

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

дисциплина: Основы администрирования операционных систем

Студент: Ко Антон Геннадьевич

Студ. билет № 1132221551

Группа: НПИбд-02-23

МОСКВА

2024 г.

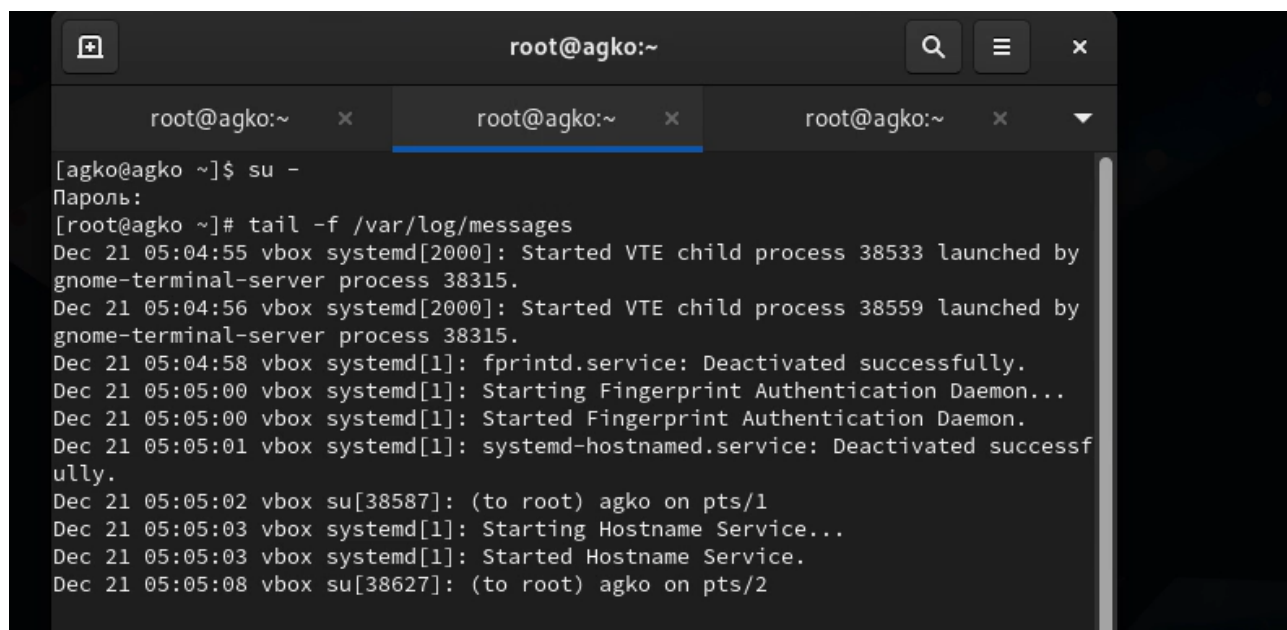
Цель работы:

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

Выполнение 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. 1.1):



```
root@agko:~  
[agko@agko ~]$ su -  
Пароль:  
[root@agko ~]# tail -f /var/log/messages  
Dec 21 05:04:55 vbox systemd[2000]: Started VTE child process 38533 launched by  
gnome-terminal-server process 38315.  
Dec 21 05:04:56 vbox systemd[2000]: Started VTE child process 38559 launched by  
gnome-terminal-server process 38315.  
Dec 21 05:04:58 vbox systemd[1]: fprintd.service: Deactivated successfully.  
Dec 21 05:05:00 vbox systemd[1]: Starting Fingerprint Authentication Daemon...  
Dec 21 05:05:00 vbox systemd[1]: Started Fingerprint Authentication Daemon.  
Dec 21 05:05:01 vbox systemd[1]: systemd-hostnamed.service: Deactivated successf  
ully.  
Dec 21 05:05:02 vbox su[38587]: (to root) agko on pts/1  
Dec 21 05:05:03 vbox systemd[1]: Starting Hostname Service...  
Dec 21 05:05:03 vbox systemd[1]: Started Hostname Service.  
Dec 21 05:05:08 vbox su[38627]: (to root) agko on pts/2
```

Рис. 1.1. Запуск трёх вкладок терминала, получение полномочий администратора в каждой вкладке, запуск на второй вкладке терминала мониторинга системных событий в реальном времени.

