

# **Лабораторная работа № 7. Управление журналами событий в системе**

**Дисциплина: основы администрирования операционных систем**

Жукова Арина Александровна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
3.1	Основные файлы журналов . . . . .	7
3.2	Категории rsyslogd . . . . .	8
3.3	Приоритеты rsyslogd . . . . .	8
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
4.1	Мониторинг журнала системных событий в реальном времени . .	9
4.2	Изменение правил rsyslog.conf . . . . .	11
4.3	Использование journalctl . . . . .	16
4.4	Постоянный журнал journald . . . . .	21
<b>5</b>	<b>Ответы на контрольные вопросы</b>	<b>23</b>
<b>6</b>	<b>Выводы</b>	<b>25</b>
	<b>Список литературы</b>	<b>26</b>

# Список иллюстраций

4.1	Запуск трех вкладок . . . . .	9
4.2	Мониторинг системных событий . . . . .	10
4.3	Отображение сообщения . . . . .	10
4.4	Вывод сообщения . . . . .	11
4.5	Вывод сообщений об ошибках . . . . .	11
4.6	Установка Apsache . . . . .	12
4.7	Запуск веб-службы . . . . .	12
4.8	Журнал сообщений об ошибках . . . . .	13
4.9	Добавление строки . . . . .	13
4.10	Создание файла . . . . .	14
4.11	Редактирование файла . . . . .	14
4.12	Перезагрузка конфигурации rsyslogd и веб-службу . . . . .	14
4.13	Редактирование файла . . . . .	15
4.14	Создание файла . . . . .	15
4.15	Внесение изменений . . . . .	15
4.16	Терминалы . . . . .	16
4.17	Журнал событий . . . . .	17
4.18	Просмотр журнала без пейджера . . . . .	17
4.19	Просмотр журнала в реальном времени . . . . .	18
4.20	Просмотр событий . . . . .	18
4.21	Отображение последних 20 строк . . . . .	19
4.22	Сообщения об ошибках . . . . .	19
4.23	Сообщения со вчерашнего дня . . . . .	20
4.24	Сообщения с ошибкой . . . . .	20
4.25	Вывод детальной информации . . . . .	21
4.26	Дополнительная информация о модуле . . . . .	21
4.27	Перезагрузка системы . . . . .	22
4.28	Вывод сообщений . . . . .	22

## **Список таблиц**

# 1 Цель работы

Получить навыки 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 Теоретическое введение

### 3.1 Основные файлы журналов

В системах на базе Unix/Linux важное место при администрировании занимает отслеживание системных событий (и в частности возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журналирование системных событий заключается в фиксировании с помощью сокета syslog в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы. Обычно лог-файлы располагаются в каталоге /var/log: – /var/log/messages — общий файл журнала, в который записывается большинство сообщений системы (наиболее часто используемый файл журнала); – /var/log/dmesg — журнал сообщений ядра системы; – /var/log/secure — журнал сообщений, связанных с аутентификацией в системе; – /var/log/boot.log — журнал сообщений, связанных с запуском системы; – /var/log/audit/audit.log — журнал сообщений аудита (например, в него записываются сообщения SELinux); – /var/log/maillog — журналы сообщений, связанных с почтовой службой; – /var/log/samba — журналы сообщений службы samba (samba по умолчанию не управляется через rsyslogd); – /var/log/sss — журналы сообщений службы sssd; – /var/log/cups — журналы службы печати cups; – /var/log/httpd/ — каталог с журналами веб-службы Apache (Apache записывает сообщения в эти файлы напрямую, а не через rsyslog).

## 3.2 Категории rsyslogd

Сообщения в rsyslogd относятся к той или иной категории. Категории сообщений и их приоритетность обеспечивают иерархичность системы хранения журналов сообщений системы и скорость реагирования на возникновение критичных для её работы событий. Выделяют следующие категории: – auth/authpriv – сообщения, связанные с аутентификацией; – cron – сообщения, генерируемые службой crond; – daemon – сообщения от неспецифицированных демонов; – kern – сообщения ядра; – lpr – сообщения, созданные через устаревшую систему печати lpd; – mail – сообщения, связанные с электронной почтой; – mark – специальный объект, который можно использовать для записи маркера; – news – сообщения, созданные системой новостей NNTP; – security – то же, что и auth/authpriv (не нужно использовать); – syslog – сообщения, созданные системой syslog; – user – сообщения, сгенерированные в пространстве пользователя; – uucp – сообщения, созданные устаревшей системой UUCP; – local0-7 – сообщения, генерируемые службами, которые настроены любым из локальных объектов.

