

Отчёт по лабораторной работе №7

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

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	15
3.4	Постоянный журнал journald	18
4	Контрольные вопросы + ответы	20
5	Выводы	24
6	Список литературы	25

Список иллюстраций

3.1	Режим суперпользователя	8
3.2	Мониторинг системных событий в реальном времени	8
3.3	Попытка получить права суперпользователя	9
3.4	Сообщение о неудачной попытке получить права root	9
3.5	Послание тестового сообщения “hello”	9
3.6	Тестовое сообщение “hello”	9
3.7	Мониторинг сообщений безопасности	10
3.8	Установка Apache	10
3.9	Запуск службы httpd	11
3.10	Журнал сообщений об ошибках веб-службы httpd	11
3.11	Получение прав пользователя root и открытие файла /etc/httpd/conf/httpd.conf	11
3.12	Редактирование файла /etc/httpd/conf/httpd.conf	12
3.13	Создание файла мониторинга событий веб-службы	12
3.14	Открытие файла /etc/rsyslog.d/httpd.conf	13
3.15	Редактирование файла /etc/rsyslog.d/httpd.conf	13
3.16	Перезагрузка конфигурации rsyslogd и веб-службы	13
3.17	Создание отдельного файла конфигурации для мониторинга отладочной информации	13
3.18	Ввод нужной команды	13
3.19	Перезапуск rsyslogd	14
3.20	Мониторинг отладочной информации	14
3.21	Создание тестового сообщения уровня debug	14
3.22	Тестовое сообщение уровня debug	14
3.23	Просмотр содержимого журнала событий с момента последнего запуска системы	15
3.24	Просмотр содержимого журнала событий без использования пейджера	15
3.25	Просмотр журнала в реальном времени	15
3.26	Просмотр конкретных параметров. Надеюсь это то))))	16
3.27	События UID0	16
3.28	Просмотр последних 20 строк журнала	16
3.29	Просмотр сообщений только об ошибках	17
3.30	Просмотр всех сообщений со вчерашнего дня	17
3.31	Просмотр всех сообщений с ошибкой приоритета со вчерашнего дня	17
3.32	Просмотр детальной информации	18
3.33	Просмотр дополнительной информации о модуле sshd	18
3.34	Режим root	18

3.35	Создание каталога для хранения записей журнала	18
3.36	Установление прав доступа для каталога /var/log/journal	19
3.37	Команда killall -USR1 systemd-journald	19
3.38	Сообщения журнала с момента последней перезагрузки	19
4.1	Вопрос №1	20
4.2	Вопрос №2	21
4.3	Вопрос №3	21
4.4	Вопрос №5	22
4.5	Вопрос №7	22
4.6	Вопрос №8 (1)	23
4.7	Вопрос №8 (2)	23
4.8	Вопрос №8 (3)	23

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Задание

1. Продемонстрировать навыки работы с журналом мониторинга событий в реальном времени
2. Продемонстрировать навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы
3. Продемонстрировать навыки работы с `journalctl`
4. Продемонстрировать навыки работы с `journal`

3 Выполнение лабораторной работы

3.1 Мониторинг журнала системных событий в реальном времени

Запускаем три вкладки терминала и в каждой из них получаем полномочия суперпользователя, используя *su* - (рис. 3.1)

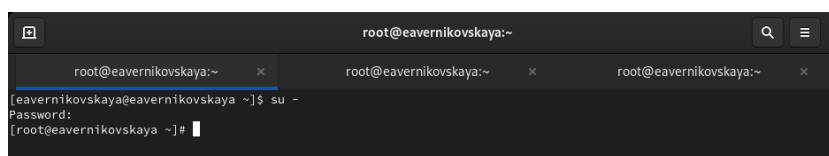


Рис. 3.1: Режим суперпользователя

На второй вкладке терминала запустите мониторинг системных событий в реальном времени, с помощью *tail -f /var/log/messages* (рис. 3.2)

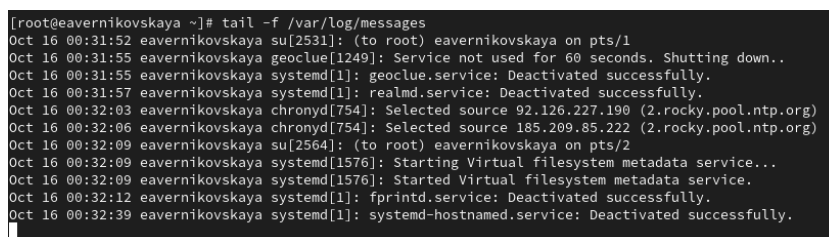


Рис. 3.2: Мониторинг системных событий в реальном времени

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя (для этого нажимаем *ctrl+d*) и пробуем получить полномочия администратора, но на этот раз вводим неправильный пароль (рис. 3.3)


```
[root@eavernikovskaya ~]#  
logout  
[eavernikovskaya@eavernikovskaya ~]$ su -  
Password:  
su: Authentication failure  
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.3: Попытка получить права суперпользователя

Во второй вкладке терминала с мониторингом событий после неудачной попытки получить права администратора появится сообщение «FAILED SU (to root) username ...» (рис. 3.4)

```
Oct 16 00:33:31 eavernikovskaya su[2622]: FAILED SU (to root) eavernikovskaya on pts/2
```

Рис. 3.4: Сообщение о неудачной попытке получить права root

В третьей вкладке терминала из оболочки пользователя вводим *logger hello* (рис. 3.5)

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

Рис. 3.5: Послание тестового сообщения “hello”

Во второй вкладке терминала с мониторингом событий мы увидим сообщение, которое до этого написали с помощью *logger* (рис. 3.6)

