

Отчёт по лабораторной работе №7

Дисциплина: Основы администрирования операционных сетей

Бызова Мария Олеговна

Содержание

1	Цель работы	6
2	Задание	7
3	Выполнение лабораторной работы	8
3.1	Мониторинг журнала системных событий в реальном времени . .	8
3.2	Изменение правил rsyslog.conf	10
3.3	Использование journalctl	13
3.4	Постоянный журнал journald	17
3.5	Ответы на контрольные вопросы	17
4	Выводы	21
	Список литературы	22

Список иллюстраций

3.1	Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.	8
3.2	Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора. .	9
3.3	Новое сообщение в мониторинге событий во второй вкладке терминала.	9
3.4	Ввод в третьей вкладке терминала.	9
3.5	Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга сообщений безопасности (последние 20 строк).	10
3.6	Установка Apsache.	10
3.7	Запуск веб-службы.	10
3.8	Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала.	11
3.9	Получение в третьей вкладке терминала полномочия администратора, открытие файла <code>httpd.conf</code> на редактирование.	11
3.10	Добавление строки в файл и сохранение.	11
3.11	Создание в каталоге <code>/etc/rsyslog.d</code> файла мониторинга событий веб-службы и открытие его на редактирование.	12
3.12	Добавление строки в файл и сохранение.	12
3.13	Открытие первой вкладки терминала и перезагрузка конфигурации <code>rsyslogd</code> и веб-службы.	12
3.14	Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.	12
3.15	Открытие первой вкладки терминала и перезапуск <code>rsyslogd</code>	13
3.16	Открытие второй вкладки терминала и запуск мониторинга отладочной информации.	13
3.17	Открытие третьей вкладки терминала и ввод команды.	13
3.18	Просмотр сообщения отладки и закрытие трассировки файла журнала.	13
3.19	Открытие второй вкладки терминала и просмотр содержимого журнала с событиями с момента последнего запуска системы.	14
3.20	Просмотр содержимого журнала без использования пейджера. . .	14

3.21 Режим просмотра журнала в реальном времени и прерывание просмотра.	14
3.22 Просмотр событий для UID0.	15
3.23 Отображение последних 20 строк журнала.	15
3.24 Просмотр только сообщений об ошибках.	15
3.25 Просмотр всех сообщений со вчерашнего дня.	16
3.26 Просмотр сообщений с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Просмотр детальной информации. .	16
3.27 Просмотр дополнительной информации о модуле sshd.	16
3.28 Запуск терминала и получение полномочий администратора, создание каталог для хранения записей журнала, корректировка прав доступа для каталога /var/log/journal, принятия изменений, просмотр сообщения журнала с момента последней перезагрузки. . .	17

Список таблиц

1 Цель работы

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

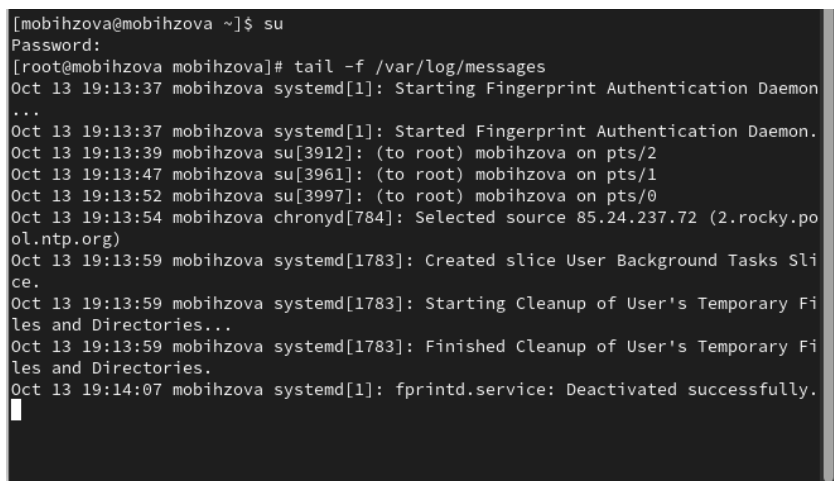
2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с `journalctl` (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с `journalld` (см. раздел 7.4.4).