## 3.3 Приоритеты rsyslogd

По важности (уровню опасности) сообщения разделяются по приоритетам: – debug – отладочные сообщения (уровень опасности 7); – info – информационные сообщения о нормальной работе (уровень опасности 6); – notice – используется для информационных сообщений об элементах, которые могут стать проблемой позже (уровень опасности 5); – warning/warn – что-то происходит, но пока нет реальной ошибки (уровень опасности 4); – err/error – некритическая ошибка (уровень опасности 3); – crit – критическая ошибка (уровень опасности 2); – alert – используется, когда доступность службы под угрозой (уровень опасности 1); – emerg/panic – сообщение генерируется, когда служба не доступна (уровень опасности 0).



## 4 Выполнение лабораторной работы

### 4.1 Мониторинг журнала системных событий в реальном времени

1. Запустила три вкладки терминала и в каждом из них получила полномочия администратора (рис. 4.1).

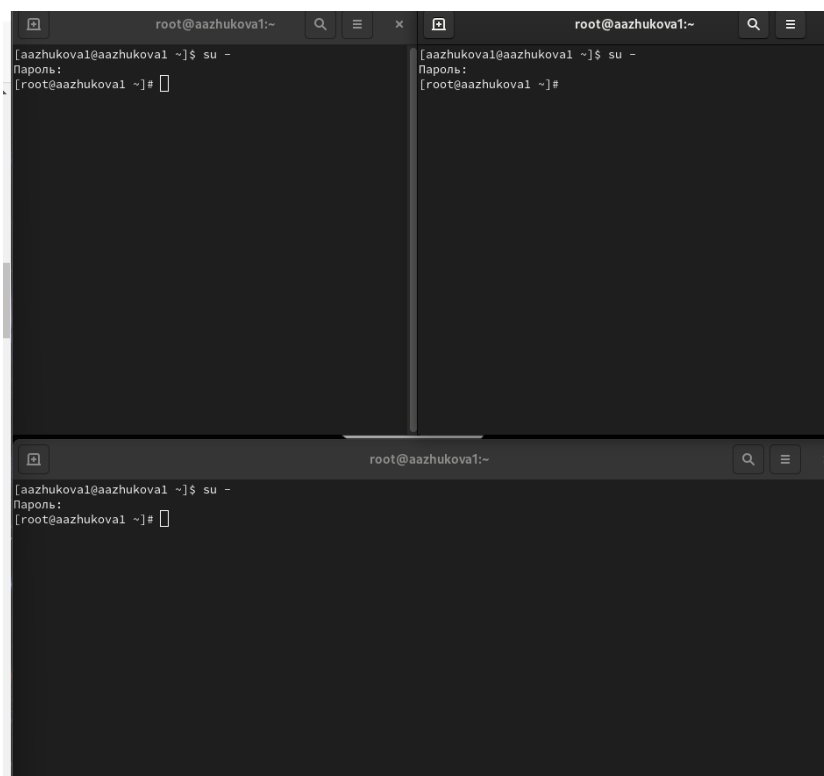


Рис. 4.1: Запуск трех вкладок

2. На второй вкладке терминала запустила мониторинг системных событий в реальном времени (рис. 4.2).

```
[root@aazhukoval ~]# tail -f /var/log/messages
Oct 18 19:14:57 aazhukoval PackageKit[1897]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct 18 19:15:01 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:15:03 aazhukoval systemd[2258]: Started VTE child process 3298 launched by gnome-terminal-server process 3071.
Oct 18 19:15:11 aazhukoval systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 18 19:15:11 aazhukoval systemd[1]: Started Fingerprint Authentication Daemon.
Oct 18 19:15:14 aazhukoval su[3328]: (to root) aazhukoval on pts/2
Oct 18 19:15:41 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:15:44 aazhukoval systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 18 19:16:07 aazhukoval systemd[2258]: Starting Mark boot as successful...
Oct 18 19:16:07 aazhukoval systemd[2258]: Finished Mark boot as successful.
Oct 18 19:16:48 aazhukoval chronyd[760]: Selected source 194.190.168.1 (2.rocky.pool.ntp.org)
```