```
Oct 16 00:34:30 eavernikovskaya eavernikovskaya[2644]: hello
```

Рис. 3.6: Тестовое сообщение “hello”

Во второй вкладке терминала с мониторингом останавливаем трассировку файла сообщений мониторинга реального времени, используя *ctrl+c*, а затем запускаем мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов), с помощью *tail -n 20 /var/log/secure*. Там мы увидим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды *su* (рис. 3.7)

```

[root@eavernikovskaya ~]# tail -n 20 /var/log/secure
Oct 16 00:30:49 eavernikovskaya polkitd[732]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Oct 16 00:30:50 eavernikovskaya sshd[1075]: Server listening on 0.0.0.0 port 22.
Oct 16 00:30:50 eavernikovskaya sshd[1075]: Server listening on :: port 22.
Oct 16 00:30:50 eavernikovskaya systemd[1106]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 16 00:30:51 eavernikovskaya gdm-launch-environment[1098]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 16 00:30:53 eavernikovskaya polkitd[732]: 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 16 00:31:06 eavernikovskaya gdm-password[1559]: gkr-pam: unable to locate daemon control file
Oct 16 00:31:06 eavernikovskaya gdm-password[1559]: gkr-pam: stashed password to try later in open session
Oct 16 00:31:06 eavernikovskaya systemd[1576]: pam_unix(systemd-user:session): session opened for user eavernikovskaya(uid=1000) by eavernikovskaya(uid=0)
Oct 16 00:31:06 eavernikovskaya gdm-password[1559]: pam_unix(gdm-password:session): session opened for user eavernikovskaya(uid=1000) by eavernikovskaya(uid=0)
Oct 16 00:31:06 eavernikovskaya gdm-password[1559]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 16 00:31:08 eavernikovskaya polkitd[732]: Registered Authentication Agent for unix-session:2 (system bus name :1.68 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 16 00:31:12 eavernikovskaya gdm-launch-environment[1098]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 16 00:31:13 eavernikovskaya polkitd[732]: 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 16 00:31:45 eavernikovskaya su[2494]: pam_unix(su-l:session): session opened for user root(uid=0) by eavernikovskaya(uid=1000)
Oct 16 00:31:52 eavernikovskaya su[2531]: pam_unix(su-l:session): session opened for user root(uid=0) by eavernikovskaya(uid=1000)
Oct 16 00:32:09 eavernikovskaya su[2564]: pam_unix(su-l:session): session opened for user root(uid=0) by eavernikovskaya(uid=1000)
Oct 16 00:33:04 eavernikovskaya su[2564]: pam_unix(su-l:session): session closed for user root
Oct 16 00:33:29 eavernikovskaya unix_chkpwd[2629]: password check failed for user (root)
Oct 16 00:33:29 eavernikovskaya su[2622]: pam_unix(su-l:auth): authentication failure; logname=eavernikovskaya uid=1000 euid=0 tty=/dev/pts/2 ruser=eavernikovskaya rhost= user=root
[root@eavernikovskaya ~]#

```

Рис. 3.7: Мониторинг сообщений безопасности

3.2 Изменение правил rsyslog.conf

По умолчанию веб-служба не регистрирует свои сообщения через rsyslog, а пишет свой собственный журнал (в каталоге /var/log/httpd). Настроим регистрацию сообщений веб-службы через syslog, создав правило, регистрирующее отладочные сообщения в отдельном лог-файле.

В первой вкладке терминала установим Apache командой *dnf -y install httpd* (рис. 3.8)

```

[root@eavernikovskaya ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               6.9 kB/s | 4.1 kB  00:00
Rocky Linux 9 - BaseOS                               2.5 MB/s | 2.3 MB  00:00
Rocky Linux 9 - AppStream                             10 kB/s | 4.5 kB  00:00
Rocky Linux 9 - AppStream                             4.4 MB/s | 8.0 MB  00:01
Rocky Linux 9 - Extras                                6.4 kB/s | 2.9 kB  00:00
Rocky Linux 9 - Extras                                19 kB/s | 15 kB   00:00
Dependencies resolved.
=====
Package Architecture Version Repository Size
-----
Installing:
httpd      x86_64      2.4.57-11.el9_4.1 appstream 44 k
Installing dependencies:

```

Рис. 3.8: Установка Apache

После окончания процесса установки запускаем веб-службу командами *systemctl start httpd* и *systemctl enable httpd* (рис. 3.9)

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

Рис. 3.9: Запуск службы httpd

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы, с помощью `tail -f /var/log/httpd/error_log`. Для закрытия используем `ctrl+c` (рис. 3.10)

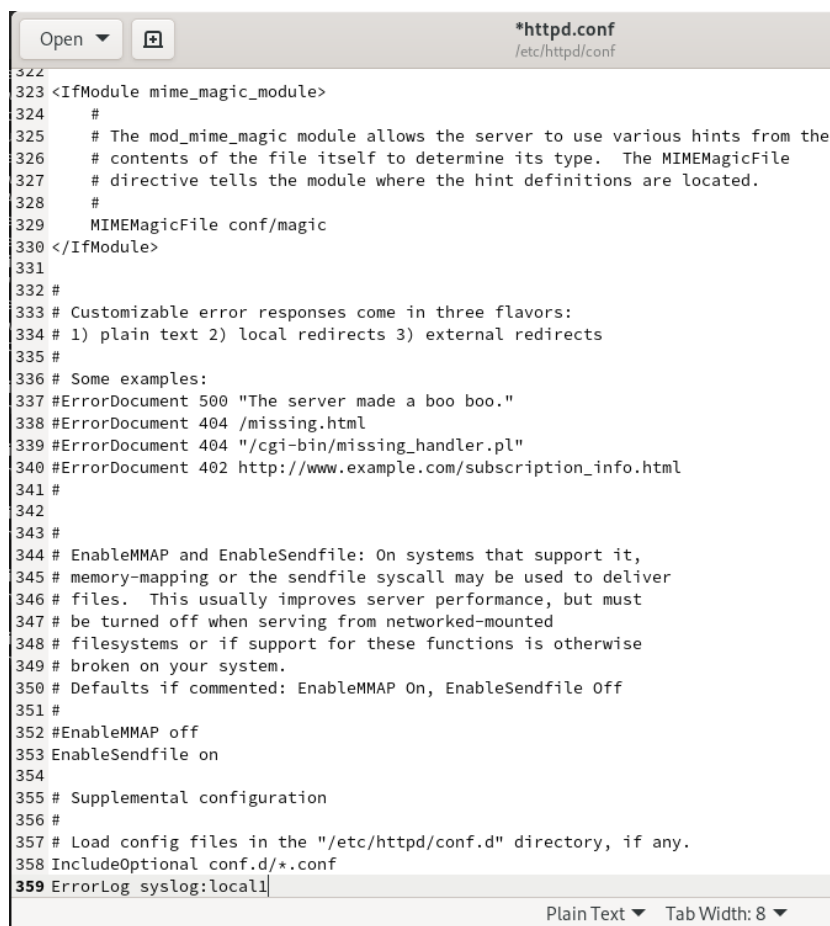
```
[root@eavernikovskaya ~]# tail -f /var/log/httpd/error_log
[Wed Oct 16 00:37:25.225485 2024] [core:notice] [pid 22150:tid 22150] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Wed Oct 16 00:37:25.227480 2024] [suexec:notice] [pid 22150:tid 22150] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Oct 16 00:37:25.262153 2024] [lbmethod_heartbeat:notice] [pid 22150:tid 22150] AH02282: No slotmem from mod_heartmonitor
[Wed Oct 16 00:37:25.273337 2024] [mpm_event:notice] [pid 22150:tid 22150] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Wed Oct 16 00:37:25.273373 2024] [core:notice] [pid 22150:tid 22150] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
^C
[root@eavernikovskaya ~]#
```

Рис. 3.10: Журнал сообщений об ошибках веб-службы httpd

В третьей вкладке терминала получаем полномочия администратора и в файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавляем строку `ErrorLog syslog:local1`. Добавление этой строки в конец файла конфигурации изменит способ регистрации ошибок веб-сервера. Ошибки будут отправляться на систему журналирования через syslog в локальную категорию `local1` (рис. 3.11), (рис. 3.12)