В третьей вкладке терминала вернёмся к учётной записи своего пользователя (нажав **Ctrl + d**) и попробуем получить полномочия администратора, но при этом вводим неправильный пароль (Рис. 1.2):

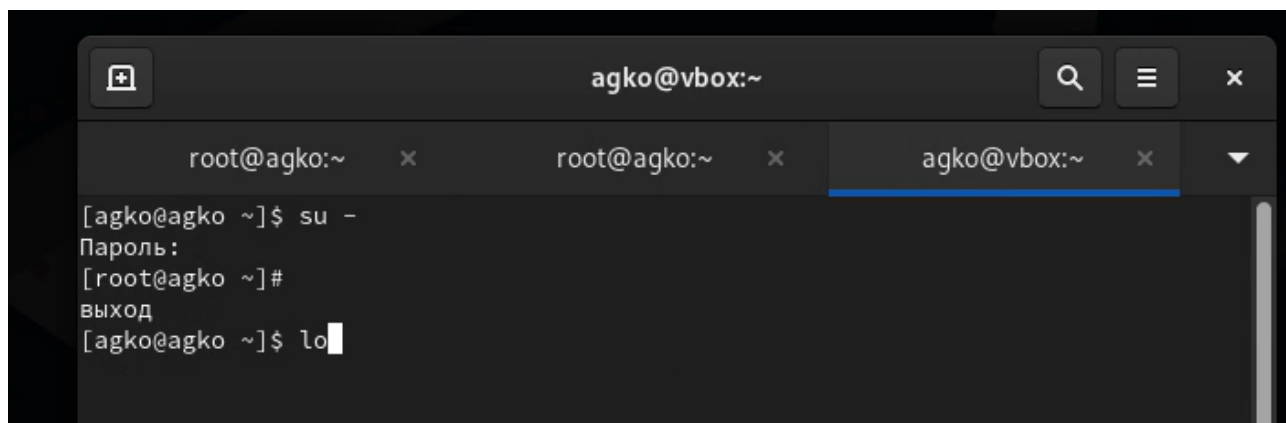


Рис. 1.2. Возвращение учётной записи своего пользователя в третьей вкладке терминала, попытка получения полномочий администратора.

Обратим внимание, что во второй вкладке терминала с мониторингом событий появилось сообщение «**FAILED SU (to root) agko on pts/2**». Отображаемые на экране сообщения также фиксируются в файле `/var/log/messages` (Рис. 1.3):

```
Dec 21 05:05:48 vbox systemd[1]: Starting Fingerprint Authentication Daemon...
Dec 21 05:05:48 vbox systemd[1]: Started Fingerprint Authentication Daemon.
Dec 21 05:05:51 vbox su[38668]: FAILED SU (to root) agko on pts/2
```

Рис. 1.3. Новое сообщение в мониторинге событий во второй вкладке терминала.