Рис. 4.2: Мониторинг системных событий

3. В третьей вкладке терминала вернулась к учётной записи своего пользователя (достаточно нажать Ctrl + d) и попыталась получить полномочия администратора, но ввела неправильный пароль. Обратила внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username». Отображаемые на экране сообщения также фиксировались в файле /var/log/messages (рис. 4.3).

```
.190.168.1 (2.rocky.pool.ntp.org)
Oct 18 19:17:31 aazhukoval systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 18 19:17:31 aazhukoval systemd[1]: Started Fingerprint Authentication Daemon.
Oct 18 19:17:38 aazhukoval su[3396]: FAILED SU (to root) aazhukoval on pts/0
```

Рис. 4.3: Отображение сообщения

4. В третьей вкладке терминала из оболочки пользователя ввела `logger hello`.  
Во второй вкладке терминала с мониторингом увидела сообщение, которое также было зафиксировано в файле `/var/log/messages` (рис. 4.4).

```
Oct 18 19:18:01 aazhukoval systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 19:18:02 aazhukoval aazhukoval[3412]: hello
```

Рис. 4.4: Вывод сообщения

5. Во второй вкладке терминала с мониторингом остановила трассировку файла сообщений мониторинга реального времени, используя `Ctrl + c`. Затем запустила мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов) при помощи `tail -n 20 /var/log/secure`. Увидела сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды `su` (рис. 4.5).

```
ser gum  
Oct 18 19:13:57 aazhukoval polkitd[740]: Unregistered Authentication Agent for unix-session:cl (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)  
Oct 18 19:14:34 aazhukoval su[3133]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:14:57 aazhukoval su[3203]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:15:14 aazhukoval su[3328]: pam_unix(su-l:session): session opened for user root(uid=0) by aazhukoval(uid=1000)  
Oct 18 19:17:24 aazhukoval su[3133]: pam_unix(su-l:session): session closed for user root  
Oct 18 19:17:35 aazhukoval unix_chkpwd[3403]: password check failed for user (root)  
Oct 18 19:17:35 aazhukoval su[3396]: pam_unix(su-l:auth): authentication failure; logname=aazhukoval uid=1000 euid=0 tty=/dev/pts/0 ruser=aazhukoval rhost= user=root  
[root@aazhukoval ~]#
```

Рис. 4.5: Вывод сообщений об ошибках

## 4.2 Изменение правил `rsyslog.conf`

1. В первой вкладке терминала установила Apache (рис. 4.6).

```
[root@aazhukoval ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS 5.8 kB/s | 4.1 kB 00:00
Rocky Linux 9 - BaseOS 1.0 MB/s | 2.3 MB 00:02
Rocky Linux 9 - AppStre 6.1 kB/s | 4.5 kB 00:00
Rocky Linux 9 - AppStre 2.5 MB/s | 8.0 MB 00:03
Rocky Linux 9 - Extras 3.1 kB/s | 2.9 kB 00:00
Rocky Linux 9 - Extras 9.3 kB/s | 15 kB 00:01
Зависимости разрешены.
=====
Пакет          Архитектура
                Версия          Репозиторий
                Размер
=====
Установка:
  httpd          x86_64 2.4.57-11.el9_4.1 appstream 44 k
Установка зависимостей:
```

Рис. 4.6: Установка Apache

2. После окончания процесса установки запустила веб-службу (рис. 4.7).