```
[eavernikovskaya@eavernikovskaya ~]$ su -
Password:
[root@eavernikovskaya ~]# gedit /etc/httpd/conf/httpd.conf
```

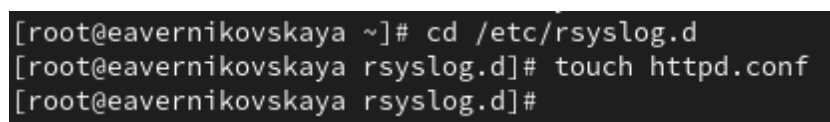
Рис. 3.11: Получение прав пользователя root и открытие файла `/etc/httpd/conf/httpd.conf`



```
322
323 <IfModule mime_magic_module>
324     #
325     # The mod_mime_magic module allows the server to use various hints from the
326     # contents of the file itself to determine its type. The MIMEMagicFile
327     # directive tells the module where the hint definitions are located.
328     #
329     MIMEMagicFile conf/magic
330 </IfModule>
331
332 #
333 # Customizable error responses come in three flavors:
334 # 1) plain text 2) local redirects 3) external redirects
335 #
336 # Some examples:
337 #ErrorDocument 500 "The server made a boo boo."
338 #ErrorDocument 404 /missing.html
339 #ErrorDocument 404 "/cgi-bin/missing_handler.pl"
340 #ErrorDocument 402 http://www.example.com/subscription_info.html
341 #
342
343 #
344 # EnableMMAP and EnableSendfile: On systems that support it,
345 # memory-mapping or the sendfile syscall may be used to deliver
346 # files. This usually improves server performance, but must
347 # be turned off when serving from networked-mounted
348 # filesystems or if support for these functions is otherwise
349 # broken on your system.
350 # Defaults if commented: EnableMMAP On, EnableSendfile Off
351 #
352 #EnableMMAP off
353 EnableSendfile on
354
355 # Supplemental configuration
356 #
357 # Load config files in the "/etc/httpd/conf.d" directory, if any.
358 IncludeOptional conf.d/*.conf
359 ErrorLog syslog:local1
```

Рис. 3.12: Редактирование файла /etc/httpd/conf/httpd.conf

Далее в каталоге /etc/rsyslog.d создаём файл мониторинга событий веб-службы (рис. 3.13)



```
[root@eavernikovskaya ~]# cd /etc/rsyslog.d
[root@eavernikovskaya rsyslog.d]# touch httpd.conf
[root@eavernikovskaya rsyslog.d]#
```

Рис. 3.13: Создание файла мониторинга событий веб-службы

Открыв его на редактирование, прописываем в нём строку local1.* - /var/log/httpd-error.log. Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log (рис. 3.14), (рис. 3.15)

```
[root@eavernikovskaya rsyslog.d]# gedit httpd.conf
```

Рис. 3.14: Открытие файла /etc/rsyslog.d/httpd.conf



Рис. 3.15: Редактирование файла /etc/rsyslog.d/httpd.conf

Переходим в первую вкладку терминала и перезагружаем конфигурацию rsyslogd и веб-службу командой `systemctl restart`. 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. 3.16)

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

Рис. 3.16: Перезагрузка конфигурации rsyslogd и веб-службы

В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации (рис. 3.17)

```
[root@eavernikovskaya log]# cd /etc/rsyslog.d
[root@eavernikovskaya rsyslog.d]# touch debug.conf
[root@eavernikovskaya rsyslog.d]#
```

Рис. 3.17: Создание отдельного файла конфигурации для мониторинга отладочной информации

В этом же терминале пишем команду `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf` (рис. 3.18)

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

Рис. 3.18: Ввод нужной команды

В первой вкладке терминала снова перезапускаем rsyslogd (рис. 3.19)

