

Отчёт по лабораторной работе 7

Управление журналами событий в системе

Вишняков Родион Сергеевич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Вывод	16
4 Контрольные вопросы	17

Список иллюстраций

2.1	root	6
2.2	Мониторинг системных событий	6
2.3	Ввод команд	7
2.4	Мониторинг системных событий	7
2.5	Мониторинг сообщений безопасности	7
2.6	Apache	7
2.7	Запуск веб-службы	7
2.8	Сообщения об ошибках	8
2.9	Добавление строки	8
2.10	Файл мониторинга	8
2.11	Перезагрузка	8
2.12	Файл конфигурации	9
2.13	Перезапуск rsyslogd	9
2.14	Мониторинг отладочной информации	9
2.15	Ввод команды	9
2.16	Содержимое журнала	10
2.17	Содержимое журнала	10
2.18	Содержимое журнала	11
2.19	Содержимое журнала	11
2.20	Просмотр событий для UIDO	12
2.21	Содержимое журнала	12
2.22	Содержимое журнала	13
2.23	Содержимое журнала	13
2.24	Содержимое журнала	14
2.25	Содержимое журнала	14
2.26	Создание каталога	14
2.27	Права доступа	15
2.28	Принятие изменений	15

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

Получаем полномочия администратора

```
rodvish@rodvishh:~$ sudo -i  
[sudo] пароль для rodvish:  
root@rodvishh:~#
```

Рис. 2.1: root

Запускаю мониторинг системных событий в реальном времени

Рис. 2.2: Мониторинг системных событий

Ввожу предоставленные команды

```
root@rodvishh:~# logger hello
```

```
root@rodvishh:~#
```

Рис. 2.3: Ввод команд

Получаю сообщение из мониторинга событий

```
Oct 18 18:44:07 rodvishh systemd[1]: systemd-coredump@166-6571-0.service: Deactivated successfully.  
Oct 18 18:44:08 rodvishh root[6582]: hello
```

Рис. 2.4: Мониторинг системных событий

Просматриваю последний 20 строк из мониторинга сообщений безопасности

```
root@rodvishh:~# tail -n 20 /var/log/secure  
Oct 18 22:47:23 rodvishh gdm-password[4734]: gkr-pam: unlocked login keyring  
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on 0.0.0.0 port 22.  
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on :: port 22.  
Oct 18 18:28:10 rodvishh (systemd)[1218]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)  
Oct 18 18:28:10 rodvishh gdm-launch-environment[1198]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)  
Oct 18 18:29:08 rodvishh gdm-password[12300]: gkr-pam: unable to locate daemon control file  
Oct 18 18:29:08 rodvishh gdm-password[12300]: gkr-pam: stashed password to try later in open session  
Oct 18 18:29:08 rodvishh (systemd)[2313]: pam_unix(systemd-user:session): session opened for user rodvish(uid=1000) by rodvish(uid=0)  
Oct 18 18:29:08 rodvishh gdm-password[12300]: session opened for user rodvish(uid=1000) by rodvish(uid=0)  
Oct 18 18:29:08 rodvishh gdm-password[12300]: gkr-pam: gnome-keyring-dæmon started properly and unlocked keyring  
Oct 18 18:29:16 rodvishh gdm-launch-environment[1198]: pam_unix(gdm-launch-environment:session): session closed for user gdm  
Oct 18 18:39:11 rodvishh sudo[5716]: rodvish : TTY=pts/0 : PWD=/root : USER=root : COMMAND=/bin/bash  
Oct 18 18:39:11 rodvishh (systemd)[5729]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)  
Oct 18 18:39:11 rodvishh sudo[5716]: pam_unix(sudo-t:session): session opened for user root(uid=0) by rodvish(uid=1000)  
Oct 18 18:40:06 rodvishh sudo[5946]: rodvish : TTY=pts/2 : PWD=/root : USER=root : COMMAND=/bin/bash  
Oct 18 18:40:06 rodvishh sudo[5946]: pam_unix(sudo-t:session): session opened for user root(uid=0) by rodvish(uid=1000)  
Oct 18 18:41:54 rodvishh unix_chkpwd[6261]: password check failed for user (rodvish)  
Oct 18 18:41:54 rodvishh sudo[6252]: pam_unix(sudo-t:auth): authentication failure; logname=rodvish uid=1000 euid=0 tty=/dev/pts/4 ruser=rodvish rh  
ost= user=rodvish  
Oct 18 18:43:37 rodvishh sudo[6252]: rodvish : TTY=pts/4 : PWD=/root : USER=root : COMMAND=/bin/bash  
Oct 18 18:43:37 rodvishh sudo[6252]: pam_unix(sudo-t:session): session opened for user root(uid=0) by rodvish(uid=1000)  
root@rodvishh:~#
```