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

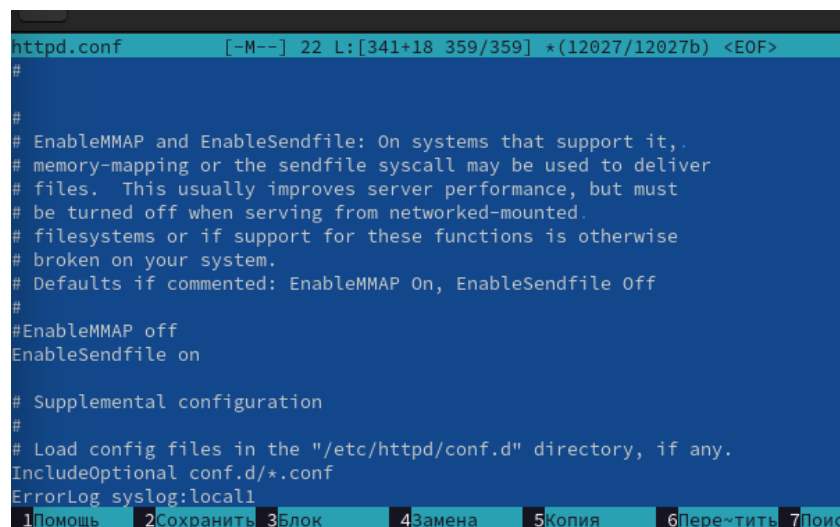
Рис. 4.7: Запуск веб-службы

3. Во второй вкладке терминала посмотрела журнал сообщений об ошибках веб-службы. Чтобы закрыть трассировку файла журнала, использовала Ctrl + c (рис. 4.8).

```
[root@aazhukoval ~]# tail -f /var/log/httpd/error_log
[Fri Oct 18 19:21:23.665777 2024] [core:notice] [pid 4022:tid 4022] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 18 19:21:23.668848 2024] [suexec:notice] [pid 4022:tid 4022] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 18 19:21:23.703744 2024] [lbmethod_heartbeat:notice] [pid 4022:tid 4022] AH02282: No slotmem from mod_heartmonitor
[Fri Oct 18 19:21:23.711354 2024] [mpm_event:notice] [pid 4022:tid 4022] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 18 19:21:23.711392 2024] [core:notice] [pid 4022:tid 4022] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4.8: Журнал сообщений об ошибках

4. В третьей вкладке терминала получила полномочия администратора и в файле конфигурации /etc/httpd/conf/httpd.conf в конце добавила следующую строку: `ErrorLog syslog:local1` (рис. 4.9).



```
httpd.conf [-M--] 22 L:[341+18 359/359] *(12027/12027b) <EOF>
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local1
```

Рис. 4.9: Добавление строки

5. В каталоге /etc/rsyslog.d создала файл мониторинга событий веб-службы (рис. 4.10).

```
[root@aazhukoval conf]# cd /etc/rsyslog.d
[root@aazhukoval rsyslog.d]# touch httpd.conf
[root@aazhukoval rsyslog.d]# ls
httpd.conf
[root@aazhukoval rsyslog.d]#
```

Рис. 4.10: Создание файла

6. Открыв его на редактирование, прописала в нём `local1.* -/var/log/httpd-error.log` (рис. 4.11).

```
/etc/rsyslog.d/httpd.conf
local1.* -/var/log/httpd-error.log
```

Рис. 4.11: Редактирование файла

Эта строка позволила отправлять все сообщения, получаемые для объекта `local1` (который теперь использовался службой `httpd`), в файл `/var/log/httpd-error.log`.

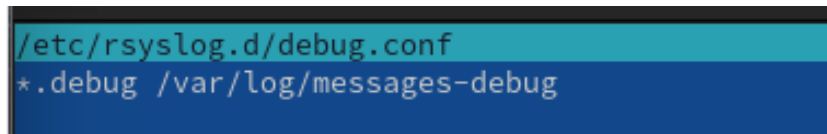
7. Перешла в первую вкладку терминала и перезагрузила конфигурацию `rsyslogd` и веб-службу (рис. 4.12).

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

Рис. 4.12: Перезагрузка конфигурации `rsyslogd` и веб-службу

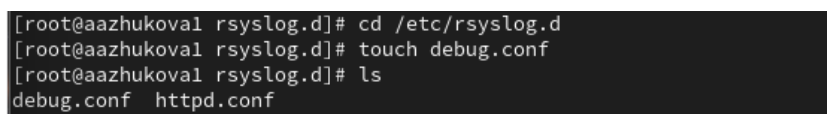
Все сообщения об ошибках веб-службы теперь были записаны в файл `/var/log/httpd-error.log`, что можно наблюдать или в режиме реального времени, используя команду `tail` с соответствующими параметрами, или непосредственно просматривая указанный файл.

8. В третьей вкладке терминала создала отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале ввела `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf` (рис. 4.13 - 4.15).




