

Лабораторная работа №7

Управление журналами событий в системе

Перфилов Александр Константинович | Группа НПИбд-03-24

Российский университет дружбы народов, Москва, Россия

18 октября 2025

Раздел 1

Информация

Докладчик

- Перфилов Александр Константинович
- Группа НПИбд-03-24
- Российский университет дружбы народов
- <https://github.com/AlexanderPErfilovKonstantinivich?tab=repositories>

Цель работы

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

Задание

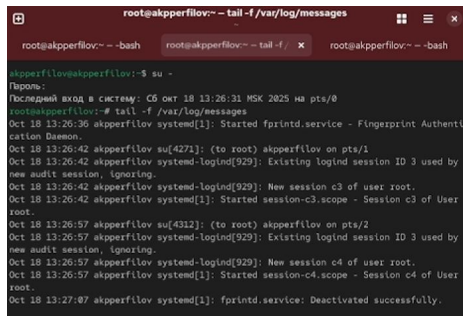
- ❶ Продemonстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
- ❷ Продemonстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
- ❸ Продemonстрируйте навыки работы с `journalctl` (см. раздел 7.4.3).
- ❹ Продemonстрируйте навыки работы с `journalld` (см. раздел 7.4.4).

Раздел 2

Выполнение лабораторной работы

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. 1)



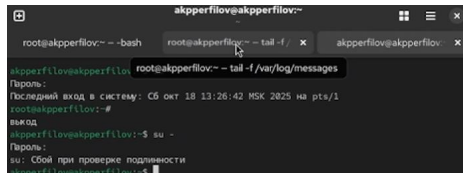
```
root@akpperfilov:~ - tail -f /var/log/messages
root@akpperfilov:~ - bash
root@akpperfilov:~ - tail -f /
root@akpperfilov:~ - bash

akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Сб окт 18 13:26:31 MSK 2025 на pts/0
root@akpperfilov:~# tail -f /var/log/messages
Oct 18 13:26:36 akpperfilov systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.
Oct 18 13:26:42 akpperfilov su[4271]: (to root) akpperfilov on pts/1
Oct 18 13:26:42 akpperfilov systemd-logind[929]: Existing logind session ID 3 used by new audit session, ignoring.
Oct 18 13:26:42 akpperfilov systemd-logind[929]: New session c3 of user root.
Oct 18 13:26:42 akpperfilov systemd[1]: Started session-c3.scope - Session c3 of User root.
Oct 18 13:26:57 akpperfilov su[4312]: (to root) akpperfilov on pts/2
Oct 18 13:26:57 akpperfilov systemd-logind[929]: Existing logind session ID 3 used by new audit session, ignoring.
Oct 18 13:26:57 akpperfilov systemd-logind[929]: New session c4 of user root.
Oct 18 13:26:57 akpperfilov systemd[1]: Started session-c4.scope - Session c4 of User root.
Oct 18 13:27:07 akpperfilov systemd[1]: fprintd.service: Deactivated successfully.
```

Рис. 1: Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.

Мониторинг журнала 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. 2)

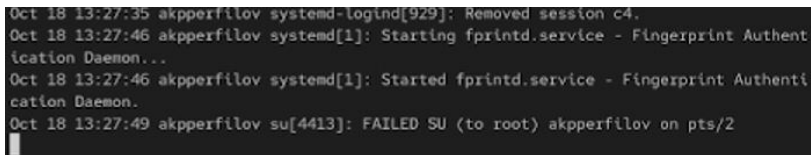


```
akpperfilov@akpperfilov:~  
root@akpperfilov:~ - bash root@akpperfilov:~ - tail -f / x akpperfilov@akpperfilov: x  
akpperfilov@akpperfilov root@akpperfilov:~ - tail -f /var/log/messages  
Пароль:  
Последний вход в систему: Сб окт 18 13:26:42 MSK 2025 на pts/1  
root@akpperfilov:~#  
выход  
akpperfilov@akpperfilov:~$ su -  
Пароль:  
su: Сбой при проверке подлинности  
akpperfilov@akpperfilov:~$
```

Рис. 2: Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора.