3 Выполнение лабораторной работы

3.1 Мониторинг журнала системных событий в реальном времени

Для начала запустим три вкладки терминала и в каждом из них получим полномочия администратора: `su -`. На второй вкладке терминала запустим мониторинг системных событий в реальном времени: `tail -f /var/log/messages` (рис. 3.1).

A screenshot of a terminal window with a dark background and light-colored text. The terminal shows a user named 'mobihzova' at a prompt. They enter 'su' to become root. Then they enter 'tail -f /var/log/messages' to view system logs. The logs show various system events, including the start of the Fingerprint Authentication Daemon, user logins, and the deactivation of the fprintd.service. The terminal output is as follows:

```
[mobihzova@mobihzova ~]$ su
Password:
[root@mobihzova mobihzova]# tail -f /var/log/messages
Oct 13 19:13:37 mobihzova systemd[1]: Starting Fingerprint Authentication Daemon
...
Oct 13 19:13:37 mobihzova systemd[1]: Started Fingerprint Authentication Daemon.
Oct 13 19:13:39 mobihzova su[3912]: (to root) mobihzova on pts/2
Oct 13 19:13:47 mobihzova su[3961]: (to root) mobihzova on pts/1
Oct 13 19:13:52 mobihzova su[3997]: (to root) mobihzova on pts/0
Oct 13 19:13:54 mobihzova chronyd[784]: Selected source 85.24.237.72 (2.rocky.p
ol.ntp.org)
Oct 13 19:13:59 mobihzova systemd[1783]: Created slice User Background Tasks Sli
ce.
Oct 13 19:13:59 mobihzova systemd[1783]: Starting Cleanup of User's Temporary Fi
les and Directories...
Oct 13 19:13:59 mobihzova systemd[1783]: Finished Cleanup of User's Temporary Fi
les and Directories.
Oct 13 19:14:07 mobihzova systemd[1]: fprintd.service: Deactivated successfully.
```

Рис. 3.1: Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.

В третьей вкладке терминала вернёмся к учётной записи своего пользователя (нажав `Ctrl + d`) и попробуем получить полномочия администратора, но при этом вводим неправильный пароль (рис. 3.2).


```
[mobihzova@mobihzova ~]$ su
Password:
[root@mobihzova mobihzova]#
exit
[mobihzova@mobihzova ~]$ su
Password:
su: Authentication failure
[mobihzova@mobihzova ~]$
```

Рис. 3.2: Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора.

Обратим внимание, что во второй вкладке терминала с мониторингом событий появилось сообщение «FAILED SU (to root) mobihzova on pts/2». Отображаемые на экране сообщения также фиксируются в файле /var/log/messages (рис. 3.3).

```
Oct 13 19:15:42 mobihzova systemd[1]: Started Fingerprint Authentication Daemon.
Oct 13 19:15:47 mobihzova su[4058]: FAILED SU (to root) mobihzova on pts/2
Oct 13 19:16:13 mobihzova systemd[1]: fprintd.service: Deactivated successfully.
```

Рис. 3.3: Новое сообщение в мониторинге событий во второй вкладке терминала.

В третьей вкладке терминала из оболочки пользователя введём: logger hello (рис. 3.4).

```
[mobihzova@mobihzova ~]$ logger hello
[mobihzova@mobihzova ~]$
```

Рис. 3.4: Ввод в третьей вкладке терминала.

Далее возвращаемся во вторую вкладку терминала с мониторингом событий и видим сообщение, которое также будет зафиксировано в файле /var/log/messages («hello»). В этой же вкладке терминала с мониторингом остановим трассировку файла сообщений мониторинга реального времени, используя Ctrl + c. Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов): tail -n 20 /var/log/secure. Мы видим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды su - (рис. 3.5).

```

Oct 13 19:17:07 mobihzova mobihzova[4088]: hello
^C
[root@mobihzova mobihzova]# tail -n 20 /var/log/secure
Oct 13 19:08:24 mobihzova polkitd[743]: Acquired the name org.freedesktop.PolicyKit1 on the system
bus
Oct 13 19:08:25 mobihzova sshd[1091]: Server listening on 0.0.0.0 port 22.
Oct 13 19:08:25 mobihzova sshd[1091]: Server listening on :: port 22.
Oct 13 19:08:25 mobihzova systemd[1132]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 13 19:08:25 mobihzova gdm-launch-environment[1118]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 13 19:08:27 mobihzova polkitd[743]: Registered Authentication Agent for unix-session:cl (system
bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent
, locale en_US.UTF-8)
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: unable to locate daemon control file
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: stashed password to try later in open sessi
on
Oct 13 19:08:35 mobihzova systemd[1783]: pam_unix(systemd-user:session): session opened for user mo
bihzova(uid=1000) by mobihzova(uid=0)
Oct 13 19:08:35 mobihzova gdm-password[1769]: pam_unix(gdm-password:session): session opened for u
ser mobihzova(uid=1000) by mobihzova(uid=0)
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: gnome-keyring-daemon started properly and u
nlocked keyring
Oct 13 19:08:36 mobihzova polkitd[743]: Unregistered Authentication Agent for unix-session:cl (syst