```
/etc/rsyslog.d/debug.conf
*.debug /var/log/messages-debug
```

Рис. 4.13: Редактирование файла



```
[root@aazhukoval rsyslog.d]# cd /etc/rsyslog.d
[root@aazhukoval rsyslog.d]# touch debug.conf
[root@aazhukoval rsyslog.d]# ls
debug.conf  httpd.conf
```

Рис. 4.14: Создание файла



```
bash: syntax error near unexpected token `newline'
[root@aazhukoval rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@aazhukoval rsyslog.d]# mc
```

Рис. 4.15: Внесение изменений

9. В первой вкладке терминала снова перезапустила `rsyslogd`. Во второй вкладке терминала запустила мониторинг отладочной информации. В третьей вкладке терминала ввела: `logger -p daemon.debug "Daemon Debug Message"` (рис. 4.16).

```
Установлен:
apr-1.7.0-12.el9_3.x86_64
apr-util-1.6.1-23.el9.x86_64
apr-util-bdb-1.6.1-23.el9.x86_64
apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.57-11.el9_4.1.x86_64
httpd-core-2.4.57-11.el9_4.1.x86_64
httpd-filesystem-2.4.57-11.el9_4.1.noarch
httpd-tools-2.4.57-11.el9_4.1.x86_64
mod_http2-2.0.26-2.el9_4.x86_64
mod_lua-2.4.57-11.el9_4.1.x86_64
rocky-logos-httpd-90.15-2.el9.noarch

Выполнено!
[root@aazhukoval ~]# systemctl start httpd
bash: systemctlstart: команда не найдена...
[root@aazhukoval ~]# systemctl start httpd
[root@aazhukoval ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@aazhukoval ~]# systemctl restart rsyslog.service
[root@aazhukoval ~]# systemctl restart httpd
[root@aazhukoval ~]# systemctl restart rsyslog.service
[root@aazhukoval ~]#

[11] Oct 18 19:21:23.711392 2024] [core:notice] [pid 4022:tid 4022] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
[root@aazhukoval ~]# tail -f /var/log/messages-debug
Oct 18 19:33:44 aazhukoval systemd[1]: Stopping System Logging Service...
Oct 18 19:33:44 aazhukoval rsyslogd[4395]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="4395" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 19:33:44 aazhukoval systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 19:33:44 aazhukoval systemd[1]: Stopped System Logging Service.
Oct 18 19:33:44 aazhukoval systemd[1]: Starting System Logging Service...
Oct 18 19:33:44 aazhukoval rsyslogd[4633]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="4633" x-info="https://www.rsyslog.com"] start
Oct 18 19:33:44 aazhukoval systemd[1]: Started System Logging Service.
Oct 18 19:33:44 aazhukoval rsyslogd[4633]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 19:34:08 aazhukoval root[4639]: Daemon Debug Message

root@aazhukoval1:/etc/rsyslog.d
root@aazhukoval rsyslog.d]# mc
root@aazhukoval rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
root@aazhukoval rsyslog.d]#
```

Рис. 4.16: Терминалы

В терминале с мониторингом посмотрела сообщение отладки. Чтобы закрыть трассировку файла журнала, использовала Ctrl + c.

## 4.3 Использование journalctl

1. Во второй вкладке терминала посмотрела содержимое журнала с событиями с момента последнего запуска системы. Для пролистывания журнала использовала или Enter (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра использовала q (рис. 4.17).