Рис. 2.5: Мониторинг сообщений безопасности

Устанавливаю Apache

```
root@rodvishh:~# dnf -y install httpd  
Rocky Linux 10 - BaseOS [====]
```

Рис. 2.6: Apache

Запускаю веб-службу

```
root@rodvishh:~# systemctl start httpd  
root@rodvishh:~# systemctl enable httpd  
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
```

Рис. 2.7: Запуск веб-службы

Просматриваю журнал сообщений об ошибках веб-службы

```
root@studubash:~# tail -f /var/log/httpd/error_log
[Sat Oct 18 18:48:25.446096 2025] [suexec:notice] [pid 7541:tid 7541] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Mon Oct 18 18:48:25.490553 2025] [httpd: Could not reliably determine the server's fully qualified domain name, using fe00::a00:27ff:fe3:bfbkengp03. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 18 18:48:25.490568 2025] [lbmethod_heartbeat:notice] [pid 7541:tid 7541] AH02282: No slotmem from mod_heartbeat
[Sat Oct 18 18:48:25.490968 2025] [systemd:notice] [pid 7541:tid 7541] SELinux policy enabled; httpd running as context system_u:object_r:httpd_t:s0
[Sat Oct 18 18:48:25.490974 2025] [mpm_event:notice] [pid 7541:tid 7541] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 18:48:25.494975 2025] [core:notice] [pid 7541:tid 7541] AH00054: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.8: Сообщения об ошибках

Добавляю предоставленную строку в конец

```
root@rodvishh:/etc/httpd/conf# echo "ErrorLog syslog:local1" >> /etc/httpd/conf/httpd.conf
root@rodvishh:/etc/httpd/conf#
```

Рис. 2.9: Добавление строки

Создаю файл мониторинга событий веб-службы и прописываю в нем следующую команду

```
root@rodvishh:/etc/httpd/conf# cd /etc/rsyslog.d
root@rodvishh:/etc/rsyslog.d# touch httpd.conf
root@rodvishh:/etc/rsyslog.d# local1.* -/var/log/httpd-error.log
bash: local1.*: команда не найдена...
root@rodvishh:/etc/rsyslog.d# nano httpd.conf
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.10: Файл мониторинга

Перезагружаю конфигурацию rsyslogd и веб-службу

```
root@rodvishh:/etc/rsyslog.d# systemctl restart rsyslog.service
root@rodvishh:/etc/rsyslog.d# systemctl restart httpd
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.11: Перезагрузка

Создаю файл конфигурации для мониторинга отладочной информации и ввожу следующую команду

```
root@rodrivishh:/etc/rsyslog.d# touch debug.conf
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" >
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" >
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Нет такого файла или каталога
root@rodrivishh:/etc/rsyslog.d# echo "*.*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@rodrivishh:/etc/rsyslog.d#
```

Рис. 2.12: Файл конфигурации

Перезапускаю rsyslogd

```
root@rodvishh:~# systemctl restart rsyslog.service  
root@rodvishh:~#
```

Рис. 2.13: Перезапуск rsyslogd

Запускаю мониторинг отладочной информации

Рис. 2.14: Мониторинг отладочной информации

Ввожу предоставленную команду