```
[root@eavernikovskaya ~]# systemctl restart rsyslog.service
[root@eavernikovskaya ~]#
```

Рис. 3.19: Перезапуск rsyslogd

Во второй вкладке терминала запускаем мониторинг отладочной информации с помощью *tail -f /var/log/messages-debug* (рис. 3.20)

```
[root@eavernikovskaya ~]# tail -f /var/log/messages-debug
Oct 16 00:48:16 eavernikovskaya systemd[1]: Stopping System Logging Service...
Oct 16 00:48:17 eavernikovskaya rsyslogd[41635]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="41635" x
-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 16 00:48:17 eavernikovskaya systemd[1]: rsyslog.service: Deactivated successfully.
Oct 16 00:48:17 eavernikovskaya systemd[1]: Stopped System Logging Service.
Oct 16 00:48:17 eavernikovskaya systemd[1]: Starting System Logging Service...
Oct 16 00:48:17 eavernikovskaya rsyslogd[41918]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="41918" x
-info="https://www.rsyslog.com"] start
Oct 16 00:48:17 eavernikovskaya systemd[1]: Started System Logging Service.
Oct 16 00:48:17 eavernikovskaya rsyslogd[41918]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try h
tps://www.rsyslog.com/e/0 ]
```

Рис. 3.20: Мониторинг отладочной информации

В третьей вкладке терминала вводим *logger -p daemon.debug "Daemon Debug Message"* (рис. 3.21)

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

Рис. 3.21: Создание тестового сообщения уровня debug

После этого мы увидим в терминале с мониторингом отладочной информации наше сообщение, которое мы создали с помощью *logger* (рис. 3.22)

```
[root@eavernikovskaya ~]# tail -f /var/log/messages-debug
Oct 16 00:48:16 eavernikovskaya systemd[1]: Stopping System Logging Service...
Oct 16 00:48:17 eavernikovskaya rsyslogd[41635]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="41635" x
-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 16 00:48:17 eavernikovskaya systemd[1]: rsyslog.service: Deactivated successfully.
Oct 16 00:48:17 eavernikovskaya systemd[1]: Stopped System Logging Service.
Oct 16 00:48:17 eavernikovskaya systemd[1]: Starting System Logging Service...
Oct 16 00:48:17 eavernikovskaya rsyslogd[41918]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="41918" x
-info="https://www.rsyslog.com"] start
Oct 16 00:48:17 eavernikovskaya systemd[1]: Started System Logging Service.
Oct 16 00:48:17 eavernikovskaya rsyslogd[41918]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try h
tps://www.rsyslog.com/e/0 ]
Oct 16 00:49:06 eavernikovskaya root[41931]: Daemon Debug Message
AC
[root@eavernikovskaya ~]#
```

Рис. 3.22: Тестовое сообщение уровня debug

3.3 Использование journalctl

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы с помощью *journalctl* (рис. 3.23)

```
[root@eavernikovskaya ~]# journalctl
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-bu
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: The list of certified hardware and cloud instances for Enterprise L
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, u
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: signal: max sigframe size: 1776
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-provided physical RAM map:
```

Рис. 3.23: Просмотр содержимого журнала событий с момента последнего запуска системы

Далее посмотрим содержимое журнала без использования пейджера с помощью *journalctl --no-pager*. Это означает, что вывод сообщений будет отображаться сразу весь, без возможности прокручивания содержимого (рис. 3.24)

```
[root@eavernikovskaya ~]# journalctl --no-pager
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-bui
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: The list of certified hardware and cloud instances for Enterprise L
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
```

Рис. 3.24: Просмотр содержимого журнала событий без использования пейджера

Далее посмотрим журнал в реальном времени командой *journalctl -f*. Для прерывания просмотра используем также *ctrl+c* (рис. 3.25)

```
[root@eavernikovskaya ~]# journalctl -f
Oct 16 00:45:45 eavernikovskaya.localdomain systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Dea
ctivated successfully.
Oct 16 00:48:16 eavernikovskaya.localdomain systemd[1]: Stopping System Logging Service...
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41635]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-p
id="41635" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Stopped System Logging Service.
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Starting System Logging Service...
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41918]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-p
id="41918" x-info="https://www.rsyslog.com"] start
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Started System Logging Service.
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41918]: imjournal: journal files changed, reloading... [v8.2310.0
-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 16 00:49:06 eavernikovskaya.localdomain root[41931]: Daemon Debug Message
^C
[root@eavernikovskaya ~]#
```

Рис. 3.25: Просмотр журнала в реальном времени

Для использования фильтрации просмотра конкретных параметров журнала вводим *journalctl* и дважды нажимаем на клавишу *Tab* (рис. 3.26)

```
[root@eavernikovskaya ~]# journalctl
Display all 108 possibilities? (y or n)
_AUDIT_LOGINUID=
_AUDIT_SESSION=
_AVAILABLE=
_AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
_CODE_FILE=
_CODE_FUNC=
_CODE_LINE=
_COMM=
_CPU_USAGE_NSEC=
_CURRENT_USE=
_CURRENT_USE_PRETTY=
_KERNEL_SUBSYSTEM=
_KERNEL_USEC=
_LEADER=
_LIMIT=
_LIMIT_PRETTY=
_MACHINE_ID=
_MAX_USE=
_MAX_USE_PRETTY=
_MESSAGE=
_MESSAGE_ID=
_NM_DEVICE=
_NM_LOG_DOMAINS=
_NM_LOG_LEVEL=
_PID=
```

Рис. 3.26: Просмотр конкретных параметров. Надеюсь это то))))

Смотрим события UID0 командой `*journalctl _UID=0*` (рис. 3.27)