```
[root@aazhukoval ~]# journalctl
окт 18 19:12:13 aazhukoval.localdomain kernel: Linux versio>
окт 18 19:12:13 aazhukoval.localdomain kernel: The list of >
окт 18 19:12:13 aazhukoval.localdomain kernel: Command line>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Sup>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Sup>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Sup>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: xst>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Enap>
окт 18 19:12:13 aazhukoval.localdomain kernel: signal: max >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-provide>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [ >
окт 18 19:12:13 aazhukoval.localdomain kernel: NX (Execute >
окт 18 19:12:13 aazhukoval.localdomain kernel: SMBIOS 2.5 pp>
окт 18 19:12:13 aazhukoval.localdomain kernel: DMI: innotek>
окт 18 19:12:13 aazhukoval.localdomain kernel: Hypervisor d>
```

Рис. 4.17: Журнал событий

2. Просмотр содержимого журнала без использования пейджера (рис. 4.18).

```
окт 18 19:33:44 aazhukoval.localdomain systemd[1]: Starting
System Logging Service...
окт 18 19:33:44 aazhukoval.localdomain rsyslogd[4633]: [orig
in software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="463
3" x-info="https://www.rsyslog.com"] start
окт 18 19:33:44 aazhukoval.localdomain systemd[1]: Started S
ystem Logging Service.
окт 18 19:33:44 aazhukoval.localdomain rsyslogd[4633]: imjou
rnal: journal files changed, reloading... [v8.2310.0-4.el9
try https://www.rsyslog.com/e/0 ]
окт 18 19:34:08 aazhukoval.localdomain root[4639]: Daemon De
bug Message
окт 18 19:36:36 aazhukoval.localdomain PackageKit[4590]: dae
mon quit
окт 18 19:36:36 aazhukoval.localdomain systemd[1]: packageki
t.service: Deactivated successfully.
[root@aazhukoval ~]# journalctl --no-pager
```

Рис. 4.18: Просмотр журнала без пейджера

3. Режим просмотра журнала в реальном времени `journalctl -f` (рис. 4.19).

```
System Logging Service...
окт 18 19:33:44 aazhukoval.localdomain rsyslogd[4633]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="4633" x-info="https://www.rsyslog.com"] start
окт 18 19:33:44 aazhukoval.localdomain systemd[1]: Started System Logging Service.
окт 18 19:33:44 aazhukoval.localdomain rsyslogd[4633]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
окт 18 19:34:08 aazhukoval.localdomain root[4639]: Daemon Debug Message
окт 18 19:36:36 aazhukoval.localdomain PackageKit[4590]: daemon quit
окт 18 19:36:36 aazhukoval.localdomain systemd[1]: packagekit.service: Deactivated successfully.
```

Рис. 4.19: Просмотр журнала в реальном времени

Использовала Ctrl + c для прерывания просмотра.

4. Просмотрела события для UID0 (рис. 4.20).

```
[root@aazhukoval ~]# journalctl _UID=0
окт 18 19:12:13 aazhukoval.localdomain systemd-journald[226]:
окт 18 19:12:13 aazhukoval.localdomain systemd-journald[226]:
окт 18 19:12:13 aazhukoval.localdomain systemd-sysusers[228]:
окт 18 19:12:13 aazhukoval.localdomain systemd-sysusers[228]:
окт 18 19:12:13 aazhukoval.localdomain systemd-sysusers[228]:
окт 18 19:12:13 aazhukoval.localdomain systemd-sysusers[228]:
окт 18 19:12:13 aazhukoval.localdomain systemd-modules-load:
окт 18 19:12:13 aazhukoval.localdomain systemd-modules-load:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Starting:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Finished:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Starting:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Finished:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Finished:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Finished:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: dracut ab
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Starting:
окт 18 19:12:13 aazhukoval.localdomain dracut-cmdline[243]:
окт 18 19:12:13 aazhukoval.localdomain dracut-cmdline[243]:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Finished:
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Starting:
```

Рис. 4.20: Просмотр событий

5. Для отображения последних 20 строк журнала ввела `journalctl -n 20` (рис. 4.21).