```
root@rodvishh:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.15: Ввод команды

Просматриваю содержимое журнала с событиями с момента последнего запуска системы

Рис. 2.16: Содержимое журнала

Просматриваю содержимое журнала без использования пейджера

```

#0 0x0000000000000000 n/a (n/a + 0x0)
#0x0000000000000000405123 n/a (n/a + 0x0)
#4 0x00007f4bc9b6430e __libc_start_main_(libc.so.6 + 0x2a30e)
#5 0x00007f4bc9b642c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
#6 0x0000000000444aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

OKT 18 19:20:36 rodvish systemd[1]: systemd-coredumpd[1726]: 12711._.service: Deactivated successfully.
OKT 18 19:20:41 rodvish kernel: traps: VBoxClient[12723] trap int 3 ip:41dd1b sp:7748bd1b4cd0 error: 0 in VBoxClient[1dd1b, 400000+bb000]
OKT 18 19:20:41 rodvish systemd-coredumpd[12727]: Process 12723 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
OKT 18 19:20:41 rodvish systemd[1]: Started systemd-coredumpd[682-12727-0].service - Process Core Dump (PID 12727/UID 0).
OKT 18 19:20:41 rodvish systemd-coredumpd[12728]: (:) Process 12723 (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 libX11-1.6.10-1.el10.x86_64
Module libXft.so.8 from rpm libXft-3.4.4-9.el10.x86_64
Module libXi.so.2 from rpm libXi-1.2.1-1.el10.x86_64
Module libXdamage.so.1 from rpm libXdamage-1.2.3-0.2.el10.x86_64
Stack trace of thread 12726:
#0 0x000000000041d1b n/a (n/a + 0x0)
#1 0x000000000041d1c n/a (n/a + 0x0)
#2 0x000000000045541c n/a (n/a + 0x0)
#3 0x0000000000435560 n/a (n/a + 0x0)
#4 0x00007f4bc9b6468 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f4bc9b3fc6c __clone3 ((libc.so.6 + 0x1056bc))

Stack trace of thread 12727:
#0 0x00007f4bc9b3d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000000434464 n/a (n/a + 0x0)
#2 0x0000000000450966 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f4bc9b6430e __libc_start_main_(libc.so.6 + 0x2a30e)
#5 0x00007f4bc9b642c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
#6 0x0000000000444aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

OKT 18 19:20:41 rodvish systemd[1]: systemd-coredumpd[682-12727-0].service: Deactivated successfully.
OKT 18 19:20:41 rodvish systemd[2313]: dbus-1.2-0.org.gnome.Nautilus@.service: Consumed 5.521s CPU time, 232.2M memory peak, 4K memory swap peak.
[rodrigo@rodvish ~]
```

Рис. 2.17: Содержимое журнала

Просматриваю содержимое в реальном времени

```

#3 0x000000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_main (libc.so.6 + 0x2a304
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 +
#6 0x0000000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

OKT 18 19:21:28 rodvishh systemd[1]: systemd-coredump@591-12846-0.service: Deactivated successfully.
OKT 18 19:21:33 rodvishh kernel: traps: VBoxClient[12860] trap int3 ip:41dd1b sp:7f48bd1c4cd0 error:0 in VBoxClient[12860]
OKT 18 19:21:33 rodvishh systemd-coredump[12861]: Process 12857 (VBoxClient) of user 1000 terminated abnormally with si
OKT 18 19:21:33 rodvishh systemd[1]: Started systemd-coredump@592-12861-0.service - Process Core Dump (PID 12861/UID 0)
OKT 18 19:21:33 rodvishh systemd-coredump[12862]: [.] Process 12857 (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 wayland-1.23.0-2.el10.x86_64
Stack trace of thread 12860:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x0000000000450401c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f48cb8ce68 start_thread (libc.so.6 + 0x94b68)
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 12857:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430e __libc_start_main (libc.so.6 + 0x2a304
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 +
#6 0x0000000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

OKT 18 19:21:33 rodvishh systemd[1]: systemd-coredump@592-12861-0.service: Deactivated successfully.

