

Лабораторная работа № 7

Отчёт

Ермишина Мария Кирилловна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Контрольные вопросы	13
4	Выводы	14

Список иллюстраций

2.1	Изменения на второй вкладке	6
2.2	Мониторинг сообщений безопасности	7
2.3	Установка Apache	7
2.4	Журнал соо. об ошибках	8
2.5	Редактирование файла	8
2.6	Работа с третьим окном	9
2.7	Журнал с событиями с момента запуска	10
2.8	Журналы без пейджера и в реальном времени	10
2.9	Фильтрация	10
2.10	Сообщения об ошибках	11
2.11	Каталог для хранения записей журнала	11
2.12	Журнал с момента посл. перезагрузки	12

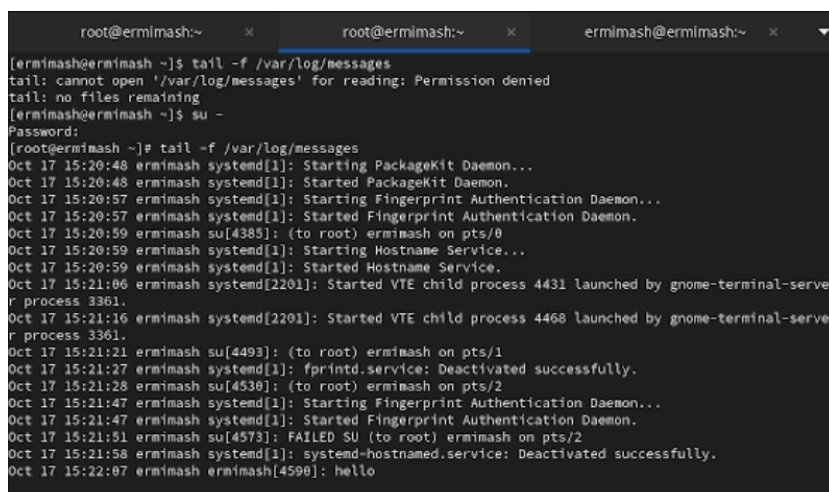
Список таблиц

1 Цель работы

Целью данной лабораторной работы является получение навыков работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

1. Мониторинг журнала системных событий в реальном времени Запустите три вкладки терминала и в каждом из них получите полномочия администратора. На второй вкладке терминала запустите мониторинг системных событий в реальном времени: (рис. 2.1)
- `tail -f /var/log/messages` В третьей вкладке терминала вернитесь к учётной записи своего пользователя и попробуйте получить полномочия администратора, но введите неправильный пароль. Обратите внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username ...». (рис. 2.1) В третьей вкладке терминала из оболочки пользователя введите `logger hello` - во второй вкладке терминала с мониторингом событий вы увидите сообщение. (рис. 2.1)



```
root@ermimash:~  
ermimash@ermimash:~$ tail -f /var/log/messages  
tail: cannot open '/var/log/messages' for reading: Permission denied  
tail: no files remaining  
ermimash@ermimash:~$ su -  
Password:  
[root@ermimash:~]# tail -f /var/log/messages  
Oct 17 15:20:48 ermimash systemd[1]: Starting PackageKit Daemon...  
Oct 17 15:20:48 ermimash systemd[1]: Started PackageKit Daemon.  
Oct 17 15:20:57 ermimash systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 17 15:20:57 ermimash systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 17 15:20:59 ermimash su[4385]: (to root) ermimash on pts/0  
Oct 17 15:20:59 ermimash systemd[1]: Starting Hostname Service...  
Oct 17 15:20:59 ermimash systemd[1]: Started Hostname Service.  
Oct 17 15:21:06 ermimash systemd[2201]: Started VTE child process 4431 launched by gnome-terminal-serve  
r process 3361.  
Oct 17 15:21:16 ermimash systemd[2201]: Started VTE child process 4468 launched by gnome-terminal-serve  
r process 3361.  
Oct 17 15:21:21 ermimash su[4493]: (to root) ermimash on pts/1  
Oct 17 15:21:27 ermimash systemd[1]: fprintd.service: Deactivated successfully.  
Oct 17 15:21:28 ermimash su[4530]: (to root) ermimash on pts/2  
Oct 17 15:21:47 ermimash systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 17 15:21:47 ermimash systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 17 15:21:51 ermimash su[4573]: FAILED SU (to root) ermimash on pts/2  
Oct 17 15:21:58 ermimash systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Oct 17 15:22:07 ermimash ermimash[4590]: hello
```