```

Рис. 3.5: Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга сообщений безопасности (последние 20 строк).

3.2 Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache: `dnf -y install httpd` (рис. 3.6).

```

[root@mobihzova mobihzova]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               682 B/s | 4.1 kB    00:06
Rocky Linux 9 - BaseOS                               85% [=====] 189 kB/s | 1.9 MB    00:01 ETA

```

Рис. 3.6: Установка Apache.

После окончания процесса установки запустим веб-службу: `systemctl start httpd` и `systemctl enable httpd` (рис. 3.7).

```

[root@mobihzova mobihzova]# systemctl start httpd
[root@mobihzova mobihzova]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@mobihzova mobihzova]#

```

Рис. 3.7: Запуск веб-службы.

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: `tail -f /var/log/httpd/error_log`. Чтобы закрыть трассировку файла журнала, используем `Ctrl + c` (рис. 3.8).

```
[root@mobihzova mobihzova]# tail -f /var/log/httpd/error_log
[Sun Oct 13 19:20:01.066569 2024] [core:notice] [pid 4765:tid 4765] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Sun Oct 13 19:20:01.066988 2024] [suexec:notice] [pid 4765:tid 4765] AH01232: suEXEC mechanism enabled (wrapper: /u
sr/sbin/suexec)
[Sun Oct 13 19:20:01.204376 2024] [lbmethod_heartbeat:notice] [pid 4765:tid 4765] AH02282: No slotmem from mod_heart
monitor
[Sun Oct 13 19:20:01.206076 2024] [mpm_event:notice] [pid 4765:tid 4765] AH00489: Apache/2.4.57 (Rocky Linux) config
ured -- resuming normal operations
[Sun Oct 13 19:20:01.206094 2024] [core:notice] [pid 4765:tid 4765] AH00094: Command line: '/usr/sbin/httpd -D FOREG
ROUND'
```

Рис. 3.8: Просмотр журнала сообщений об ошибках веб-службы, закрытие трас-сировки файла журнала.

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавляем следующую строку: ErrorLog syslog:local (рис. 3.9, рис. 3.10).

Здесь local0 — local7 — это «настраиваемые» средства (объекты), которые syslog предоставляет пользователю для регистрации событий приложения в системном журнале.

```
[mobihzova@mobihzova ~]$ su
Password:
[root@mobihzova mobihzova]# mcedit /etc/httpd/conf/httpd.conf
```

Рис. 3.9: Получение в третьей вкладке терминала полномочия администратора, открытие файла httpd.conf на редактирование.

```
#EnableMMAP off
#EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9Undo 10Quit
```

Рис. 3.10: Добавление строки в файл и сохранение.

В каталоге /etc/rsyslog.d создаём файл мониторинга событий веб-службы:

```
cd /etc/rsyslog.d touch httpd.conf
```

Открыв его на редактирование, пропишем в нём local1.* -/var/log/httpd-error.log (Рис. 2.7). Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpderror.log (рис. 3.11, рис. 3.12).

```
[root@mobihzova mobihzova]# cd /etc/rsyslog.d
[root@mobihzova rsyslog.d]# touch httpd.conf
[root@mobihzova rsyslog.d]# mcedit httpd.conf
```

Рис. 3.11: Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование.