```
[root@eavernikovskaya ~]# journalctl _UID=0
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-journald[227]: Journal started
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-journald[227]: Runtime Journal (/run/log/journal/b9202024839e4f958b
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-sysusers[229]: Creating group 'nobody' with GID 65534.
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-modules-load[228]: Inserted module 'fuse'
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-modules-load[228]: Module 'msr' is built in
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-sysusers[229]: Creating group 'users' with GID 100.
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-sysusers[229]: Creating group 'dbus' with GID 81.
Oct 16 00:30:44 eavernikovskaya.localdomain systemd-sysusers[229]: Creating user 'dbus' (System Message Bus) with UID 0
```

Рис. 3.27: События UID0

Для отображения последних 20 строк журнала вводим команду `journalctl -n 20` (рис. 3.28)

```
[root@eavernikovskaya ~]# journalctl -n 20
Oct 16 00:44:01 eavernikovskaya.localdomain httpd[41643]: Server configured, listening on: port 80
Oct 16 00:44:01 eavernikovskaya.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 16 00:45:29 eavernikovskaya.localdomain systemd[1576]: Started VTE child process 41863 launched by gnome-terminal-
Oct 16 00:45:45 eavernikovskaya.localdomain systemd[1]: Starting Cleanup of Temporary Directories...
Oct 16 00:45:45 eavernikovskaya.localdomain systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Oct 16 00:45:45 eavernikovskaya.localdomain systemd[1]: Finished Cleanup of Temporary Directories.
Oct 16 00:45:45 eavernikovskaya.localdomain systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: De
Oct 16 00:48:16 eavernikovskaya.localdomain systemd[1]: Stopping System Logging Service...
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41635]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-b
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Stopped System Logging Service.
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Starting System Logging Service...
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41918]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-b
Oct 16 00:48:17 eavernikovskaya.localdomain systemd[1]: Started System Logging Service.
Oct 16 00:48:17 eavernikovskaya.localdomain rsyslogd[41918]: imjournal: journal files changed, reloading... [v8.2310.
Oct 16 00:49:06 eavernikovskaya.localdomain root[41931]: Daemon Debug Message
Oct 16 01:01:01 eavernikovskaya.localdomain CROND[42022]: (root) CMD (run-parts /etc/cron.hourly)
Oct 16 01:01:01 eavernikovskaya.localdomain run-parts[42025]: (/etc/cron.hourly) starting 0anacron
Oct 16 01:01:01 eavernikovskaya.localdomain run-parts[42037]: (/etc/cron.hourly) finished 0anacron
Oct 16 01:01:01 eavernikovskaya.localdomain CROND[42021]: (root) CMDEND (run-parts /etc/cron.hourly)
Lines 1-20/20 (END)
```

Рис. 3.28: Просмотр последних 20 строк журнала

Для просмотра только сообщений об ошибках вводим `journalctl -p err` (рис. 3.29)


```

[root@eavernikovskaya ~]# journalctl -p err
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to
Oct 16 00:30:44 eavernikovskaya.localdomain systemd[1]: Invalid DMI field header.
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Oct 16 00:30:47 eavernikovskaya.localdomain systemd[1]: Invalid DMI field header.
Oct 16 00:30:48 eavernikovskaya.localdomain systemd-udevd[620]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only no
Oct 16 00:30:48 eavernikovskaya.localdomain systemd-udevd[624]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only no
Oct 16 00:30:49 eavernikovskaya.localdomain alsactl[767]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 16 00:30:50 eavernikovskaya.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 16 00:30:51 eavernikovskaya.localdomain rsyslogd[1160]: imjournal: fscanf on state file /var/lib/rsyslog/imjournal
Oct 16 00:30:51 eavernikovskaya.localdomain rsyslogd[1160]: imjournal: ignoring invalid state file /var/lib/rsyslog/im
Oct 16 00:31:06 eavernikovskaya.localdomain gdm-password[11559]: gkr-pam: unable to locate daemon control file
Oct 16 00:31:09 eavernikovskaya.localdomain systemd[1576]: Failed to start Application launched by gnome-session-binar
Oct 16 00:31:09 eavernikovskaya.localdomain systemd[1576]: Failed to start Application launched by gnome-session-binar
Oct 16 00:31:12 eavernikovskaya.localdomain gdm-wayland-session[1150]: GLib: Source ID 2 was not found when attempting
Oct 16 00:31:12 eavernikovskaya.localdomain gdm-launch-environment[1098]: GLib-GObject: g_object_unref: assertion 'G
lines 1-18/18 (END)

```

Рис. 3.29: Просмотр сообщений только 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.

Для просмотра всех сообщений со вчерашнего дня вводим `journalctl –since yesterday` (рис. 3.30)

```

[root@eavernikovskaya ~]# journalctl --since yesterday
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iadi-prod-bu
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: The list of certified hardware and cloud instances for Enterprise
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Command line: BOOT_IMAGE=(hdd,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, up
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: signal: max sigframe size: 1776
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-provided physical RAM map:

```

Рис. 3.30: Просмотр всех сообщений со вчерашнего дня

Далее просматриваем все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Для этого используем команду `journalctl –since yesterday -p err` (рис. 3.31)