Рис. 2.1: Изменения на второй вкладке

Во второй вкладке терминала с мониторингом остановите трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем запустите мониторинг сообщений безопасности: (рис. 2.2) - tail -n 20 /var/log/secure

```
[root@ermimash ~]# tail -n 20 /var/log/secure
Oct 17 14:11:00 ermimash sshd[1216]: Server listening on 0.0.0.0 port 22.
Oct 17 14:11:00 ermimash sshd[1216]: Server listening on :: port 22.
Oct 17 14:11:01 ermimash systemd[1250]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 17 14:11:03 ermimash gdm-launch-environment[1245]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 17 14:11:23 ermimash polkitd[838]: Registered Authentication Agent for unix-session:c1 (system bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 17 14:11:32 ermimash gdm-password[2186]: gkr-pam: unable to locate daemon control file
Oct 17 14:11:32 ermimash gdm-password[2186]: gkr-pam: stashed password to try later in open session
Oct 17 14:11:32 ermimash systemd[2201]: pam_unix(systemd-user:session): session opened for user ermimash(uid=1000) by ermimash(uid=0)
Oct 17 14:11:33 ermimash gdm-password[2186]: pam_unix(gdm-password:session): session opened for user ermimash(uid=1000) by ermimash(uid=0)
Oct 17 14:11:33 ermimash gdm-password[2186]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 17 14:11:34 ermimash polkitd[838]: Registered Authentication Agent for unix-session:2 (system bus name :1.60 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 17 14:11:37 ermimash gdm-launch-environment[1245]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 17 14:11:37 ermimash polkitd[838]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct 17 15:17:59 ermimash gdm-password[4298]: gkr-pam: unlocked login keyring
Oct 17 15:20:59 ermimash su[4385]: pam_unix(su-l:session): session opened for user root(uid=0) by ermimash(uid=1000)
Oct 17 15:21:21 ermimash su[4401]: pam_unix(su-l:session): session opened for user root(uid=0) by ermimash(uid=1000)
```

Рис. 2.2: Мониторинг сообщений безопасности

2. Изменение правил rsyslog.conf В первой вкладке терминала установите Apache, если он не был ранее инсталлирован: (рис. 2.3)

- dnf -y install httpd После окончания процесса установки запустите веб-службу: (рис. 2.3)
- systemctl start httpd
- systemctl enable httpd

```
Running scriptlet: mod_http2-2.0.26-4.el9_0.1.x86_64 11/11
Verifying      : apr-util-bdb-1.6.1-23.el9.x86_64 1/11
Verifying      : httpd-tools-2.4.62-4.el9_6.4.x86_64 2/11
Verifying      : httpd-2.4.62-4.el9_6.4.x86_64 3/11
Verifying      : apr-util-1.6.1-23.el9.x86_64 4/11
Verifying      : rocky-logos-httpd-90.16-1.el9.noarch 5/11
Verifying      : httpd-core-2.4.62-4.el9_6.4.x86_64 6/11
Verifying      : httpd-filesystem-2.4.62-4.el9_6.4.noarch 7/11
Verifying      : mod_lua-2.4.62-4.el9_6.4.x86_64 8/11
Verifying      : mod_http2-2.0.26-4.el9_6.1.x86_64 9/11
Verifying      : apr-util-openssl-1.6.1-23.el9.x86_64 10/11
Verifying      : apr-1.7.0-12.el9_3.x86_64 11/11

Installed:
apr-1.7.0-12.el9_3.x86_64          apr-util-1.6.1-23.el9.x86_64
apr-util-bdb-1.6.1-23.el9.x86_64 apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.62-4.el9_6.4.x86_64    httpd-core-2.4.62-4.el9_6.4.x86_64
httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x86_64
mod_http2-2.0.26-4.el9_6.1.x86_64 mod_lua-2.4.62-4.el9_6.4.x86_64
rocky-logos-httpd-90.16-1.el9.noarch

Complete!
[root@ermimash ~]# systemctl start httpd
[root@ermimash ~]# systemctl enable httpd
```