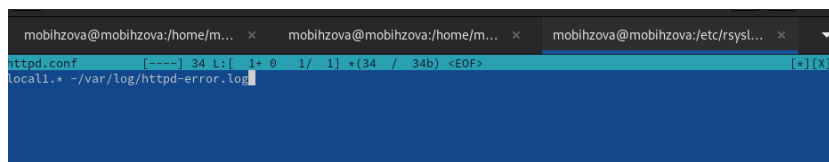


Рис. 3.12: Добавление строки в файл и сохранение.

Перейдём в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу:

```
systemctl restart rsyslog.service systemctl restart httpd
```

Все сообщения об ошибках веб-службы теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени, используя команду tail с соответствующими параметрами, или непосредственно просматривая указанный файл. (рис. 3.13).

```
[root@mobihzova mobihzova]# systemctl restart rsyslog.service
[root@mobihzova mobihzova]# systemctl restart httpd
```

Рис. 3.13: Открытие первой вкладки терминала и перезагрузка конфигурации rsyslogd и веб-службы.

В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации:

```
cd /etc/rsyslog.d touch debug.conf
```

В этом же терминале вводим: echo “*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf (рис. 3.14).

```
[root@mobihzova rsyslog.d]# cd /etc/rsyslog.d
[root@mobihzova rsyslog.d]# touch debug.conf
[root@mobihzova rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
```

Рис. 3.14: Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.

В первой вкладке терминала снова перезапустим rsyslogd: `systemctl restart rsyslog.service` (рис. 3.15).

```
[root@mobihzova mobihzova]# systemctl restart rsyslog.service
[root@mobihzova mobihzova]#
```

Рис. 3.15: Открытие первой вкладки терминала и перезапуск rsyslogd.

Во второй вкладке терминала запустим мониторинг отладочной информации: `tail -f /var/log/messages-debug` (рис. 3.16).

```
[root@mobihzova mobihzova]# tail -f /var/log/messages-debug
Oct 13 19:29:23 mobihzova systemd[1]: Stopping System Logging Service...
Oct 13 19:29:23 mobihzova rsyslogd[5468]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5468" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 13 19:29:23 mobihzova systemd[1]: rsyslog.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova systemd[1]: Stopped System Logging Service.
Oct 13 19:29:23 mobihzova systemd[1]: Starting System Logging Service...
Oct 13 19:29:23 mobihzova rsyslogd[5694]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5694" x-info="https://www.rsyslog.com"] start
Oct 13 19:29:23 mobihzova systemd[1]: Started System Logging Service.
Oct 13 19:29:23 mobihzova rsyslogd[5694]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

Рис. 3.16: Открытие второй вкладки терминала и запуск мониторинга отладочной информации.

В третьей вкладке терминала введём: `logger -p daemon.debug "Daemon Debug Message"` (рис. 3.17).

```
[root@mobihzova rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
[root@mobihzova rsyslog.d]#
```

Рис. 3.17: Открытие третьей вкладки терминала и ввод команды.

В терминале с мониторингом посмотрим сообщение отладки. Чтобы закрыть трассировку файла журнала, используем `Ctrl + c` (рис. 3.18).

```
Oct 13 19:29:23 mobihzova rsyslogd[5694]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 13 19:30:27 mobihzova root[5714]: Daemon Debug Message
```

Рис. 3.18: Просмотр сообщения отладки и закрытие трассировки файла журнала.

3.3 Использование journalctl

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: `journalctl`. Для пролистывания журнала

можно использовать или Enter (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра используется q (рис. 3.19).

```
[root@mobihzova mobihzova]# journalctl
Oct 13 19:08:21 mobihzova.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build)
Oct 13 19:08:21 mobihzova.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux
Oct 13 19:08:21 mobihzova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x86_64
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using xstate
Oct 13 19:08:21 mobihzova.localdomain kernel: signal: max sigframe size: 1776
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-provided physical RAM map:
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000000fffff] usable
```

Рис. 3.19: Открытие второй вкладки терминала и просмотр содержимого журнала с событиями с момента последнего запуска системы.

Посмотрим содержимое журнала без использования пейджера: journalctl --no-pager (рис. 3.20).