Мониторинг журнала системных событий в реальном времени

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)




```
Oct 18 13:27:35 akpperfilov systemd-logind[929]: Removed session c4.  
Oct 18 13:27:46 akpperfilov systemd[1]: Starting fprintd.service - Fingerprint Authentication Daemon...  
Oct 18 13:27:46 akpperfilov systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.  
Oct 18 13:27:49 akpperfilov su[4413]: FAILED SU (to root) akpperfilov on pts/2
```

Рис. 3: Новое сообщение в мониторинге событий во второй вкладке терминала.

Мониторинг журнала системных событий в реальном времени

В третьей вкладке терминала из оболочки пользователя введём: `logger hello` (рис. 4)



```
akpperfilov@akpperfilov:~$ logger hello
akpperfilov@akpperfilov:~$
```

Рис. 4: Ввод в третьей вкладке терминала.

Мониторинг журнала системных событий в реальном времени

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. 5)

Мониторинг журнала системных событий в реальном времени

```
Oct 18 13:28:31 akpperfilov akpperfilov[4459]: hello
^C
root@akpperfilov:~# tail -n 20 /var/log/secure
Oct 18 13:26:12 akpperfilov unix_chkpwd[4177]: password check failed for user (root)
Oct 18 13:26:12 akpperfilov su[4154]: pam_unix(su-l:auth): authentication failure; log
name=akpperfilov uid=1000 euid=0 tty=/dev/pts/0 ruser=akpperfilov rhost= user=root
Oct 18 13:26:31 akpperfilov (systemd)[4215]: pam_unix(systemd-user:session): session o
pened for user root(uid=0) by root(uid=0)
Oct 18 13:26:31 akpperfilov su[4209]: pam_unix(su-l:session): session opened for user
root(uid=0) by akpperfilov(uid=1000)
Oct 18 13:26:42 akpperfilov su[4271]: pam_unix(su-l:session): session opened for user
root(uid=0) by akpperfilov(uid=1000)
Oct 18 13:26:57 akpperfilov su[4312]: pam_unix(su-l:session): session opened for user
root(uid=0) by akpperfilov(uid=1000)
Oct 18 13:27:35 akpperfilov su[4312]: pam_unix(su-l:session): session closed for user
root
Oct 18 13:27:47 akpperfilov unix_chkpwd[4422]: password check failed for user (root)
Oct 18 13:27:47 akpperfilov su[4413]: pam_unix(su-l:auth): authentication failure; log
name=akpperfilov uid=1000 euid=0 tty=/dev/pts/2 ruser=akpperfilov rhost= user=root
root@akpperfilov:~#
```

Рис. 5: Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга

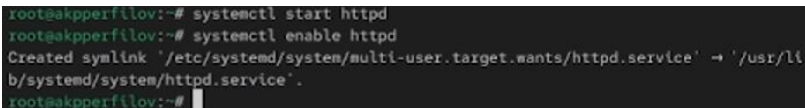
Изменение правил rsyslog.conf

В первой вкладке терминала установим Apache: `dnf -y install httpd` (рис. 6).

```
root@akpreifilov:~# dnf -y install httpd
Последняя проверка окончания срока действия метаданных: 0:03:42 назад, Сб 18 окт 2025
13:26:22.
Зависимости разрешены.
=====
Пакет                Архитектура  Версия                Репозиторий          Размер
=====
Установка:
httpd                 x86_64       2.4.63-1.el10_0.2     appstream             52 k
Установка зависимостей:
apr                   x86_64       1.7.5-2.el10          appstream             128 k
apr-util              x86_64       1.6.3-21.el10         appstream             98 k
apr-util-ldb          x86_64       1.6.3-21.el10         appstream             14 k
httpd-core            x86_64       2.4.63-1.el10_0.2     appstream             1.5 M
httpd-filesystem      noarch       2.4.63-1.el10_0.2     appstream             13 k
httpd-tools           x86_64       2.4.63-1.el10_0.2     appstream             80 k
rocky-logos-httpd     noarch       100.4-7.el10          appstream             24 k
Установка слабых зависимостей:
apr-util-openssl      x86_64       1.6.3-21.el10         appstream             16 k
mod_http2              x86_64       2.0.29-2.el10_0.1     appstream            164 k
mod_lua                x86_64       2.4.63-1.el10_0.2     appstream             59 k
Результат транзакции
=====
```