Рис. 2.3: Установка Apache

Во второй вкладке терминала посмотрите журнал сообщений об ошибках веб-службы: (рис. 2.4) - `tail -f /var/log/httpd/error_log`

```
Oct 17 14:11:37 erlimash polkitd[838]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct 17 15:17:59 erlimash gdm-password[4298]: gkr-pam: unlocked login keyring
Oct 17 15:20:59 erlimash su[4385]: pam_unix(su-l:session): session opened for user root(uid=0) by erlimash(uid=1000)
Oct 17 15:21:21 erlimash su[4493]: pam_unix(su-l:session): session opened for user root(uid=0) by erlimash(uid=1000)
Oct 17 15:21:28 erlimash su[4530]: pam_unix(su-l:session): session opened for user root(uid=0) by erlimash(uid=1000)
Oct 17 15:21:40 erlimash su[4530]: pam_unix(su-l:session): session closed for user root
Oct 17 15:21:49 erlimash unix_chkpwd[4580]: password check failed for user (root)
Oct 17 15:21:49 erlimash su[4573]: pam_unix(su-l:auth): authentication failure; logname=erlimash uid=1000 euid=0 tty=/dev/pts/2 ruser=erlimash rhost= user=root
[erlimash@erlimash ~]$ tail -f /var/log/httpd/error_log
[Fri Oct 17 15:23:09.619517 2025] [core:notice] [pid 11017:tid 11017] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s8
[Fri Oct 17 15:23:09.620172 2025] [suexec:notice] [pid 11017:tid 11017] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 17 15:23:09.637054 2025] [lbmethod_heartbeat:notice] [pid 11017:tid 11017] AH02282: No slotmem from mod_heartbeat
[Fri Oct 17 15:23:09.640397 2025] [mpm_event:notice] [pid 11017:tid 11017] AH00489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 17 15:23:09.650116 2025] [core:notice] [pid 11017:tid 11017] AH00957: Command Line: /usr/sbin/httpd -D
```

Рис. 2.4: Журнал соо. об ошибках

В каталоге `/etc/rsyslog.d` создайте файл мониторинга событий веб-службы: - `cd /etc/rsyslog.d - touch httpd.conf` Открыв его на редактирование, пропишите в нём: (рис. 2.5) - `local1.* -/var/log/httpd-error.log`

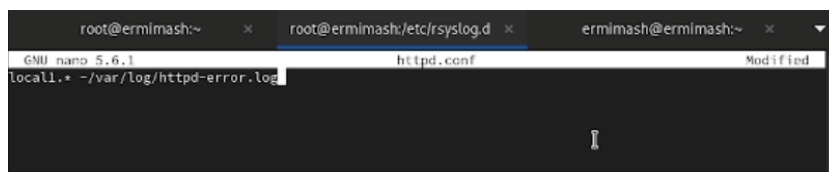


Рис. 2.5: Редактирование файла

Перейдите в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу: - `systemctl restart rsyslog.service - systemctl restart httpd`

В третьей вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации: (рис. 2.6) - `cd /etc/rsyslog.d - touch debug.conf`

В этом же терминале введите: (рис. 2.6) - `echo "'.debug /var/log/messages-debug'" > /etc/rsyslog.d/debug.conf`

В первой вкладке терминала снова перезапустите rsyslogd: - `systemctl restart rsyslog.service`

Во второй вкладке терминала запустите мониторинг отладочной информации: - `tail -f /var/log/messages-debug`

В третьей вкладке терминала введите: (рис. 2.6) - `logger -p daemon.debug`
“Daemon Debug Message”

В терминале с мониторингом посмотрите сообщение отладки.

```
[ermimash@ermimash rsyslog.d]$ su -  
Password:  
[root@ermimash ~]# touch debug.conf  
[root@ermimash ~]# rm -r debug.conf  
rm: remove regular empty file 'debug.conf'? y  
[root@ermimash ~]# cd /etc/rsyslog.d  
[root@ermimash rsyslog.d]# touch debug.conf  
[root@ermimash rsyslog.d]# echo "*.debug /var/log/messages-debug" >  
/etc/rsyslog.d/debug.conf  
-bash: syntax error near unexpected token 'newline'  
-bash: /etc/rsyslog.d/debug.conf: Permission denied  
[root@ermimash rsyslog.d]#  
logout  
[ermimash@ermimash rsyslog.d]$ echo "*.debug /var/log/messages-debug" >  
/etc/rsyslog.d/debug.conf  
bash: syntax error near unexpected token 'newline'  
bash: /etc/rsyslog.d/debug.conf: Permission denied  
[ermimash@ermimash rsyslog.d]# echo "*.debug /var/log/messages-debug" >  
bash: syntax error near unexpected token 'newline'  
[ermimash@ermimash rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
bash: /etc/rsyslog.d/debug.conf: Permission denied  
[ermimash@ermimash rsyslog.d]# su -  
Password:  
[root@ermimash ~]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf  
[root@ermimash ~]# logger -p daemon.debug "Daemon Debug Message"  
[root@ermimash ~]#
```