```
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 19:27:12 mobihzova.localdomain httpd[5482]: Server configured, listening on: port 80
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 19:28:57 mobihzova.localdomain PackageKit[4414]: daemon quit
Oct 13 19:28:57 mobihzova.localdomain systemd[1]: packagekit.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Stopping System Logging Service...
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5468]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5468" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Stopped System Logging Service.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Starting System Logging Service...
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5694]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5694" x-info="https://www.rsyslog.com"] start
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Started System Logging Service.
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5694]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 13 19:30:27 mobihzova.localdomain root[5714]: Daemon Debug Message
[root@mobihzova mobihzova]# journalctl --no-pager
```

Рис. 3.20: Просмотр содержимого журнала без использования пейджера.

Режим просмотра журнала в реальном времени: journalctl -f. Для прерывания просмотра: Ctrl + c (рис. 3.21).

```
[root@mobihzova mobihzova]# journalctl -f
Oct 13 19:28:57 mobihzova.localdomain systemd[1]: packagekit.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Stopping System Logging Service...
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5468]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5468" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Stopped System Logging Service.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Starting System Logging Service...
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5694]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="5694" x-info="https://www.rsyslog.com"] start
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Started System Logging Service.
Oct 13 19:29:23 mobihzova.localdomain rsyslogd[5694]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 13 19:30:27 mobihzova.localdomain root[5714]: Daemon Debug Message
^C
```

Рис. 3.21: Режим просмотра журнала в реальном времени и прерывание просмотра.

Посмотрим события для UID0: journalctl _UID=0 (рис. 3.22).

```
[root@mobihzova mobihzova]# journalctl _UID=0
Oct 13 19:08:21 mobihzova.localdomain systemd-journald[226]: Journal started
Oct 13 19:08:21 mobihzova.localdomain systemd-journald[226]: Runtime Journal (/run/log/journal/754f3d55d9704718a00d5
Oct 13 19:08:21 mobihzova.localdomain systemd-sysusers[228]: Creating group 'nobody' with GID 65534.
Oct 13 19:08:21 mobihzova.localdomain systemd-sysusers[228]: Creating group 'users' with GID 100.
Oct 13 19:08:21 mobihzova.localdomain systemd-sysusers[228]: Creating group 'dbus' with GID 81.
Oct 13 19:08:21 mobihzova.localdomain systemd-sysusers[228]: Creating user 'dbus' (System Message Bus) with UID 81
Oct 13 19:08:21 mobihzova.localdomain systemd[1]: Starting Create Static Device Nodes in /dev...
Oct 13 19:08:21 mobihzova.localdomain systemd[1]: Starting Create Volatile Files and Directories...
Oct 13 19:08:21 mobihzova.localdomain systemd[1]: Finished Create Static Device Nodes in /dev.
Oct 13 19:08:21 mobihzova.localdomain systemd[1]: Finished Create Volatile Files and Directories.
Oct 13 19:08:21 mobihzova.localdomain systemd-modules-load[227]: Inserted module 'fuse'
Oct 13 19:08:21 mobihzova.localdomain systemd-modules-load[227]: Module 'msr' is built in
```

Рис. 3.22: Просмотр событий для UID=0.

Для отображения последних 20 строк журнала введём: `journalctl -n 20` (рис. 3.23).

```
[root@mobihzova mobihzova]# journalctl -n 20
Oct 13 19:27:03 mobihzova.localdomain rsyslogd[5468]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid=5
Oct 13 19:27:03 mobihzova.localdomain systemd[1]: Started System Logging Service.
Oct 13 19:27:03 mobihzova.localdomain rsyslogd[5468]: imjournal: journal files changed, reloading... [v8.2310.0-4.
Oct 13 19:27:11 mobihzova.localdomain systemd[1]: Stopping The Apache HTTP Server...
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: httpd.service: Deactivated successfully.
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: Stopped The Apache HTTP Server.
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 19:27:12 mobihzova.localdomain httpd[5482]: Server configured, listening on: port 80
Oct 13 19:27:12 mobihzova.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 19:28:57 mobihzova.localdomain PackageKit[4414]: daemon quit
Oct 13 19:28:57 mobihzova.localdomain systemd[1]: packagekit.service: Deactivated successfully.
Oct 13 19:29:23 mobihzova.localdomain systemd[1]: Stopping System Logging Service...
```

Рис. 3.23: Отображение последних 20 строк журнала.

Для просмотра только сообщений об ошибках введём: `journalctl -p err` (рис. 3.24).