```

[root@eavernikovskaya ~]# journalctl --since yesterday -p err
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to
Oct 16 00:30:44 eavernikovskaya.localdomain systemd[1]: Invalid DMI field header.
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Oct 16 00:30:45 eavernikovskaya.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Oct 16 00:30:47 eavernikovskaya.localdomain systemd[1]: Invalid DMI field header.
Oct 16 00:30:48 eavernikovskaya.localdomain systemd-udevd[620]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only no
Oct 16 00:30:48 eavernikovskaya.localdomain systemd-udevd[624]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only no
Oct 16 00:30:49 eavernikovskaya.localdomain alsactl[767]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Oct 16 00:30:50 eavernikovskaya.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 16 00:30:51 eavernikovskaya.localdomain rsyslogd[1160]: imjournal: fscanf on state file /var/lib/rsyslog/imjournal
Oct 16 00:30:51 eavernikovskaya.localdomain rsyslogd[1160]: imjournal: ignoring invalid state file /var/lib/rsyslog/im
Oct 16 00:31:06 eavernikovskaya.localdomain gdm-password[11559]: gkr-pam: unable to locate daemon control file
Oct 16 00:31:09 eavernikovskaya.localdomain systemd[1576]: Failed to start Application launched by gnome-session-binar
Oct 16 00:31:09 eavernikovskaya.localdomain systemd[1576]: Failed to start Application launched by gnome-session-binar
Oct 16 00:31:12 eavernikovskaya.localdomain gdm-wayland-session[1150]: GLib: Source ID 2 was not found when attempting
Oct 16 00:31:12 eavernikovskaya.localdomain gdm-launch-environment[1098]: GLib-GObject: g_object_unref: assertion 'G
lines 1-18/18 (END)

```

Рис. 3.31: Просмотр всех сообщений с ошибкой приоритета со вчерашнего дня

Посмотрим детальную информацию с помощью *journalctl -o verbose* (рис. 3.32)

```
[root@eavernikovskaya ~]# journalctl -o verbose
Wed 2024-10-16 00:30:44.395183 MSK [s=6e98d83e22404fe09fala3e144ff378c;i=1;b=4617e2adf43644c78e7f41f38e3b5dd3;m=140107]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC)
  _BOOT_ID=4617e2adf43644c78e7f41f38e3b5dd3
  _MACHINE_ID=b9202024839e4f95856600f1e460ebe9
  _HOSTNAME=eavernikovskaya.localdomain
  _RUNTIME_SCOPE=initrd
Wed 2024-10-16 00:30:44.395213 MSK [s=6e98d83e22404fe09fala3e144ff378c;i=2;b=4617e2adf43644c78e7f41f38e3b5dd3;m=140126]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=4617e2adf43644c78e7f41f38e3b5dd3
  _MACHINE_ID=b9202024839e4f95856600f1e460ebe9
  _HOSTNAME=eavernikovskaya.localdomain
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Eco
```

Рис. 3.32: Просмотр детальной информации

Для просмотра дополнительной информации о модуле *sshd* вводим **journalctl _SYSTEMD_UNIT=sshd.service** (рис. 3.33)

```
[root@eavernikovskaya ~]# journalctl _SYSTEMD_UNIT=sshd.service
Oct 16 00:30:50 eavernikovskaya.localdomain sshd[1075]: Server listening on 0.0.0.0 port 22.
Oct 16 00:30:50 eavernikovskaya.localdomain sshd[1075]: Server listening on :: port 22.
[root@eavernikovskaya ~]#
```

Рис. 3.33: Просмотр дополнительной информации о модуле *sshd*

3.4 Постоянный журнал *journald*

Запускаем терминал и получаем полномочия администратора (рис. 3.34)

```
[eavernikovskaya@eavernikovskaya ~]$ su -
Password:
[root@eavernikovskaya ~]#
```

Рис. 3.34: Режим *root*

Создаём каталог для хранения записей журнала *mkdir -p /var/log/journal* (рис. 3.35)

```
[root@eavernikovskaya ~]# mkdir -p /var/log/journal
[root@eavernikovskaya ~]#
```

Рис. 3.35: Создание каталога для хранения записей журнала

Скорректируем права доступа для каталога `/var/log/journal`, чтобы `journal` смог записывать в него информацию. Для этого введём команды `chown root:systemd-journal /var/log/journal` и `chmod 2755 /var/log/journal` (рис. 3.36)

```
[root@eavernikovskaya ~]# chown root:systemd-journal /var/log/journal
[root@eavernikovskaya ~]# chmod 2755 /var/log/journal
[root@eavernikovskaya ~]#
```

Рис. 3.36: Установление прав доступа для каталога `/var/log/journal`

Для принятия изменений необходимо или перезагрузить систему (перезапустить службу `systemd-journald` недостаточно), или использовать команду `killall -USR1 systemd-journald`, что мы и делаем (рис. 3.37)

```
[root@eavernikovskaya ~]# killall -USR1 systemd-journald
[root@eavernikovskaya ~]#
```

Рис. 3.37: Команда `killall -USR1 systemd-journald`

Журнал `systemd` теперь постоянный. Теперь посмотрим сообщения журнала с момента последней перезагрузки с помощью команды `journalctl -b` (рис. 3.38)

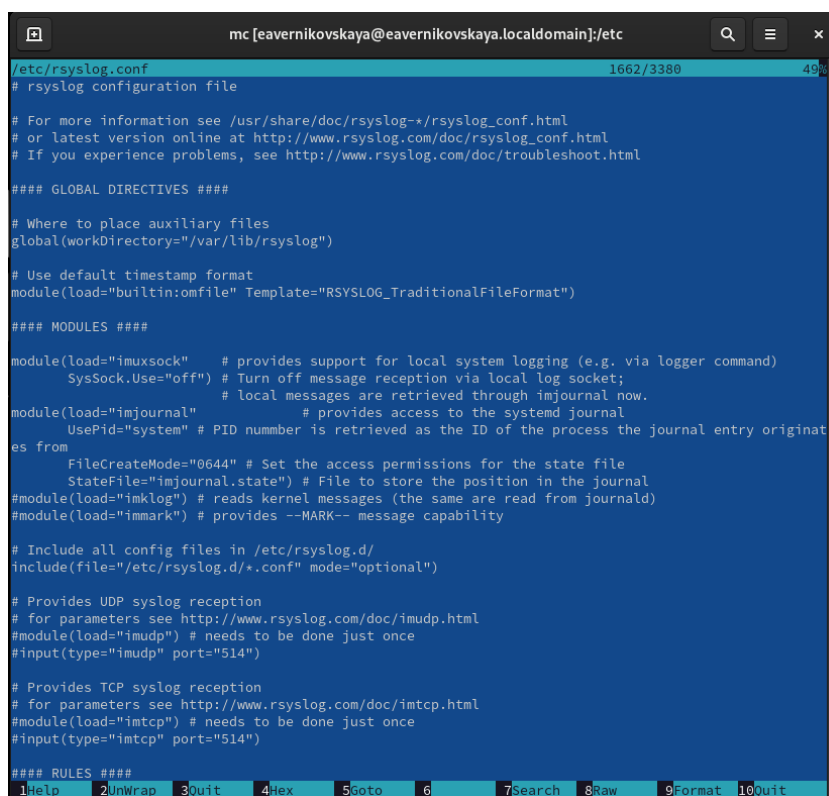
```
[root@eavernikovskaya ~]# journalctl -b
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-bu
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: The list of certified hardware and cloud instances for Enterprise
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, u
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: signal: max sigframe size: 1776
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-provided physical RAM map:
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
```

Рис. 3.38: Сообщения журнала с момента последней перезагрузки

4 Контрольные вопросы + ответы

1. Какой файл используется для настройки rsyslogd?

/etc/rsyslog.conf (рис. 4.1)