Изменение правил rsyslog.conf

После окончания процесса установки запустим веб-службу: `systemctl start httpd` и `systemctl enable httpd` (рис. 7)

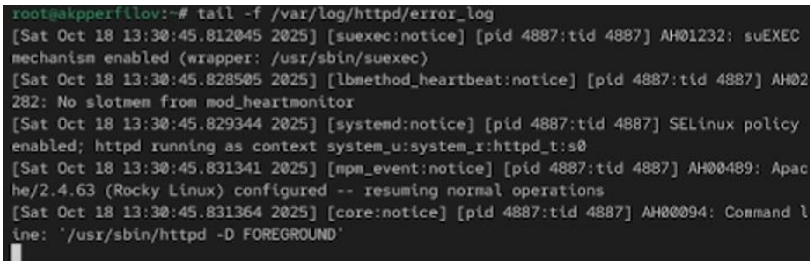


```
root@akpperfilov:~# systemctl start httpd
root@akpperfilov:~# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@akpperfilov:~#
```

Рис. 7: Запуск веб-службы.

Изменение правил rsyslog.conf

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. 8)



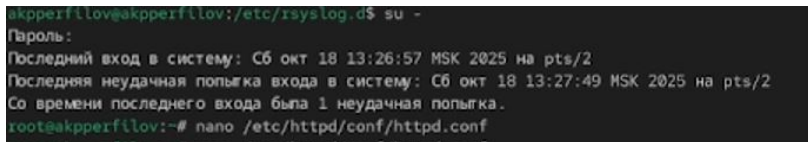
```
root@akpperfilov:~# tail -f /var/log/httpd/error_log
[Sat Oct 18 13:30:45.812045 2025] [suexec:notice] [pid 4887:tid 4887] AH01232: suEXEC
mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 18 13:30:45.828505 2025] [lbmethod_heartbeat:notice] [pid 4887:tid 4887] AH02
282: No slotmen from mod_heartmonitor
[Sat Oct 18 13:30:45.829344 2025] [systemd:notice] [pid 4887:tid 4887] SELinux policy
enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 13:30:45.831341 2025] [mpm_event:notice] [pid 4887:tid 4887] AH00489: Apac
he/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 13:30:45.831364 2025] [core:notice] [pid 4887:tid 4887] AH00094: Command l
ine: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 8: Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала.

Изменение правил rsyslog.conf

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. 9, рис. 10).

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



```
akpperfilov@akpperfilov:/etc/rsyslog.d$ su -
Пароль:
Последний вход в систему: Сб окт 18 13:26:57 MSK 2025 на pts/2
Последняя неудачная попытка входа в систему: Сб окт 18 13:27:49 MSK 2025 на pts/2
Со времени последнего входа была 1 неудачная попытка.
root@akpperfilov:~# nano /etc/httpd/conf/httpd.conf
```

Рис. 9: Получение в третьей вкладке терминала полномочия администратора, открытие файла `httpd.conf` на редактирование.

Изменение правил rsyslog.conf

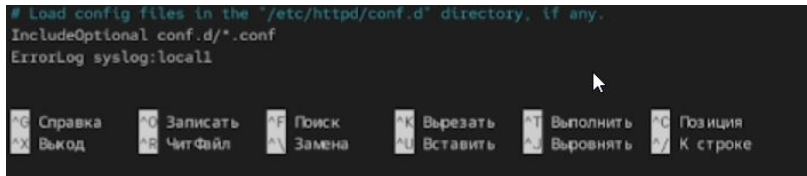


Рис. 10: Добавление строки в файл и сохранение.

Изменение правил rsyslog.conf

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. 11, рис. 12).

Изменение правил rsyslog.conf