```
[root@mobihzova mobihzova]# journalctl -p err
Oct 13 19:08:21 mobihzova.localdomain systemd[1]: Invalid DMI field header.
Oct 13 19:08:21 mobihzova.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 13 19:08:22 mobihzova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an a
Oct 13 19:08:22 mobihzova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broke
Oct 13 19:08:22 mobihzova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graph
Oct 13 19:08:23 mobihzova.localdomain systemd[1]: Invalid DMI field header.
Oct 13 19:08:23 mobihzova.localdomain systemd-udevd[632]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only netw
Oct 13 19:08:23 mobihzova.localdomain systemd-udevd[625]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only netw
Oct 13 19:08:24 mobihzova.localdomain alsactl[773]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 13 19:08:25 mobihzova.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 13 19:08:35 mobihzova.localdomain gdm-password[1769]: gkr-pam: unable to locate daemon control file
```

Рис. 3.24: Просмотр только сообщений об ошибках.

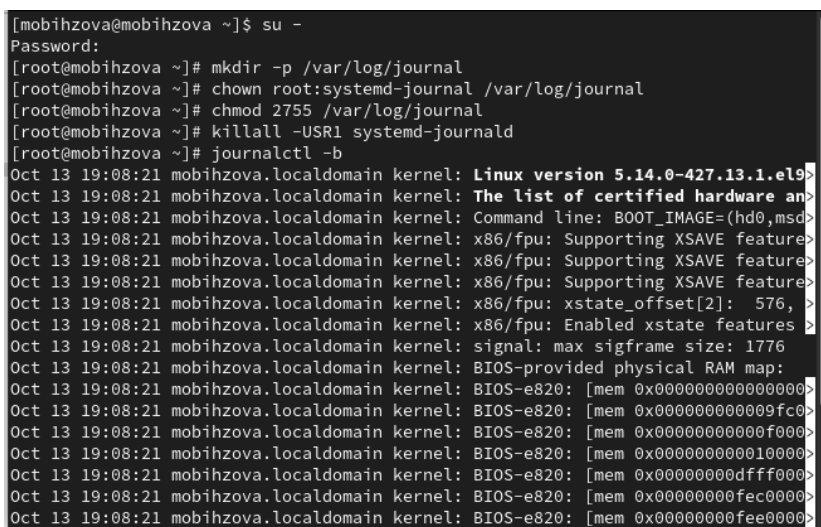
Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, мы можем использовать параметры `–since` и `–until`. Обе опции принимают параметр времени в формате `YYYY-MM-DD hh:mm:ss`. Кроме того, мы можем использовать `yesterday`, `today` и `tomorrow` в качестве параметров. Например, для просмотра всех сообщений со вчерашнего дня введём: `journalctl –since yesterday` (рис. 3.25).

3.4 Постоянный журнал journald

Запустим терминал и получим полномочия администратора: `su -`. Далее создадим каталог для хранения записей журнала: `mkdir -p /var/log/journal` и скорректируем 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 использовать команду: `killall -USR1 systemd-journald`. Журнал `systemd` теперь постоянный. Если мы хотим видеть сообщения журнала с момента последней перезагрузки, используем: `journalctl -b` (рис. 3.28).

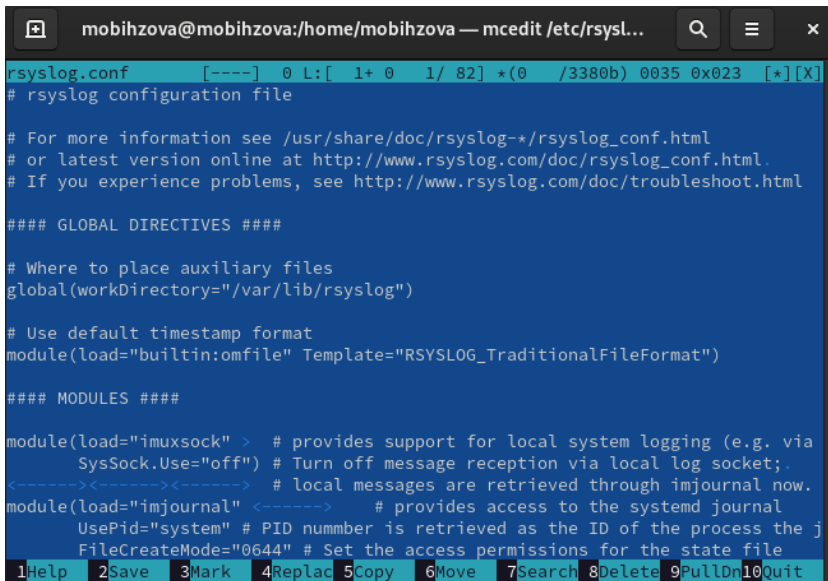