```

Рис. 2.18: Содержимое журнала

Просматриваю конкретные параметры

```

OKT 18 18:27:57 rodvishh systemd-journald[200]: Journal started
OKT 18 18:27:57 rodvishh systemd-journald[256]: Runtime Journal (/run/log/journal/ee3d489206ca4b85bcaa
OKT 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'msr' is built in
OKT 18 18:27:57 rodvishh systemd-modules-load[257]: Inserted module 'fuse'
OKT 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_alua' is built in
OKT 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_emc' is built in
OKT 18 18:27:57 rodvishh systemd-modules-load[257]: Module 'scsi_dh_rdac' is built in
OKT 18 18:27:57 rodvishh systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static
OKT 18 18:27:57 rodvishh systemd[1]: Starting systemd-sysusers.service - Create System Users...
OKT 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'nobody' with GID 65534.
OKT 18 18:27:57 rodvishh systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
OKT 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'users' with GID 100.
OKT 18 18:27:57 rodvishh systemd-sysusers[270]: Creating group 'systemd-journal' with GID 190.
OKT 18 18:27:57 rodvishh systemd[1]: Finished systemd-sysusers.service - Create System Users.
OKT 18 18:27:57 rodvishh systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Devic
OKT 18 18:27:58 rodvishh systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
OKT 18 18:27:58 rodvishh systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline pa
OKT 18 18:27:58 rodvishh systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
OKT 18 18:27:58 rodvishh dracut-cmdline[280]: dracut-105-4.el10_0
OKT 18 18:27:58 rodvishh dracut-cmdline[280]: Using kernel command line parameters: BOOT_IMAGE=(hd0
OKT 18 18:27:58 rodvishh systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Devic
OKT 18 18:27:58 rodvishh systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
OKT 18 18:27:58 rodvishh systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
OKT 18 18:27:58 rodvishh systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
OKT 18 18:27:58 rodvishh systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device Ev
OKT 18 18:27:58 rodvishh systemd-udevd[379]: Using default interface naming scheme 'rhel-10.0'.
OKT 18 18:27:58 rodvishh systemd[1]: Started systemd-udevd.service - Rule-based Manager for Device Eve
OKT 18 18:27:58 rodvishh systemd[1]: dracut-pre-trigger.service - dracut pre-trigger hook was skipped
OKT 18 18:27:58 rodvishh systemd[1]: Starting systemd-udev-trigger.service - Coldplug All udev Devices
OKT 18 18:27:58 rodvishh systemd[1]: Created slice system-modprobe.slice - Slice /system/modprobe.
OKT 18 18:27:58 rodvishh systemd[1]: Starting modprobe@configfs.service - Load Kernel Module configfs.
OKT 18 18:27:58 rodvishh systemd[1]: Finished systemd-udev-trigger.service - Coldplug All udev Devices
OKT 18 18:27:58 rodvishh systemd[1]: Starting dracut-initqueue.service - dracut initqueue hook...
OKT 18 18:27:58 rodvishh systemd[1]: Starting plymouth-start.service - Show Plymouth Boot Screen...
OKT 18 18:27:58 rodvishh systemd[1]: modprobe@configfs.service: Deactivated successfully.
OKT 18 18:27:58 rodvishh systemd[1]: Finished modprobe@configfs.service - Load Kernel Module configfs.
OKT 18 18:27:58 rodvishh systemd[1]: Received SIGRTMIN+20 from PID 401 (plymouthd).