```
root@akpperfilov:~# cd /etc/rsyslog.d
root@akpperfilov:/etc/rsyslog.d# touch httpd.conf
root@akpperfilov:/etc/rsyslog.d# nano httpd.conf
```

Рис. 11: Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование.

Изменение правил rsyslog.conf

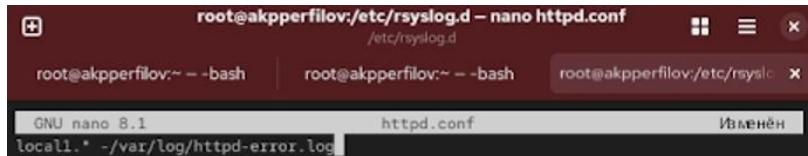


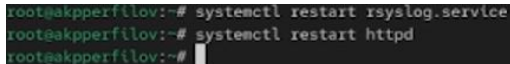
Рис. 12: Добавление строки в файл и сохранение.

Изменение правил rsyslog.conf

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. 13).



```
root@akpperfilov:~# systemctl restart rsyslog.service
root@akpperfilov:~# systemctl restart httpd
root@akpperfilov:~#
```

Рис. 13: Открытие первой вкладки терминала и перезагрузка конфигурации rsyslogd и веб-службы.

Изменение правил rsyslog.conf

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. 14)].

A screenshot of a terminal window showing a series of commands and their outputs. The prompt is root@akpperfilov:~#. The commands are: cd /etc/rsyslog.d, touch debug.conf, and echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf. The output of the last command is root@akpperfilov:~#.

```
root@akpperfilov:~# cd /etc/rsyslog.d
root@akpperfilov:~# touch debug.conf
root@akpperfilov:~# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@akpperfilov:~#
```

Рис. 14: Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.

Изменение правил rsyslog.conf

В первой вкладке терминала снова перезапустим rsyslogd: `systemctl restart rsyslog.service` (рис. 15).

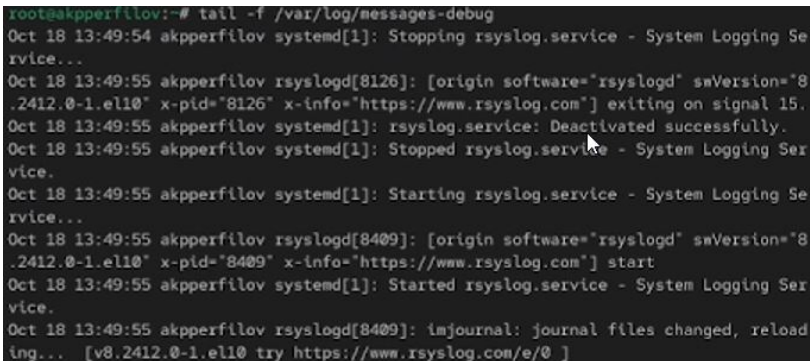


```
root@akpperfilov:~# systemctl restart rsyslog.service
root@akpperfilov:~#
```

Рис. 15: Открытие первой вкладки терминала и перезапуск rsyslogd.

Изменение правил rsyslog.conf

Во второй вкладке терминала запустим мониторинг отладочной информации: `tail -f /var/log/messages-debug` (рис. 16).