```
[mobihzova@mobihzova ~]$ su -
Password:
[root@mobihzova ~]# mkdir -p /var/log/journal
[root@mobihzova ~]# chown root:systemd-journal /var/log/journal
[root@mobihzova ~]# chmod 2755 /var/log/journal
[root@mobihzova ~]# killall -USR1 systemd-journald
[root@mobihzova ~]# journalctl -b
Oct 13 19:08:21 mobihzova.localdomain kernel: Linux version 5.14.0-427.13.1.el9>
Oct 13 19:08:21 mobihzova.localdomain kernel: The list of certified hardware an>
Oct 13 19:08:21 mobihzova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msd>
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature>
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature>
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Supporting XSAVE feature>
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: xstate_offset[2]: 576,>
Oct 13 19:08:21 mobihzova.localdomain kernel: x86/fpu: Enabled xstate features >
Oct 13 19:08:21 mobihzova.localdomain kernel: signal: max sigframe size: 1776
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-provided physical RAM map:
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc0>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x000000000000f000>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x0000000000010000>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x000000000dfff000>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000>
Oct 13 19:08:21 mobihzova.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000>
```

Рис. 3.28: Запуск терминала и получение полномочий администратора, создание каталог для хранения записей журнала, корректировка прав доступа для каталога `/var/log/journal`, принятия изменений, просмотр сообщения журнала с момента последней перезагрузки.

3.5 Ответы на контрольные вопросы

1. Какой файл используется для настройки `rsyslogd`? `/etc/rsyslog.conf`



```
rsyslog.conf  [----] 0 L:[ 1+ 0 1/ 82] *(0 /3380b) 0035 0x023 [*][X]
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog_conf.html.
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

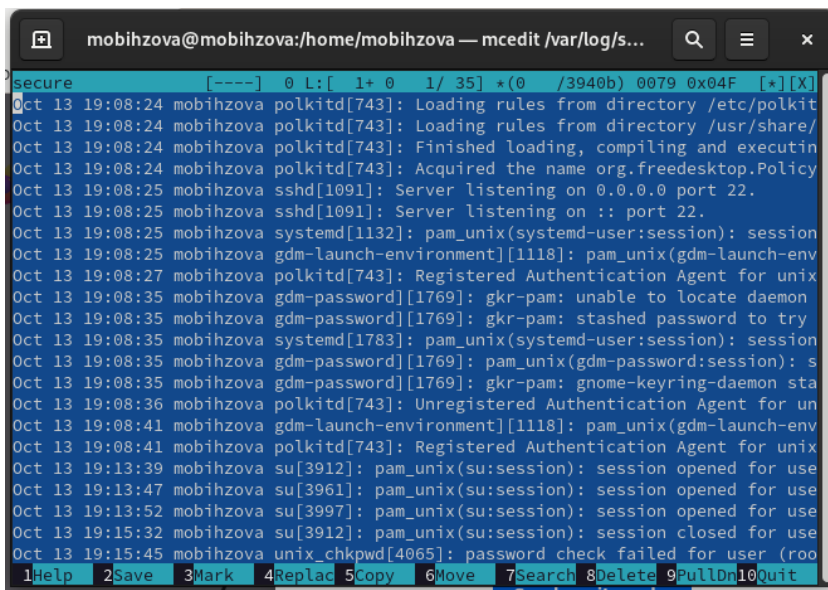
# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