```

Рис. 2.19: Содержимое журнала

Просматриваю события для UIDO

```

OKT 18 19:23:07 rodvishh systemd[1]: Process 13078 (VBoxClient) of user 1000 terminated
OKT 18 19:23:07 rodvishh systemd[1]: Started systemd-coredump@610-13082-0.service - Process Core Dump
OKT 18 19:23:07 rodvishh systemd-coredump[13083]: [..] Process 13078 (VBoxClient) of user 1000 dumped core

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.2-1.el10.x86_64

Stack trace of thread 13081:
#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 0x00007f48cb8ceb68 start_thread (libc.so.6 + 0x105)
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x105)

Stack trace of thread 13078:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x103)
#1 0x00000000004344e2 n/a (n/a + 0x0)
#2 0x0000000000450066 n/a (n/a + 0x0)
#3 0x0000000000405123 n/a (n/a + 0x0)
#4 0x00007f48cb86430c __libc_start_main (libc.so.6 + 0x105)
#5 0x00007f48cb8643c9 __libc_start_main@@GLIBC_2.2.5 (libc.so.6 + 0x105)
#6 0x00000000004044aa n/a (n/a + 0x0)

ELF object binary architecture: AMD x86-64

OKT 18 19:23:07 rodvishh systemd[1]: systemd-coredump@610-13082-0.service: Deactivated successfully.
OKT 18 19:23:12 rodvishh kernel: traps: VBoxClient[13093] trap int3 ip:41dd1b sp:7f48b814cd0 error:0
OKT 18 19:23:12 rodvishh systemd-coredump[13094]: Process 13090 (VBoxClient) of user 1000 terminated
OKT 18 19:23:12 rodvishh systemd[1]: Started systemd-coredump@611-13094-0.service - Process Core Dump
OKT 18 19:23:12 rodvishh systemd-coredump[13095]: [..] Process 13090 (VBoxClient) of user 1000 dumped core

Module libXau.so.6 from rpm libXau-1.0.11-8.el10.
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.2-1.el10.x86_64

lines 1-38

```

Рис. 2.20: Просмотр событий для UIDO

Просматриваю последний 20 строк журнала

```

OKT 18 18:27:55 rodvishh kernel: vmmgfx 0000:00:02.0: [drm] Linux fb configuration is likely wrong
OKT 18 18:27:59 rodvishh kernel: vmmgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graph
OKT 18 18:28:07 rodvishh kernel: Warning: Unmaintained driver is detected: e1000
OKT 18 18:28:08 rodvishh alsactl[889]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to i
OKT 18 18:28:09 rodvishh kernel: Warning: Unmaintained driver is detected: ip_set
OKT 18 18:28:21 rodvishh rsyslogd[1290]: imjournal: fscancf on state file '/var/lib/rsyslog/imjournal.s
OKT 18 18:28:21 rodvishh rsyslogd[1290]: imjournal: ignoring invalid state file /var/lib/rsyslog/imjou
OKT 18 18:29:08 rodvishh gdm-password[2300]: gkr-pam: unable to locate daemon control file
OKT 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-gnome\x2dkkeyring\x2dpkcs11-2426.scope
OKT 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-gnome\x2dkkeyring\x2dssh-2421.scope -
OKT 18 18:29:12 rodvishh systemd[2313]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2437.scope - App
OKT 18 18:29:24 rodvishh systemd-coredump[3151]: [..] Process 3138 (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 wayland-1.2-1.el10.x86_64

Stack trace of thread 3142:
#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 0x00007f48cb8ceb68 start_thread (libc.so.6 + 0x105)
#5 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x105)

Stack trace of thread 3139:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x103)
#1 0x00000000004343c30 n/a (n/a + 0x0)
#2 0x0000000000450bf8 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 0x00007f48cb8ceb68 start_thread (libc.so.6 + 0x105)
#7 0x00007f48cb93f6bc __clone3 (libc.so.6 + 0x105)

Stack trace of thread 3140:

```

Рис. 2.21: Содержимое журнала

Просматриваю только сообщения об ошибках

```
OKT 18 18:27:57 rodvishh kernel: Command 'ether-boot-image-(hd0,gpt2)/vmlinuz2-0.12.0-55.52.1.61v_0.x86
OKT 18 18:27:57 rodvishh kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
OKT 18 18:27:57 rodvishh kernel: BIOS-provided physical RAM map:
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000000fc00-0x000000000009ffff] reserved
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x000000000000f000-0x00000000000fffff] reserved
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfffffff] usable
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000dff0000-0x00000000fec00000] ACPI data
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000fec0000-0x00000000fec000ff] reserved
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000fee0000-0x00000000fee0ffff] reserved
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x00000000ffffffffff] reserved
OKT 18 18:27:57 rodvishh kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff] usable
OKT 18 18:27:57 rodvishh kernel: NX (Execute Disable) protection: active
OKT 18 18:27:57 rodvishh kernel: APIC: Static calls initialized
OKT 18 18:27:57 rodvishh kernel: SMBIOS 2.5 present.
OKT 18 18:27:57 rodvishh kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
OKT 18 18:27:57 rodvishh kernel: DMI: Memory slots populated: 0/0
OKT 18 18:27:57 rodvishh kernel: Hypervisor detected: KVM
OKT 18 18:27:57 rodvishh kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
OKT 18 18:27:57 rodvishh kernel: kvm-clock: using sched offset of 12642684577 cycles
OKT 18 18:27:57 rodvishh kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e
OKT 18 18:27:57 rodvishh kernel: tsc: Detected 3293.814 MHz processor
OKT 18 18:27:57 rodvishh kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
OKT 18 18:27:57 rodvishh kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
OKT 18 18:27:57 rodvishh kernel: last_pfn = 0x120000 max_arch_pfn = 0x40000000
OKT 18 18:27:57 rodvishh kernel: total RAM covered: 4096M
OKT 18 18:27:57 rodvishh kernel: Found optimal setting for mtrr clean up
OKT 18 18:27:57 rodvishh kernel: gran_size: 64K      chunk_size: 1G      num_reg: 3      loc
OKT 18 18:27:57 rodvishh kernel: MTTR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 vari
OKT 18 18:27:57 rodvishh kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
OKT 18 18:27:57 rodvishh kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> reserved
OKT 18 18:27:57 rodvishh kernel: last_pfn = 0xe00000 max_arch_pfn = 0x40000000
OKT 18 18:27:57 rodvishh kernel: found SMP MP-table at [mem 0x00009fb0-0x00009fbff]
OKT 18 18:27:57 rodvishh kernel: RAMDISK: [mem 0x33e23000-0x35f09fff]
OKT 18 18:27:57 rodvishh kernel: ACPI: Early table checksum verification disabled
OKT 18 18:27:57 rodvishh kernel: ACPI: RSDP 0x0000000000E0000 000024 (v02 VBOX )
OKT 18 18:27:57 rodvishh kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX  VBOXXSDT 00000001 AS
lines 1-38
```