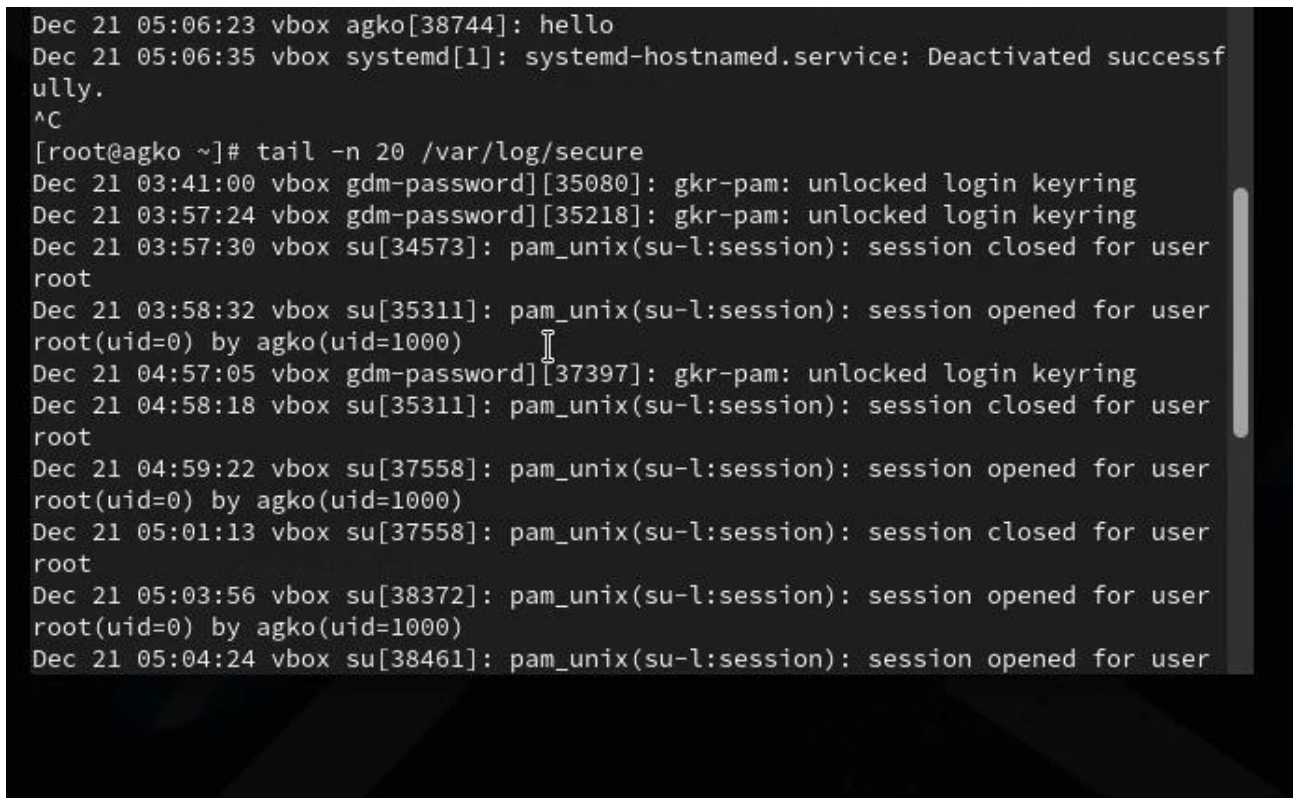
В третьей вкладке терминала из оболочки пользователя введём: **logger hello** (Рис. 1.4):

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

Рис. 1.4. Ввод в третьей вкладке терминала.

Далее возвращаемся во вторую вкладку терминала с мониторингом событий и видим сообщение, которое также будет зафиксировано в файле `/var/log/messages` («**hello**»). В этой же вкладке терминала с мониторингом

остановим трассировку файла сообщений мониторинга реального времени, используя **Ctrl + c**. Затем запустим мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов): **tail -n 20 /var/log/secure**. Мы видим сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды **su -** (Рис. 1.5):

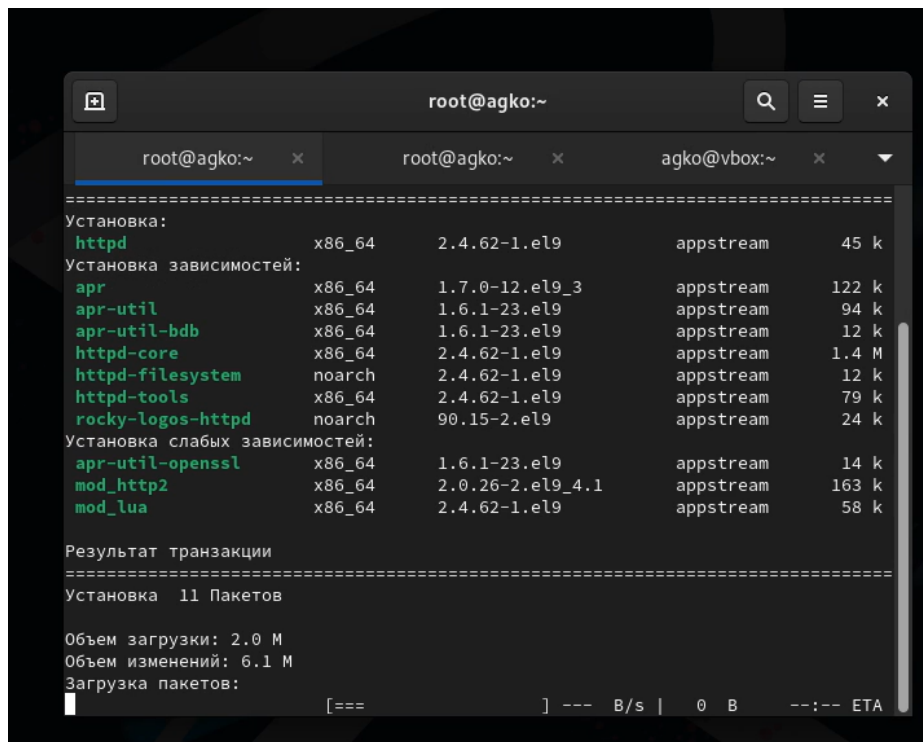


```
Dec 21 05:06:23 vbox agko[38744]: hello
Dec 21 05:06:35 vbox systemd[1]: systemd-hostnamed.service: Deactivated successfully.
^C
[root@agko ~]# tail -n 20 /var/log/secure
Dec 21 03:41:00 vbox gdm-password[35080]: gkr-pam: unlocked login keyring
Dec 21 03:57:24 vbox gdm-password[35218]: gkr-pam: unlocked login keyring
Dec 21 03:57:30 vbox su[34573]: pam_unix(su-l:session): session closed for user root
Dec 21 03:58:32 vbox su[35311]: pam_unix(su-l:session): session opened for user root(uid=0) by agko(uid=1000)
Dec 21 04:57:05 vbox gdm-password[37397]: gkr-pam: unlocked login keyring
Dec 21 04:58:18 vbox su[35311]: pam_unix(su-l:session): session closed for user root
Dec 21 04:59:22 vbox su[37558]: pam_unix(su-l:session): session opened for user root(uid=0) by agko(uid=1000)
Dec 21 05:01:13 vbox su[37558]: pam_unix(su-l:session): session closed for user root
Dec 21 05:03:56 vbox su[38372]: pam_unix(su-l:session): session opened for user root(uid=0) by agko(uid=1000)
Dec 21 05:04:24 vbox su[38461]: pam_unix(su-l:session): session opened for user
```