#### MODULES ####

module(load="imuxsock" > # provides support for local system logging (e.g. via
SysSock.Use="off") # Turn off message reception via local log socket;
<-----><-----><-----> # local messages are retrieved through imjournal now.
module(load="imjournal" <-----> # provides access to the systemd journal
UsePid="system" # PID number is retrieved as the ID of the process the j
FileCreateMode="0644" # Set the access permissions for the state file

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? /var/log/secure



```
secure  [----] 0 L:[ 1+ 0 1/ 35] *(0 /3940b) 0079 0x04F [*][X]
Oct 13 19:08:24 mobihzova polkitd[743]: Loading rules from directory /etc/polkit
Oct 13 19:08:24 mobihzova polkitd[743]: Loading rules from directory /usr/share/
Oct 13 19:08:24 mobihzova polkitd[743]: Finished loading, compiling and executin
Oct 13 19:08:24 mobihzova polkitd[743]: Acquired the name org.freedesktop.Policy
Oct 13 19:08:25 mobihzova sshd[1091]: Server listening on 0.0.0.0 port 22.
Oct 13 19:08:25 mobihzova sshd[1091]: Server listening on :: port 22.
Oct 13 19:08:25 mobihzova systemd[1132]: pam_unix(systemd-user:session): session
Oct 13 19:08:25 mobihzova gdm-launch-environment[1118]: pam_unix(gdm-launch-env
Oct 13 19:08:27 mobihzova polkitd[743]: Registered Authentication Agent for unix
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: unable to locate daemon
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: stashed password to try
Oct 13 19:08:35 mobihzova systemd[1783]: pam_unix(systemd-user:session): session
Oct 13 19:08:35 mobihzova gdm-password[1769]: pam_unix(gdm-password:session): s
Oct 13 19:08:35 mobihzova gdm-password[1769]: gkr-pam: gnome-keyring-daemon sta
Oct 13 19:08:36 mobihzova polkitd[743]: Unregistered Authentication Agent for un
Oct 13 19:08:41 mobihzova gdm-launch-environment[1118]: pam_unix(gdm-launch-env
Oct 13 19:08:41 mobihzova polkitd[743]: Registered Authentication Agent for unix
Oct 13 19:13:39 mobihzova su[3912]: pam_unix(su:session): session opened for use
Oct 13 19:13:47 mobihzova su[3961]: pam_unix(su:session): session opened for use
Oct 13 19:13:52 mobihzova su[3997]: pam_unix(su:session): session opened for use
Oct 13 19:15:32 mobihzova su[3912]: pam_unix(su:session): session closed for use
Oct 13 19:15:45 mobihzova unix_chkpwd[4065]: password check failed for user (roo
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

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

```
logrotate.conf [---] 0 L: [ 1+ 0 1/ 24] *(0 / 496b) 0035 0x023 [*][X]
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d
```

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 /var/log/messages

```
[root@mobihzova mobihzova]# tail -f /var/log/messages
Oct 13 19:41:55 mobihzova systemd[1783]: gnome-terminal-server.service: Consumed 10.801s CPU time.
Oct 13 19:42:00 mobihzova systemd[1783]: app-gnome-gnome\x2dcontrol\x2dcenter-2832.scope: Consumed 1.615s CPU time.
Oct 13 19:42:01 mobihzova systemd[1783]: Started Application launched by gnome-shell.
Oct 13 19:42:01 mobihzova systemd[1783]: Starting GNOME Terminal Server...
Oct 13 19:42:01 mobihzova systemd[1783]: Started GNOME Terminal Server.
Oct 13 19:42:01 mobihzova systemd[1783]: Started VTE child process 5970 launched by gnome-terminal-server process 5952.
Oct 13 19:42:05 mobihzova systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 13 19:42:05 mobihzova systemd[1]: Started Fingerprint Authentication Daemon.
Oct 13 19:42:07 mobihzova su[5998]: (to root) mobihzova on pts/0
Oct 13 19:42:36 mobihzova systemd[1]: fprintd.service: Deactivated successfully.
```

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 "2022-02-01 09:00:00" --until "2022-02-01 15:00:00"
7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы? journalctl -b
8. Какая процедура позволяет сделать журнал journald постоянным?

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

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

4 Выводы

В ходе выполнения лабораторной работы были получены навыки работы с журналами мониторинга различных событий в системе.

Список литературы

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — (Классика Computer Science).
4. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
5. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т.Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.