выводе отразились стандартные сообщения ядра и параметры запуска.

3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**
   Основной файл конфигурации — `/etc/rsyslog.conf`. Дополнительные правила могут храниться в каталоге `/etc/rsyslog.d/`.

2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**
   Сообщения об аутентификации обычно записываются в файл `/var/log/secure`.

3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**
   По умолчанию ротация журналов выполняется еженедельно (настраивается через `logrotate`).

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

5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**
   Для этого используется команда:
   `journalctl -f`

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

Используется команда:

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

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

   Для этого используется команда:

   ```
   journalctl -b
   ```

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

   Нужно создать каталог `/var/log/journal`, назначить владельца и права:

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

4 Заключение

В ходе выполнения лабораторной работы я изучила принципы работы системных журналов Linux и научилась настраивать их хранение и просмотр.
Я освоила использование команд `journalctl` и различных параметров фильтрации, научилась отслеживать ошибки и события в режиме реального времени, а также работать с приоритетами сообщений.
Кроме того, я настроила службу `rsyslogd` для перенаправления логов веб-сервера Apache и добавила правила для записи отладочной информации в отдельный файл.
Я также сделала журнал journald постоянным, чтобы записи сохранялись после перезагрузки системы.

Все выполненные действия позволили закрепить знания о механизмах логирования в Linux, а также получить практические навыки администрирования, которые необходимы для обеспечения контроля и диагностики работы системы.