Рис. 2.6: Работа с третьим окном

3. Использование `journalctl` Во второй вкладке терминала посмотрите содержимое журнала с событиями с момента последнего запуска системы: (рис. 2.7)

- `journalctl` Просмотр содержимого журнала без использования пейджера: (рис. 2.8)
- `journalctl --no-pager` Режим просмотра журнала в реальном времени: (рис. 2.8)
- `journalctl -f`

```

Oct 17 14:10:38 erminash.localdomain kernel: BPF: 1 zonelists, mobility grouping on. Total pages: 25
Oct 17 14:10:38 erminash.localdomain kernel: Policy zone: Normal
Oct 17 14:10:38 erminash.localdomain kernel: mem auto-init: stack:off, heap alloc:off, heap free:off
Oct 17 14:10:38 erminash.localdomain kernel: software IO TLB: area num 8.
Oct 17 14:10:38 erminash.localdomain kernel: Memory: 3413084K/10485304K available (16384K kernel code, 1
Oct 17 14:10:38 erminash.localdomain kernel: SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=6, Nodes=1
Oct 17 14:10:38 erminash.localdomain kernel: ftrace: allocating 49070 entries in 192 pages
Oct 17 14:10:38 erminash.localdomain kernel: ftrace: allocated 192 pages with 2 groups
Oct 17 14:10:38 erminash.localdomain kernel: Dynamic Preempt: voluntary
Oct 17 14:10:38 erminash.localdomain kernel: rcu: Preemptible hierarchical RCU implementation.
Oct 17 14:10:38 erminash.localdomain kernel: rcu: RCU event tracing is enabled.
Oct 17 14:10:38 erminash.localdomain kernel: rcu: RCU restricting CPUs from NR_CPUS=8192 to nr
Oct 17 14:10:38 erminash.localdomain kernel: Trampoline variant of Tasks RCU enabled.
Oct 17 14:10:38 erminash.localdomain kernel: Rude variant of Tasks RCU enabled.
Oct 17 14:10:38 erminash.localdomain kernel: Tracing variant of Tasks RCU enabled.
Oct 17 14:10:38 erminash.localdomain kernel: rcu: RCU calculated value of scheduler-enlistment delay is
Oct 17 14:10:38 erminash.localdomain kernel: rcu: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_id
Oct 17 14:10:38 erminash.localdomain kernel: RCU Tasks: Setting shift to 3 and lim to 1 rcu_task_cb_ad
Oct 17 14:10:38 erminash.localdomain kernel: RCU Tasks Rude: Setting shift to 3 and lim to 1 rcu_task
Oct 17 14:10:38 erminash.localdomain kernel: RCU Tasks Trace: Setting shift to 3 and lim to 1 rcu_task
Oct 17 14:10:38 erminash.localdomain kernel: NR_IRQS: 524544, nr_irqs: 472, preallocated irq: 16
Oct 17 14:10:38 erminash.localdomain kernel: rcu: srcu_init: Setting srcu_struct sizes based on conten
Oct 17 14:10:38 erminash.localdomain kernel: kfence: initialized - using 2097152 bytes for 255 object
Oct 17 14:10:38 erminash.localdomain kernel: Console: colour VGA+ 80x25
Oct 17 14:10:38 erminash.localdomain kernel: printk: legacy console [tty0] enabled
Oct 17 14:10:38 erminash.localdomain kernel: ACPI: Core revision 20230331
Oct 17 14:10:38 erminash.localdomain kernel: APIC: Switch to symmetric I/O mode setup
Oct 17 14:10:38 erminash.localdomain kernel: x2apic enabled