```
root@akpperfilov:~# tail -f /var/log/messages-debug
Oct 18 13:49:54 akpperfilov systemd[1]: Stopping rsyslog.service - System Logging Service...
Oct 18 13:49:55 akpperfilov rsyslogd[8126]: [origin software="rsyslogd" smVersion="8.2412.0-1.el10" x-pid="8126" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 13:49:55 akpperfilov systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 13:49:55 akpperfilov systemd[1]: Stopped rsyslog.service - System Logging Service.
Oct 18 13:49:55 akpperfilov systemd[1]: Starting rsyslog.service - System Logging Service...
Oct 18 13:49:55 akpperfilov rsyslogd[8409]: [origin software="rsyslogd" smVersion="8.2412.0-1.el10" x-pid="8409" x-info="https://www.rsyslog.com"] start
Oct 18 13:49:55 akpperfilov systemd[1]: Started rsyslog.service - System Logging Service.
Oct 18 13:49:55 akpperfilov rsyslogd[8409]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
```

Рис. 16: Открытие второй вкладки терминала и запуск мониторинга отладочной информации.

Изменение правил rsyslog.conf

В третьей вкладке терминала введём: `logger -p daemon.debug "Daemon Debug Message"` (рис. 17).




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

Рис. 17: Открытие третьей вкладки терминала и ввод команды.

Изменение правил rsyslog.conf

В терминале с мониторингом посмотрим сообщение отладки. Чтобы закрыть трассировку файла журнала, используем Ctrl + c (рис. 18).



```
Oct 18 13:49:55 akpperfilov rsyslogd[8409]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Oct 18 13:50:24 akpperfilov root[8449]: Daemon Debug Message
^C
root@akpperfilov:~#
```

Рис. 18: Просмотр сообщения отладки и закрытие трассировки файла журнала.

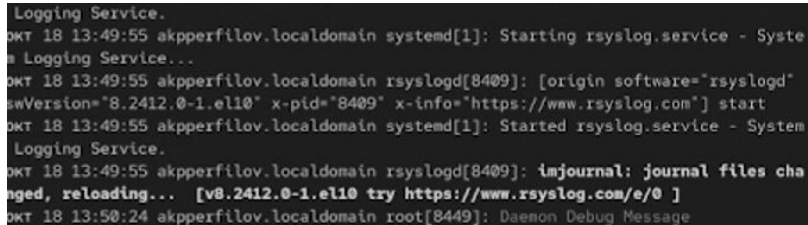
Использование journalctl

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. 19).

```
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: Linux version 6.12.0-55.32.1.el10_0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-provided physical RAM map:
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc00-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff0000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: NX (Execute Disable) protection: ac
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: APIC: Static calls initialized
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: SMBIOS 2.5 present.
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: DMI: innotek GmbH VirtualBox/Virtua
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: DMI: Memory slots populated: 0/0
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: Hypervisor detected: KVM
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 0
```

Использование journalctl

Посмотрим содержимое журнала без использования пейджера: journalctl – no-pager (рис. 20).



```
Logging Service.  
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Starting rsyslog.service - System Logging Service...  
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="8409" x-info="https://www.rsyslog.com"] start  
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Started rsyslog.service - System Logging Service.  
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]  
окт 18 13:50:24 akpperfilov.localdomain root[8449]: Daemon Debug Message
```

Рис. 20: Просмотр содержимого журнала без использования пейджера.

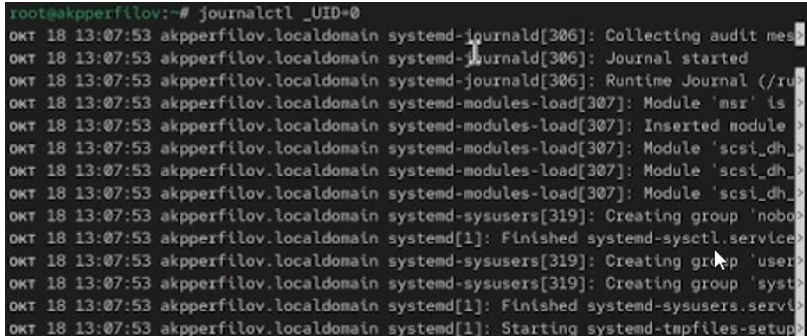
Использование journalctl

Режим просмотра журнала в реальном времени: `journalctl -f`. Для прерывания просмотра: `Ctrl + c` (рис. 21).