Рис. 1.5. Возвращение во вторую вкладку терминала с мониторингом событий, просмотр сообщения, остановка трассировки файла сообщений мониторинга реального времени, запуск мониторинга сообщений безопасности (последние 20 строк).

Изменение правил **rsyslog.conf**:

В первой вкладке терминала установим Apache: **dnf -y install httpd** (Рис. 2.1).



```
root@agko:~  
=====
```

Установка:	архитектура	версия	источник	размер
httpd	x86_64	2.4.62-1.el9	appstream	45 k

```
Установка зависимостей:
```

пакет	архитектура	версия	источник	размер
apr	x86_64	1.7.0-12.el9_3	appstream	122 k
apr-util	x86_64	1.6.1-23.el9	appstream	94 k
apr-util-bdb	x86_64	1.6.1-23.el9	appstream	12 k
httpd-core	x86_64	2.4.62-1.el9	appstream	1.4 M
httpd-filesystem	noarch	2.4.62-1.el9	appstream	12 k
httpd-tools	x86_64	2.4.62-1.el9	appstream	79 k
rocky-logos-httpd	noarch	90.15-2.el9	appstream	24 k

```
Установка слабых зависимостей:
```

пакет	архитектура	версия	источник	размер
apr-util-openssl	x86_64	1.6.1-23.el9	appstream	14 k
mod_http2	x86_64	2.0.26-2.el9_4.1	appstream	163 k
mod_lua	x86_64	2.4.62-1.el9	appstream	58 k

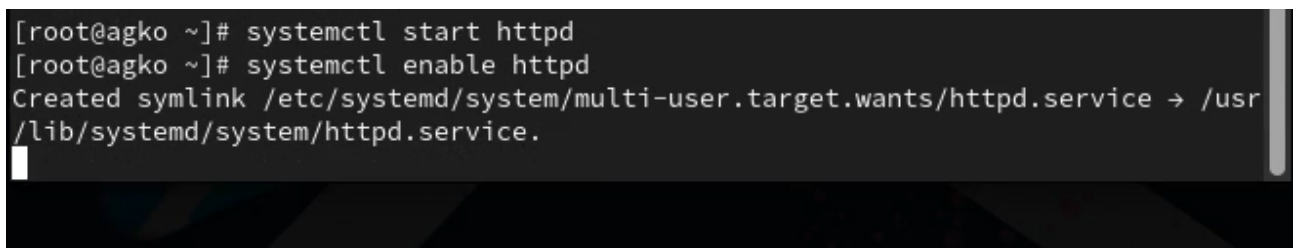
```
Результат транзакции  
=====
```

Установка	Пакетов
11	

```
Объем загрузки: 2.0 М  
Объем изменений: 6.1 М  
Загрузка пакетов:  
[=== ] --- B/s | 0 B --:-- ETA
```

Рис. 2.1. Установка Apache.