```

Рис. 2.7: Журнал с событиями с момента запуска

```

Oct 17 15:27:03 erminash.localdomain systemd[1]: Starting Hostname Service...
Oct 17 15:27:03 erminash.localdomain systemd[1]: Started Hostname Service.
Oct 17 15:27:18 erminash.localdomain systemd[1]: Stopping System Logging Service...
Oct 17 15:27:18 erminash.localdomain rsyslogd[43996]: [origin software="rsyslogd" swVersion="8.2412.0-1
.el9" x-pid="43996" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 17 15:27:18 erminash.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 17 15:27:18 erminash.localdomain systemd[1]: Stopped System Logging Service.
Oct 17 15:27:18 erminash.localdomain systemd[1]: Starting System Logging Service...
Oct 17 15:27:18 erminash.localdomain rsyslogd[44372]: [origin software="rsyslogd" swVersion="8.2412.0-1
.el9" x-pid="44372" x-info="https://www.rsyslog.com"] start
Oct 17 15:27:18 erminash.localdomain systemd[1]: Started System Logging Service.
Oct 17 15:27:18 erminash.localdomain rsyslogd[44372]: imjournal: journal files changed, reloading... [
v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 17 15:27:32 erminash.localdomain systemd[1]: fprintd.service: Deactivated successfully.
Oct 17 15:27:33 erminash.localdomain systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 17 15:27:41 erminash.localdomain root[44394]: Daemon Debug Message
Oct 17 15:28:08 erminash.localdomain PackageKit[4375]: daemon quit
Oct 17 15:28:08 erminash.localdomain systemd[1]: packagekit.service: Deactivated successfully.
[root@erminash rsyslog.d]# journalctl -f
Oct 17 15:27:18 erminash.localdomain systemd[1]: Stopped System Logging Service.
Oct 17 15:27:18 erminash.localdomain systemd[1]: Starting System Logging Service...
Oct 17 15:27:18 erminash.localdomain rsyslogd[44372]: [origin software="rsyslogd" swVersion="8.2412.0-1

```

Рис. 2.8: Журналы без пейджера и в реальном времени

Для использования фильтрации просмотра конкретных параметров журнала введите - journalctl и дважды нажмите клавишу Tab (рис. 2.9)

```

COMMAND=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
DBUS_BROKER_MESSAGE_DESTINATION=
DBUS_BROKER_MESSAGE_INTERFACE=
DBUS_BROKER_MESSAGE_MEMBER=
DBUS_BROKER_MESSAGE_PATH=
DBUS_BROKER_MESSAGE_SERIAL=
DBUS_BROKER_MESSAGE_SIGNATURE=
DBUS_BROKER_MESSAGE_TYPE=
DBUS_BROKER_MESSAGE_UNIX_FDS=
DBUS_BROKER_METRICS_DISPATCH_AVG=
DBUS_BROKER_METRICS_DISPATCH_COUNT=
DBUS_BROKER_METRICS_DISPATCH_MAX=
DBUS_BROKER_METRICS_DISPATCH_MIN=
DBUS_BROKER_METRICS_DISPATCH_STDDEV=
DBUS_BROKER_POLICY_TYPE=
DBUS_BROKER_RECEIVER_SECURITY_LABEL=
DBUS_BROKER_RECEIVER_UNIQUE_NAME=
DBUS_BROKER_RECEIVER_WELL_KNOWN_NAME_0=
NM_DEVICE=
NM_LOG_DOMAINS=
NM_LOG_LEVEL=
_PID=
_PRIORITY=
_REALMD_OPERATION=
_RUNTIME_SCOPE=
_SEAT_ID=
_SELINUX_CONTEXT=
_SESSION_ID=
_SOURCE_MONOTONIC_TIMESTAMP=
_SOURCE_REALTIME_TIMESTAMP=
_SSSD_DOMAIN=
_SSSD_PRG_NAME=
_STREAM_ID=
_SYSLOG_FACILITY=
_SYSLOG_IDENTIFIER=
_SYSLOG_PID=
_SYSLOG_RAW=
_SYSLOG_TIMESTAMP=
_SYSTEMD_CGROUP=
_SYSTEMD_INVOCATION_ID=

```

Рис. 2.9: Фильтрация

Просмотрите события для UID0: - journalctl _UID=0 Для отображения последних 20 строк журнала введите: - journalctl -n 20 Для просмотра только сообщений об ошибках введите: (рис. 2.10) - journalctl -p err Для просмотра всех сообщений со вчерашнего дня введите: - journalctl -since yesterday

Если вы хотите показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используйте: - journalctl -since yesterday -p err Если вам нужна детальная информация, то используйте: - journalctl -o verbose Для просмотра дополнительной информации о модуле sshd введите: - journalctl _SYSTEMD_UNIT=sshd.service

```
[root@ermimash rsyslog.d]# journalctl -p err
Oct 17 14:10:38 ermimash.localdomain kernel: Warning: Unmaintained driver is detected: #1000
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup
Oct 17 14:10:49 ermimash.localdomain alsactl[876]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:
Oct 17 14:10:59 ermimash.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 17 14:11:32 ermimash.localdomain gdm-password[2186]: gkr-pam: unable to locate daemon control file
Oct 17 14:11:35 ermimash.localdomain systemd[2201]: failed to start application launched by gdm-session
```