```
/etc/rsyslog.conf 1662/3380 49%
# 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 logger command)
        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 journal entry originates from
        FileCreateMode="0644" # Set the access permissions for the state file
        StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

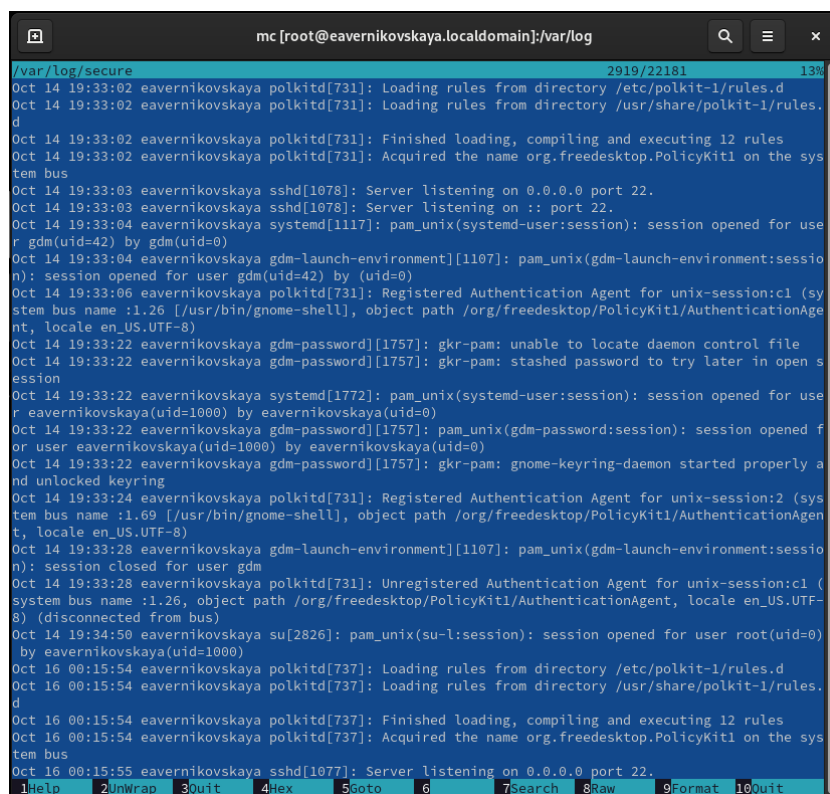
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")

#### RULES ####
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

Рис. 4.1: Вопрос №1

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

/var/log/secure (рис. 4.2)