После окончания процесса установки запустим веб-службу: **systemctl start httpd** и **systemctl enable httpd** (Рис. 2.2).



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

Рис. 2.2. Запуск веб-службы.

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: **tail -f /var/log/httpd/error_log**. Чтобы закрыть трассировку файла журнала, используем **Ctrl + c** (Рис. 2.3).

```
[root@agko ~]# tail -f /var/log/httpd/error_log
[Sat Dec 21 05:08:28.875807 2024] [core:notice] [pid 39135:tid 39135] SELinux po
lity enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Dec 21 05:08:28.877717 2024] [suexec:notice] [pid 39135:tid 39135] AH01232:
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using fe80::a00:27ff:fee8:d6bf%enp0s3. Set the 'ServerName' directive glo
bally to suppress this message
[Sat Dec 21 05:08:29.975592 2024] [lbmethod_heartbeat:notice] [pid 39135:tid 391
35] AH02282: No slotmem from mod_heartbeat
[Sat Dec 21 05:08:29.995059 2024] [mpm_event:notice] [pid 39135:tid 39135] AH004
89: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sat Dec 21 05:08:29.995098 2024] [core:notice] [pid 39135:tid 39135] AH00094: C
ommand line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.3. Просмотр журнала сообщений об ошибках веб-службы, закрытие трассировки файла журнала.

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавляем (Рис. 2.4) следующую строку: **ErrorLog syslog:local** (Рис. 2.5).

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

```
[root@agko ~]# vim /etc/httpd/conf/
```

Рис. 2.4. Получение в третьей вкладке терминала полномочия администратора, открытие файла `httpd.conf` на редактирование.

```
includeOptional conf.d/*.conf
ErrorLog syslog:local
"/etc/httpd/conf/httpd.conf" 360L, 12029B записано 360,22 Внизу
```

Рис. 2.5. Добавление строки в файл и сохранение.

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

```
cd /etc/rsyslog.d
```

```
touch httpd.conf
```

Открыв его на редактирование (Рис. 2.6), 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.

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

Рис. 2.6. Создание в каталоге /etc/rsyslog.d файла мониторинга событий веб-службы и открытие его на редактирование.

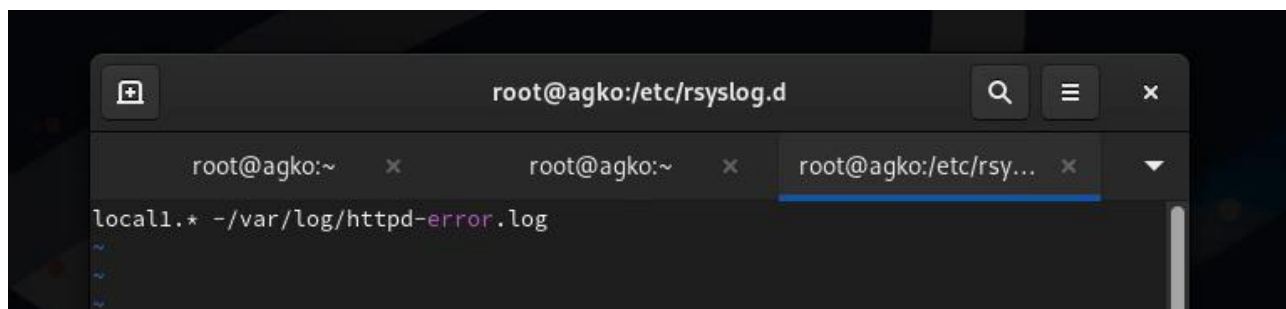


Рис. 2.7. Добавление строки в файл и сохранение.

Перейдём в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу (Рис. 2.8):

```
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.

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

Рис. 2.8. Открытие первой вкладки терминала и перезагрузка конфигурации `rsyslogd` и веб-службы.