```
root@akpperfilov:~# journalctl -f
окт 18 13:48:45 akpperfilov.localdomain systemd[1]: Started httpd.service - The Apache HTTP Server.
окт 18 13:49:54 akpperfilov.localdomain systemd[1]: Stopping rsyslog.service - System Logging Service...
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8126]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="8126" x-info="https://www.rsyslog.com"] exiting on signal 15.
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Stopped rsyslog.service - System Logging Service.
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Starting rsyslog.service - System Logging Service...
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="8409" x-info="https://www.rsyslog.com"] start
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Started rsyslog.service - System Logging Service.
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
```

Использование journalctl

Посмотрим события для UID0: journalctl _UID=0 (рис. 22).

A screenshot of a terminal window with a dark background and light green text. The prompt is 'root@akpperfilov:~#'. The command 'journalctl _UID=0' has been entered. The output shows a series of log messages from the system journal, all filtered for UID=0. The messages include the journal starting, runtime journal location, module loading (msr, scsi_dh), and user group creation (nobody, user, systemd).

```
root@akpperfilov:~# journalctl _UID=0
окт 18 13:07:53 akpperfilov.localdomain systemd-journald[306]: Collecting audit messages
окт 18 13:07:53 akpperfilov.localdomain systemd-journald[306]: Journal started
окт 18 13:07:53 akpperfilov.localdomain systemd-journald[306]: Runtime Journal (/run
окт 18 13:07:53 akpperfilov.localdomain systemd-modules-load[307]: Module 'msr' is >
окт 18 13:07:53 akpperfilov.localdomain systemd-modules-load[307]: Inserted module >
окт 18 13:07:53 akpperfilov.localdomain systemd-modules-load[307]: Module 'scsi_dh_>
окт 18 13:07:53 akpperfilov.localdomain systemd-modules-load[307]: Module 'scsi_dh_>
окт 18 13:07:53 akpperfilov.localdomain systemd-modules-load[307]: Module 'scsi_dh_>
окт 18 13:07:53 akpperfilov.localdomain systemd-sysusers[319]: Creating group 'nobod
окт 18 13:07:53 akpperfilov.localdomain systemd[1]: Finished systemd-sysctl.service
окт 18 13:07:53 akpperfilov.localdomain systemd-sysusers[319]: Creating group 'user
окт 18 13:07:53 akpperfilov.localdomain systemd-sysusers[319]: Creating group 'sysd
окт 18 13:07:53 akpperfilov.localdomain systemd[1]: Finished systemd-sysusers.servi
окт 18 13:07:53 akpperfilov.localdomain systemd[1]: Starting systemd-tmpfiles-setup
```

Рис. 22: Просмотр событий для UID0.

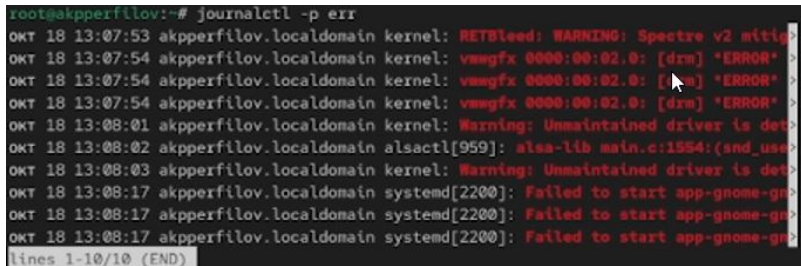
Использование journalctl

Для отображения последних 20 строк журнала введём: `journalctl -n 20` (рис. 23).