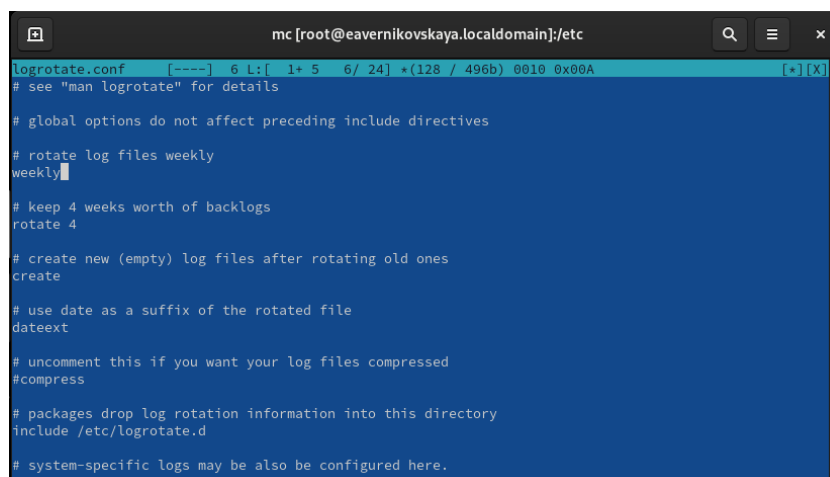


```
mc [root@eavernikovskaya.localdomain]:/var/log
/var/log/secure 2919/22181 13%
Oct 14 19:33:02 eavernikovskaya polkitd[731]: Loading rules from directory /etc/polkit-1/rules.d
Oct 14 19:33:02 eavernikovskaya polkitd[731]: Loading rules from directory /usr/share/polkit-1/rules.d
Oct 14 19:33:02 eavernikovskaya polkitd[731]: Finished loading, compiling and executing 12 rules
Oct 14 19:33:02 eavernikovskaya polkitd[731]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Oct 14 19:33:03 eavernikovskaya sshd[1078]: Server listening on 0.0.0.0 port 22.
Oct 14 19:33:03 eavernikovskaya sshd[1078]: Server listening on :: port 22.
Oct 14 19:33:04 eavernikovskaya systemd[1117]: pam_unix(systemd-user:session): session opened for user r gdm(uid=42) by gdm(uid=0)
Oct 14 19:33:04 eavernikovskaya gdm-launch-environment[1107]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 14 19:33:06 eavernikovskaya polkitd[731]: 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 14 19:33:22 eavernikovskaya gdm-password[1757]: gkr-pam: unable to locate daemon control file
Oct 14 19:33:22 eavernikovskaya gdm-password[1757]: gkr-pam: stashed password to try later in open session
Oct 14 19:33:22 eavernikovskaya systemd[1772]: pam_unix(systemd-user:session): session opened for user r eavernikovskaya(uid=1000) by eavernikovskaya(uid=0)
Oct 14 19:33:22 eavernikovskaya gdm-password[1757]: pam_unix(gdm-password:session): session opened for user eavernikovskaya(uid=1000) by eavernikovskaya(uid=0)
Oct 14 19:33:22 eavernikovskaya gdm-password[1757]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 14 19:33:24 eavernikovskaya polkitd[731]: Registered Authentication Agent for unix-session:2 (system bus name :1.69 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 14 19:33:28 eavernikovskaya gdm-launch-environment[1107]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 14 19:33:28 eavernikovskaya polkitd[731]: 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 14 19:34:50 eavernikovskaya su[2826]: pam_unix(su-l:session): session opened for user root(uid=0) by eavernikovskaya(uid=1000)
Oct 16 00:15:54 eavernikovskaya polkitd[737]: Loading rules from directory /etc/polkit-1/rules.d
Oct 16 00:15:54 eavernikovskaya polkitd[737]: Loading rules from directory /usr/share/polkit-1/rules.d
Oct 16 00:15:54 eavernikovskaya polkitd[737]: Finished loading, compiling and executing 12 rules
Oct 16 00:15:54 eavernikovskaya polkitd[737]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Oct 16 00:15:55 eavernikovskaya sshd[1077]: Server listening on 0.0.0.0 port 22.
1Help 2Unwrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

Рис. 4.2: Вопрос №2

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

Неделя (рис. 4.3)



```
mc [root@eavernikovskaya.localdomain]:/etc
logrotate.conf [----] 6 L: [ 1+ 5 6/ 24] *(128 / 496b) 0010 0x00A [*][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

# system-specific logs may be also be configured here.
```

Рис. 4.3: Вопрос №3

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 (рис. 4.4)

```
[root@eavernikovskaya ~]# tail -f /var/log/messages
Oct 16 00:31:52 eavernikovskaya su[2531]: (to root) eavernikovskaya on pts/1
Oct 16 00:31:55 eavernikovskaya geoclue[1249]: Service not used for 60 seconds. Shutting down..
Oct 16 00:31:55 eavernikovskaya systemd[1]: geoclue.service: Deactivated successfully.
Oct 16 00:31:57 eavernikovskaya systemd[1]: realmd.service: Deactivated successfully.
Oct 16 00:32:03 eavernikovskaya chronyd[754]: Selected source 92.126.227.190 (2.rocky.pool.ntp.org)
Oct 16 00:32:06 eavernikovskaya chronyd[754]: Selected source 185.209.85.222 (2.rocky.pool.ntp.org)
Oct 16 00:32:09 eavernikovskaya su[2564]: (to root) eavernikovskaya on pts/2
Oct 16 00:32:09 eavernikovskaya systemd[1576]: Starting Virtual filesystem metadata service...
Oct 16 00:32:09 eavernikovskaya systemd[1576]: Started Virtual filesystem metadata service.
Oct 16 00:32:12 eavernikovskaya systemd[1]: fprintd.service: Deactivated successfully.
Oct 16 00:32:39 eavernikovskaya systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

Рис. 4.4: Вопрос №5

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 "2024-10-16 09:00:00" --until "2024-10-16 15:00:00"

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

journalctl -b (рис. 4.5)

```
[root@eavernikovskaya ~]# journalctl -b
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iadi-prod-bu
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: The list of certified hardware and cloud instances for Enterprise R
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, u
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: signal: max sigframe size: 1776
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-provided physical RAM map:
Oct 16 00:30:44 eavernikovskaya.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009f00] usable
```

Рис. 4.5: Вопрос №7

8. Какая процедура позволяет сделать журнал journald постоянным?

- запустить терминал и получить права пользователя root

- создать каталог для хранения записей журнала: `mkdir -p /var/log/journal` (рис. 4.6)
- скорректировать права доступа для каталога `/var/log/journal`, чтобы `journal` смог записывать в него информацию: `chown root:systemd-journal /var/log/journal` и `chmod 2755 /var/log/journal` (рис. 4.7)
- для принятия изменений используем команду `killall -USR1 systemd-journald` (рис. 4.8)

```
[root@eavernikovskaya ~]# mkdir -p /var/log/journal
[root@eavernikovskaya ~]#
```

Рис. 4.6: Вопрос №8 (1)

```
[root@eavernikovskaya ~]# chown root:systemd-journal /var/log/journal
[root@eavernikovskaya ~]# chmod 2755 /var/log/journal
[root@eavernikovskaya ~]#
```

Рис. 4.7: Вопрос №8 (2)

```
[root@eavernikovskaya ~]# killall -USR1 systemd-journald
[root@eavernikovskaya ~]#
```

Рис. 4.8: Вопрос №8 (3)

5 Выводы

В ходе выполнения лабораторной работы мы получили навыки работы с журналами мониторинга различных событий в системе.

6 Список литературы

1. Лабораторная работа №7 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/11777/mod_resource/content/1/syslog.pdf