```
[root@aazhukoval ~]# journalctl -n 20
окт 18 19:31:07 aazhukoval.localdomain sys
окт 18 19:31:07 aazhukoval.localdomain sys
окт 18 19:31:07 aazhukoval.localdomain sys
окт 18 19:31:07 aazhukoval.localdomain htt
окт 18 19:31:07 aazhukoval.localdomain sys
окт 18 19:31:31 aazhukoval.localdomain sys
окт 18 19:31:31 aazhukoval.localdomain Pac
окт 18 19:31:31 aazhukoval.localdomain sys
окт 18 19:31:32 aazhukoval.localdomain Pac
окт 18 19:33:44 aazhukoval.localdomain sys
окт 18 19:33:44 aazhukoval.localdomain rsy
окт 18 19:33:44 aazhukoval.localdomain sys
```

Рис. 4.21: Отображение последних 20 строк

6. Для просмотра только сообщений об ошибках ввела `journalctl -p err` (рис. 4.22).

```
[root@aazhukoval ~]# journalctl -p err
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:12:13 aazhukoval.localdomain kernel: Warning: Unmaintained driver is detected: e1000
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running o
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported
окт 18 19:12:16 aazhukoval.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[622]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[651]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only
окт 18 19:12:18 aazhukoval.localdomain alsactl[778]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed
окт 18 19:12:19 aazhukoval.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
окт 18 19:13:36 aazhukoval.localdomain gdm-password[2208]: gkr-pam: unable to locate daemon control file
окт 18 19:13:50 aazhukoval.localdomain gdm-password[2246]: gkr-pam: unable to locate daemon control file
окт 18 19:13:57 aazhukoval.localdomain gdm-wayland-session[1250]: GLib: Source ID 2 was not found when attempt
окт 18 19:13:57 aazhukoval.localdomain gdm-launch-environment[1108]: GLib-GObject: g_object_unref: assertion 2
```

Рис. 4.22: Сообщения об ошибках

7. Для просмотра всех сообщений со вчерашнего дня ввела `journalctl --since yesterday` (рис. 4.23).

```
[root@aazhukoval ~]# journalctl --since yesterday
окт 18 19:12:13 aazhukoval.localdomain kernel: Linux versi>
окт 18 19:12:13 aazhukoval.localdomain kernel: The list of>
окт 18 19:12:13 aazhukoval.localdomain kernel: Command lin>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Su>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Su>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Su>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: xs>
окт 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: En>
окт 18 19:12:13 aazhukoval.localdomain kernel: signal: max>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-provid>
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: >
окт 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: >
```

Рис. 4.23: Сообщения со вчерашнего дня

8. Для просмотра всех сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, использовала `journalctl --since yesterday -p err` (рис. 4.24).

```
[root@aazhukoval ~]# journalctl --since yesterday -p err
окт 18 19:12:13 aazhukoval.localdomain systemd[1]: Invalid>
окт 18 19:12:13 aazhukoval.localdomain kernel: Warning: Un>
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000>
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000>
окт 18 19:12:13 aazhukoval.localdomain kernel: vmwgfx 0000>
окт 18 19:12:16 aazhukoval.localdomain systemd[1]: Invalid>
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[622]:>
окт 18 19:12:17 aazhukoval.localdomain systemd-udevd[651]:>
окт 18 19:12:18 aazhukoval.localdomain alsactl[778]: alsa->
окт 18 19:12:19 aazhukoval.localdomain kernel: Warning: Un>
окт 18 19:13:36 aazhukoval.localdomain gdm-password[2208]>
окт 18 19:13:50 aazhukoval.localdomain gdm-password[2246]>
окт 18 19:13:57 aazhukoval.localdomain gdm-wayland-session>
окт 18 19:13:57 aazhukoval.localdomain gdm-launch-environm>
```

Рис. 4.24: Сообщения с ошибкой

9. Если нужна детальная информация, использовала `journalctl -o verbose` (рис. 4.25).