```
root@akpperfilov:~# journalctl -n 20
окт 18 13:48:35 akpperfilov.localdomain systemd[1]: Starting rsyslog.service - Syst
окт 18 13:48:35 akpperfilov.localdomain rsyslogd[8126]: [origin software="rsyslogd">
окт 18 13:48:35 akpperfilov.localdomain systemd[1]: Started rsyslog.service - Syst
окт 18 13:48:35 akpperfilov.localdomain rsyslogd[8126]: imjournal: journal files ch>
окт 18 13:48:43 akpperfilov.localdomain systemd[1]: Stopping httpd.service - The Ap>
окт 18 13:48:45 akpperfilov.localdomain systemd[1]: httpd.service: Deactivated succ>
окт 18 13:48:45 akpperfilov.localdomain systemd[1]: Stopped httpd.service - The Apa>
окт 18 13:48:45 akpperfilov.localdomain systemd[1]: Starting httpd.service - The Ap>
окт 18 13:48:45 akpperfilov.localdomain (httpd)[8146]: httpd.service: Referenced bu>
окт 18 13:48:45 akpperfilov.localdomain httpd[8146]: Server configured, listening o>
окт 18 13:48:45 akpperfilov.localdomain systemd[1]: Started httpd.service - The Apa>
окт 18 13:49:54 akpperfilov.localdomain systemd[1]: Stopping rsyslog.service - Syst
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8126]: [origin software="rsyslogd">
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: rsyslog.service: Deactivated su>
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Stopped rsyslog.service - Syst
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Starting rsyslog.service - Syst
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: [origin software="rsyslogd">
окт 18 13:49:55 akpperfilov.localdomain systemd[1]: Started rsyslog.service - Syst
окт 18 13:49:55 akpperfilov.localdomain rsyslogd[8409]: imjournal: journal files ch>
окт 18 13:50:24 akpperfilov.localdomain root[8449]: Daemon Debug Message
lines 1-20/20 (END)
```

Использование journalctl

Для просмотра только сообщений об ошибках введём: `journalctl -p err` (рис. 24).



```
root@akpperfilov:~# journalctl -p err
окт 18 13:07:53 akpperfilov.localdomain kernel: RETbleed: WARNING: Spectre v2 mitig>
окт 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
окт 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
окт 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
окт 18 13:08:01 akpperfilov.localdomain kernel: Warning: Unmaintained driver is det>
окт 18 13:08:02 akpperfilov.localdomain alsactl[959]: alsa-lib main.c:1554:(snd_use>
окт 18 13:08:03 akpperfilov.localdomain kernel: Warning: Unmaintained driver is det>
окт 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn>
окт 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn>
окт 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn>
lines 1-10/10 (END)
```

Рис. 24: Просмотр только сообщений об ошибках.

Использование journalctl

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. 25).

```
root@akpperfilov:~# journalctl --since yesterday
OCT 18 13:07:53 akpperfilov.localdomain kernel: Linux version 6.12.0-55.32.1.el10_0
OCT 18 13:07:53 akpperfilov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-provided physical RAM map:
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x000000000000ffc00-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x000000000dfff0000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000ffff0000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0
OCT 18 13:07:53 akpperfilov.localdomain kernel: NX (Execute Disable) protection: ac
OCT 18 13:07:53 akpperfilov.localdomain kernel: APIC: Static calls initialized
OCT 18 13:07:53 akpperfilov.localdomain kernel: SMBIOS 2.5 present.
OCT 18 13:07:53 akpperfilov.localdomain kernel: DMI: innotek GmbH VirtualBox/Virtua
OCT 18 13:07:53 akpperfilov.localdomain kernel: DMI: Memory slots populated: 0/0
OCT 18 13:07:53 akpperfilov.localdomain kernel: Hypervisor detected: KVM
OCT 18 13:07:53 akpperfilov.localdomain kernel: kvm-clock: Using msrc 4b564d01 and
OCT 18 13:07:53 akpperfilov.localdomain kernel: kvm-clock: using sched offset of 510
OCT 18 13:07:53 akpperfilov.localdomain kernel: clocksource: kvm-clock: mask: 0xffff
OCT 18 13:07:53 akpperfilov.localdomain kernel: tsc: Detected 2904.002 MHz processor
OCT 18 13:07:53 akpperfilov.localdomain kernel: e820: update [mem 0x00000000-0x0000
OCT 18 13:07:53 akpperfilov.localdomain kernel: e820: remove [mem 0x00000000-0x0000
OCT 18 13:07:53 akpperfilov.localdomain kernel: last_pfn = 0x220000 max_arch_pfn =
```

Использование journalctl

Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используем: `journalctl --since yesterday -p err`, а если нам нужна детальная информация, то используем: `journalctl -o verbose` (рис. 26).