Рис. 2.22: Содержимое журнала

Просматриваю все сообщения вчерашнего дня

```
OKT 18 18:27:59 rodvishh kernel: vmmwgfx 0000:00:00.0: [drm] known hw configuration is likely broken.
OKT 18 18:27:59 rodvishh kernel: vmmwgfx 0000:00:00.0: [drm] *ERROR* Please switch to a supported graphics device to avoid problems.
OKT 18 18:28:07 rodvishh kernel: Warning: Unmaintained driver is detected: el1000
OKT 18 18:28:08 rodvishh alsactl[899]: alsa-lib main.c:1954([snd_use_case_mgr_open]) error: failed to import hw:0 use case configuration -2
OKT 18 18:28:09 rodvishh kernel: Warning: Unmaintained driver is detected: ip_set
OKT 18 18:28:10 rodvishh syslogd[1290]: [kern/note] fsck on state file '/var/lib/syslogd/journal.state' failed [v8.2412.0-1.el10 try https://www.fedoraproject.org/wiki/Cloud/Upgrading_Fedora#fsck]
OKT 18 18:28:21 rodvishh syslogd[1290]: [kern/note] ignoring invalid state file '/var/lib/syslogd/journal.state' [v8.2412.0-1.el10]
OKT 18 18:28:21 rodvishh gdm-pulseaudio[2300]: pulse unable to locate configuration file /etc/pulse/client.conf
OKT 18 18:29:12 rodvishh systemd[2113]: Failed to start app-gnome-gnome-vzddekeyring@2dpkcs11-2426.scope - Application launched by gnome-session-binary
OKT 18 18:29:12 rodvishh systemd[2113]: Failed to start app-gnome-gnome-vzddekeyring@2dssh-2421.scope - Application launched by gnome-session-binary
OKT 18 18:29:12 rodvishh systemd[2113]: Failed to start app-gnome-dg@xd2duser@2ddirs-2427.scope - Application launched by gnome-session-binary
OKT 18 18:29:24 rodvishh systemd-coredump[3151]: [?] Process 3138 (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 libXi.so.6 from rpm libXi-1.8.10-1.el10.x86_64
Module liblffi.so.8 from rpm liblffi-3.4-4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.23-0-2.el10.x86_64
Stack trace of thread 3142:
#0 0x000000000041d1b n/a (n/a + 0x0)
#1 0x000000000041d24 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f48cb93f6bc start_thread (libc.so.6 + 0x94b68)
#5 0x00007f48cb93f6bc _clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 3139:
#0 0x00007f48cb93d4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x00000000004509b n/a (n/a + 0x0)
#3 0x0000000000435564 n/a (n/a + 0x0)
#4 0x000000000045641c n/a (n/a + 0x0)
#5 0x00000000004355d0 n/a (n/a + 0x0)
#6 0x00007f48cb93f6bc start_thread (libc.so.6 + 0x94b68)
#7 0x00007f48cb93f6bc _clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 3140:
lines 1-38
```

Рис. 2.23: Содержимое журнала

Просматриваю сообщения с ошибкой приоритета со вчерашнего дня

```

Sat 2025-10-18 18:27:57.911107 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=1;b=8548b42490354a79a0b0a266beafbe4;m=15ed24;t=641707eb0a043;x=d313ed4408
._SOURCE_BOOTTIME_TIMESTAMP=0
._SOURCE_MONOTONIC_TIMESTAMP=0
._TRANSPORT=kernel
.PRIORITY=5
.SYSLOG_FACILITY=0
.SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@iadi1-prod-build001.bld.eqi.rockylinux.org) (gcc (GCC) 14.2.1 20250110 (Red Hat 14
._BOOT_ID=8548b42490354a79a0b0a266beafbe4
._MACHINE_ID=e3d489206ca4b85bc当地50f2993d21da
._HOSTNAME=rodvishh
._RUNTIME_SCOPE=initrd
.PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.32.1.el10_0.x86_64 root=/dev/mapper/r1_vbox-root ro resume=UUID=fad36b5c-0c75-4fe
Sat 2025-10-18 18:27:57.911162 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=3;b=8548b42490354a79a0b0a266beafbe4;m=15ed5d;t=641707eb0a07a;x=a475f4e35
._SOURCE_BOOTTIME_TIMESTAMP=0
._SOURCE_MONOTONIC_TIMESTAMP=0
._TRANSPORT=kernel
.PRIORITY=5
.SYSLOG_FACILITY=0
.SYSLOG_IDENTIFIER=kernel
._BOOT_ID=8548b42490354a79a0b0a266beafbe4
._MACHINE_ID=e3d489206ca4b85bc当地50f2993d21da
._HOSTNAME=rodvishh
._RUNTIME_SCOPE=initrd
.PRIORITY=6
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sat 2025-10-18 18:27:57.911171 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=4;b=8548b42490354a79a0b0a266beafbe4;m=15ed63;t=641707eb0a083;x=dec775efad
._SOURCE_BOOTTIME_TIMESTAMP=0