Рис. 2.10: Сообщения об ошибках

4. Постоянный журнал journald Запустите терминал и получите полномочия администратора. Создайте каталог для хранения записей журнала: (рис. 2.11)

 - mkdir -p /var/log/journal Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию: (рис. ??)
 - chown root:systemd-journal /var/log/journal
 - chmod 2755 /var/log/journal Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: (рис. 2.11)
 - killall -USR1 systemd-journald

```
[ermimash@ermimash rsyslog.d]$ su -
Password:
[root@ermimash ~]# mkdir -p /var/log/journal
[root@ermimash ~]# chown root:systemd-journal /var/log/journal
[root@ermimash ~]# chmod 2755 /var/log/journal
[root@ermimash ~]# killall -USR1 systemd-journald
[root@ermimash ~]#
```

Рис. 2.11: Каталог для хранения записей журнала

Если вы хотите видеть сообщения журнала с момента последней перезагрузки, используйте: (рис. 2.12) - journalctl -b

```
Oct 17 14:10:38 erminash.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-provided physical RAM map:
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] us
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] re
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000009ffff] re
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] us
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x0000000000dfffff-0x0000000000dfffff] AC
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] re
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] re
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffffff] re
Oct 17 14:10:38 erminash.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x0000000029ffffff] us
Oct 17 14:10:38 erminash.localdomain kernel: NX (Execute Disable) protection: active
Oct 17 14:10:38 erminash.localdomain kernel: APIC: Static calls initialized
Oct 17 14:10:38 erminash.localdomain kernel: SMBIOS 2.5 present.
Oct 17 14:10:38 erminash.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox
Oct 17 14:10:38 erminash.localdomain kernel: Hypervisor detected: KVM
Oct 17 14:10:38 erminash.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 17 14:10:38 erminash.localdomain kernel: kvm-clock: using sched offset of 5170905296 cycles
Oct 17 14:10:38 erminash.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles
Oct 17 14:10:38 erminash.localdomain kernel: tsc: Detected 3693.066 MHz processor
Oct 17 14:10:38 erminash.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> rese
Oct 17 14:10:38 erminash.localdomain kernel: e820: remove [mem 0x00000000-0x0000ffff] usable
Oct 17 14:10:38 erminash.localdomain kernel: last_pfn = 0x2a0000 max_arch_pfn = 0x40000000
Oct 17 14:10:38 erminash.localdomain kernel: total RAM covered: 10240M
Oct 17 14:10:38 erminash.localdomain kernel: Found optimal setting for mtrr clean up
Oct 17 14:10:38 erminash.localdomain kernel: gran_size: 64K chunk_size: 64K num_reg:
Oct 17 14:10:38 erminash.localdomain kernel: MTRR map: 5 entries (3 fixed + 2 variable; max 35), built
Oct 17 14:10:38 erminash.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC-
Oct 17 14:10:38 erminash.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> rese
Oct 17 14:10:38 erminash.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x40000000
Oct 17 14:10:38 erminash.localdomain kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
Oct 17 14:10:38 erminash.localdomain kernel: RAMDISK: [mem 0x30cc1000-0x34658fff]
Oct 17 14:10:38 erminash.localdomain kernel: ACPI: Early table checksum verification disabled
Oct 17 14:10:38 erminash.localdomain kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
Oct 17 14:10:38 erminash.localdomain kernel: ACPI: XSDT 0x0000000000000000 000026 (v01 VBOX )
```

Рис. 2.12: Журнал с момента посл. перезагрузки

3 Контрольные вопросы

1. `/etc/rsyslog.conf`
2. `/var/log/secure`
3. Неделя
4. `info.* - /var/log/messages.info`
5. `tail -f /var/log/messages`
6. `journalctl _PID=1 -since "2025-02-01 09:00:00" --until "2025-02-01 15:00:00"`
7. `journalctl -b`
8. Запустите терминал и получите полномочия администратора: `su` – Создайте каталог для хранения записей журнала:
 - `mkdir -p /var/log/journal` Скорректируйте права доступа для каталога `/var/log/journal`, чтобы `journald` смог записывать в него информацию:
 - `chown root:systemd-journal /var/log/journal`
 - `chmod 2755 /var/log/journal` Для принятия изменений необходимо или перезагрузить систему (перезапустить службу `systemd-journald` недостаточно), или использовать команду:
 - `killall -USR1 systemd-journald`

4 Выводы

Получены навыки работы с журналами мониторинга различных событий в системе.