```

root@akpperfilov:~# journalctl --since yesterday -p err
ОКТ 18 13:07:53 akpperfilov.localdomain kernel: RETbleed: WARNING: Spectre v2 mitig
ОКТ 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
ОКТ 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
ОКТ 18 13:07:54 akpperfilov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] "ERROR" >
ОКТ 18 13:08:01 akpperfilov.localdomain kernel: Warning: Unmaintained driver is det
ОКТ 18 13:08:02 akpperfilov.localdomain alsactl[959]: alsa-lib main.c:1554:(snd_usa
ОКТ 18 13:08:03 akpperfilov.localdomain kernel: Warning: Unmaintained driver is det
ОКТ 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn
ОКТ 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn
ОКТ 18 13:08:17 akpperfilov.localdomain systemd[2200]: Failed to start app-gnome-gn
root@akpperfilov:~# journalctl -o verbose
Sat 2025-10-18 13:07:53.596912 MSK [s=5eefd4cd51c24aa6b72bbc87e51abf82;i=1;b=bbd5b8b
  _SOURCE_BOOTTIME_TIMESTAMP=0
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 6.12.0-55.32.1.el10_0.x86_64 (mockbuild@iad1-prod-build00
  _BOOT_ID=bbd5b8b7d3e34e5eb384829922ef0ffa
  _MACHINE_ID=d53daec287194888a4ada4a71f550e32
  _HOSTNAME=akpperfilov.localdomain
  _RUNTIME_SCOPE=initrd
Sat 2025-10-18 13:07:53.596934 MSK [s=5eefd4cd51c24aa6b72bbc87e51abf82;i=2;b=bbd5b8b
  _SOURCE_BOOTTIME_TIMESTAMP=0

```

Использование journalctl

Для просмотра дополнительной информации о модуле sshd введём: `journalctl _SYSTEMD_UNIT=sshd.service` (рис. 27).

```
root@akpperfilov:~# journalctl _SYSTEMD_UNIT=sshd.service
окт 18 13:08:04 akpperfilov.localdomain (sshd)[1022]: sshd.service: Referenced but >
окт 18 13:08:04 akpperfilov.localdomain sshd[1022]: Server listening on 0.0.0.0 port
окт 18 13:08:04 akpperfilov.localdomain sshd[1022]: Server listening on :: port 22.
lines 1-3/3 (END)
```

Рис. 27: Просмотр дополнительной информации о модуле sshd.

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. 28).

Постоянный журнал journald

```
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Сб окт 18 13:41:07 MSK 2025 на pts/2
root@akpperfilov:~# mkdir -p /var/log/journal
root@akpperfilov:~# chown root:systemd-journal /var/log/journal
root@akpperfilov:~# chmod 2755 /var/log/journal
root@akpperfilov:~# killall -USR1 systemd-journald
root@akpperfilov:~# journalctl -b
окт 18 13:07:53 akpperfilov.localdomain kernel: Linux version 6.12.0-55.32.1.el10_0
окт 18 13:07:53 akpperfilov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-provided physical RAM map:
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x000000000dff0000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0
окт 18 13:07:53 akpperfilov.localdomain kernel: NX (Execute Disable) protection: ac
окт 18 13:07:53 akpperfilov.localdomain kernel: APIC: Static calls initialized
```

Рис. 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.

Выводы

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