```

Рис. 2.24: Содержимое журнала

Просматриваю дополнительную информацию о модуле sshd

```

MESSAGE=Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@iadi1-prod-build001.bld.eqi.rockylinux.org) (gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-1), GNU ld version
._BOOT_ID=8548b42490354a79a0b0a266beafbe4
._MACHINE_ID=e3d489206ca4b85bc当地50f2993d1da
._HOSTNAME=rodvishh
._RUNTIME_SCOPE=initrd
.PRIORITY=4
MESSAGE=Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.32.1.el10_0.x86_64 root=/dev/mapper/r1_vbox-root ro resume=UUID=fad36b5c-0c75-4fe2-ba2f-abd4877e7f72 rd
Sat 2025-10-18 18:27:57.911133 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=2;b=8548b42490354a79a0b0a266beafbe4;m=15ed3d;t=641707eb0a05d;x=5793ab561703e379]
._SOURCE_BOOTTIME_TIMESTAMP=0
._SOURCE_MONOTONIC_TIMESTAMP=0
._TRANSPORT=kernel
.PRIORITY=5
.SYSLOG_FACILITY=0
.SYSLOG_IDENTIFIER=kernel
._BOOT_ID=8548b42490354a79a0b0a266beafbe4
._MACHINE_ID=e3d489206ca4b85bc当地50f2993d21da
._HOSTNAME=rodvishh
._RUNTIME_SCOPE=initrd
.PRIORITY=4
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sat 2025-10-18 18:27:57.911162 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=3;b=8548b42490354a79a0b0a266beafbe4;m=15ed5d;t=641707eb0a07a;x=a475f4e35
._SOURCE_BOOTTIME_TIMESTAMP=0
._SOURCE_MONOTONIC_TIMESTAMP=0
._TRANSPORT=kernel
.PRIORITY=5
.SYSLOG_FACILITY=0
.SYSLOG_IDENTIFIER=kernel
._BOOT_ID=8548b42490354a79a0b0a266beafbe4
._MACHINE_ID=e3d489206ca4b85bc当地50f2993d1da
._HOSTNAME=rodvishh
._RUNTIME_SCOPE=initrd
.PRIORITY=6
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sat 2025-10-18 18:27:57.911171 MSK [s=f21c5c9c32ec4654a5e004ece3a77c5;i=4;b=8548b42490354a79a0b0a266beafbe4;m=15ed63;t=641707eb0a083;x=dec775efad9085e]
._SOURCE_BOOTTIME_TIMESTAMP=0
root@rodvishh:~# journalctl _SYSTEMD_UNIT=sshd.service
Oct 18 18:28:09 rodvishh (sshd)[1154]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on 0.0.0.0 port 22.
Oct 18 18:28:09 rodvishh sshd[1154]: Server listening on :: port 22.
root@rodvishh:~#

```

Рис. 2.25: Содержимое журнала

Создаю каталог для хранения записей журнала

```

root@rodvishh:/etc/rsyslog.d# mkdir -p /var/log/journal
root@rodvishh:/etc/rsyslog.d#

```

Рис. 2.26: Создание каталога

Корректирую права доступа

```
root@rodvishh:/etc/rsyslog.d# chown root:systemd-journal /var/log/journal  
root@rodvishh:/etc/rsyslog.d# chmod 2755 /var/log/journal  
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.27: Права доступа

Для принятия изменений ввожу следующую команду

```
root@rodvishh:/etc/rsyslog.d# killall -USR1 systemd-journald  
root@rodvishh:/etc/rsyslog.d#
```

Рис. 2.28: Принятие изменений

3 Вывод

Мы получили навыки работы с журналами мониторинга различных событий в системе.

4 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd? /etc/rsyslog.conf
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?
`/var/log/auth.log` (в Red Hat-системах — `/var/log/secure`)
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов? Еженедельно
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?
`tail -f` для файлов журналов или `journalctl -f` для systemd
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 вас видеть сообщения journald после последней перезагрузки системы? `journalctl -b`
8. Какая процедура позволяет сделать журнал journald постоянным? Создать директорию `/var/log/journal` и перезапустить systemd-journald