```

[root@aazhukoval ~]# journalctl -o verbose
Fri 2024-10-18 19:12:13.150761 MSK [s=06486c08906148d2bfe9>
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 5.14.0-427.37.1.el9_4.x86_64 (mo>
  _BOOT_ID=96fbe0efbe2b462fb16bbcfc75df6e7c
  _MACHINE_ID=be1b7ad166564f34a1efe465c5099819
  _HOSTNAME=aazhukoval.localdomain
  _RUNTIME_SCOPE=initrd
Fri 2024-10-18 19:12:13.151090 MSK [s=06486c08906148d2bfe9>
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=96fbe0efbe2b462fb16bbcfc75df6e7c
  _MACHINE_ID=be1b7ad166564f34a1efe465c5099819
  _HOSTNAME=aazhukoval.localdomain
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of certified hardware and cloud insta>
Fri 2024-10-18 19:12:13.151106 MSK [s=06486c08906148d2bfe9>

```

Рис. 4.25: Вывод детальной информации

10. Для просмотра дополнительной информации о модуле `sshd` ввела `journalctl_SYSTEMD_UNIT=sshd.service` (рис. 4.26).

```

[root@aazhukoval ~]# journalctl _SYSTEMD_UNIT=sshd.service
окт 18 19:12:20 aazhukoval.localdomain sshd[1072]: Server >
окт 18 19:12:20 aazhukoval.localdomain sshd[1072]: Server >
lines 1-2/2 (END)

```

Рис. 4.26: Дополнительная информация о модуле

## 4.4 Постоянный журнал `journald`

1. Запустила терминал и получила полномочия администратора. Создала каталог для хранения записей журнала. Скорректировала права доступа для каталога `/var/log/journal`, чтобы `journald` смог записывать в него информацию. Для принятия изменений необходимо либо перезагрузить систему

(перезапустить службу systemd-journald недостаточно), либо использовать команду `killall -USR1 systemd-journald` (рис. 4.27).

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

Рис. 4.27: Перезагрузка системы

2. Журнал systemd теперь постоянный. Для вывод сообщения журнала с момента последней перезагрузки использовала `journalctl -b` (рис. 4.28).

```
[root@aazhukoval ~]# journalctl -b
OCT 18 19:12:13 aazhukoval.localdomain kernel: Linux version 5.14.0-427.37.1.el9_4.x86_64 (mockbuild@iad1-prod-bui
OCT 18 19:12:13 aazhukoval.localdomain kernel: The list of certified hardware and cloud instances for Enterprise L
OCT 18 19:12:13 aazhukoval.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.37.1.el9_4
OCT 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regist
OCT 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
OCT 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
OCT 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
OCT 18 19:12:13 aazhukoval.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, us
OCT 18 19:12:13 aazhukoval.localdomain kernel: signal: max sigframe size: 1776
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-provided physical RAM map:
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x000000000000100000-0x000000000000dfffff] usable
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x000000000000ffff0000-0x000000000000dfffff] ACPI data
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
OCT 18 19:12:13 aazhukoval.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
```

Рис. 4.28: Вывод сообщений

## 5 Ответы на контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

- rsyslog.conf

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

- auth.log

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

- По умолчанию файлы журналов будут ротироваться каждые неделю.

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?

- journalctl -f

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

- `journalctl –since ‘2023-10-26 09:00:00’ –until ‘2023-10-26 15:00:00’ _PID=1`  
(замените дату на актуальную)

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

- `journalctl -b`

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

- 1. Запустите терминал с правами администратора.
- 2. Создайте каталог для хранения записей журнала: `mkdir -p /var/log/journal`
- 3. Установите права доступа для каталога: `chown root:systemd-journal /var/log/journal` и `chmod 2755 /var/log/journal`
- 4. Перезагрузите систему или используйте `killall -USR1 systemd-journald`.



## **6 Выводы**

Я получила навыки работы с журналами мониторинга различных событий в системе.

## Список литературы

1. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: <http://wiki.opennet.ru/Systemd>.
2. Емельянов А. Управление логгированием в systemd. — 2015. — URL: <https://blog.selectel.ru/upravlenie-loggirovaniem-v-systemd/>.
3. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
4. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017.
5. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.