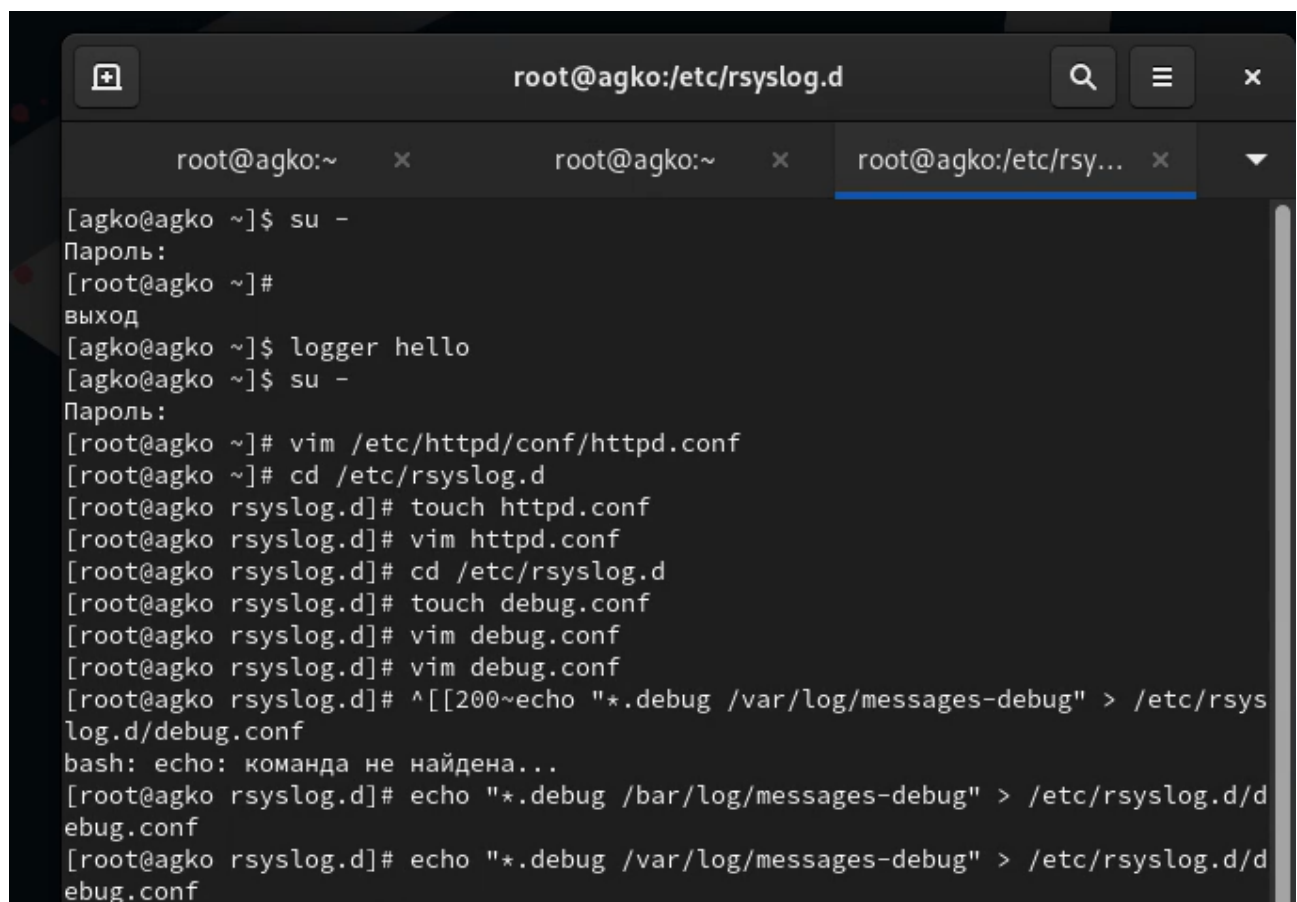
В третьей вкладке терминала создаём отдельный файл конфигурации для мониторинга отладочной информации:

```
cd /etc/rsyslog.d
```

```
touch debug.conf
```

В этом же терминале вводим:

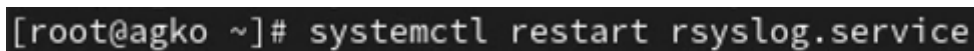
echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf (Рис. 2.9):



```
root@agko:/etc/rsyslog.d
[agko@agko ~]$ su -
Пароль:
[root@agko ~]#
выход
[agko@agko ~]$ logger hello
[agko@agko ~]$ su -
Пароль:
[root@agko ~]# vim /etc/httpd/conf/httpd.conf
[root@agko ~]# cd /etc/rsyslog.d
[root@agko rsyslog.d]# touch httpd.conf
[root@agko rsyslog.d]# vim httpd.conf
[root@agko rsyslog.d]# cd /etc/rsyslog.d
[root@agko rsyslog.d]# touch debug.conf
[root@agko rsyslog.d]# vim debug.conf
[root@agko rsyslog.d]# ^[[200~echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
bash: echo: команда не найдена...
[root@agko rsyslog.d]# echo "*.debug /bar/log/messages-debug" > /etc/rsyslog.d/d
ebug.conf
[root@agko rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/d
ebug.conf
```


Рис. 2.9. Открытие третьей вкладки терминала, создание отдельного файла конфигурации для мониторинга отладочной информации, ввод заданной строки.

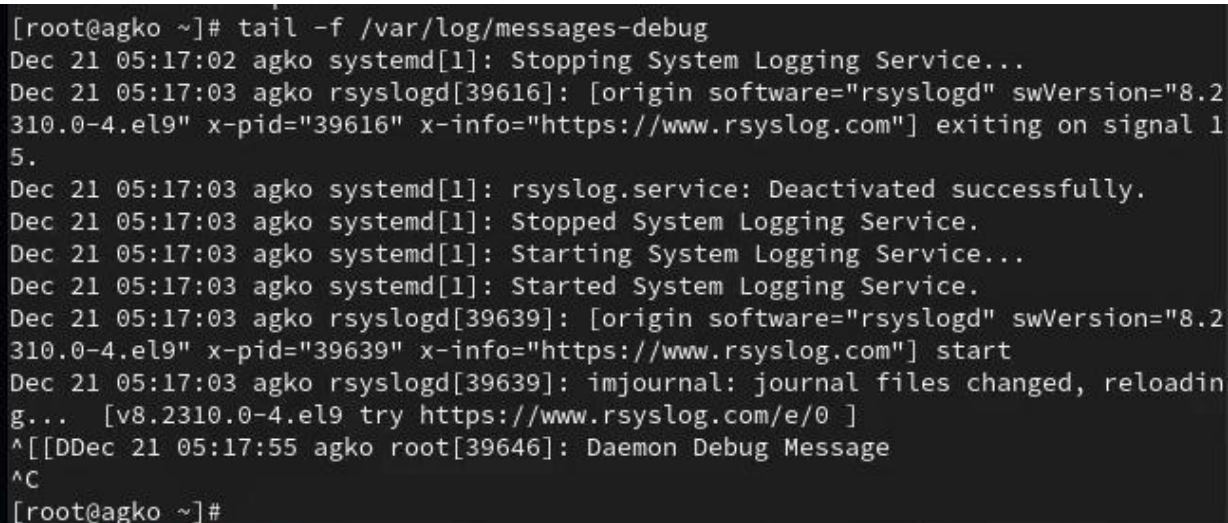
В первой вкладке терминала снова перезапустим rsyslogd: **systemctl restart rsyslog.service** (Рис. 2.10):



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

Рис. 2.10. Открытие первой вкладки терминала и перезапуск rsyslogd.

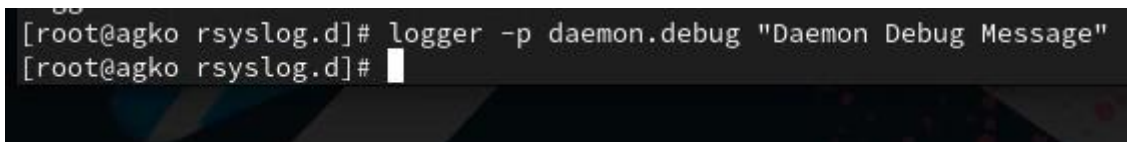
Во второй вкладке терминала запустим мониторинг отладочной информации: **tail -f /var/log/messages-debug** (Рис. 2.11):



```
[root@agko ~]# tail -f /var/log/messages-debug
Dec 21 05:17:02 agko systemd[1]: Stopping System Logging Service...
Dec 21 05:17:03 agko rsyslogd[39616]: [origin software="rsyslogd" swVersion="8.2
310.0-4.el9" x-pid="39616" x-info="https://www.rsyslog.com"] exiting on signal 1
5.
Dec 21 05:17:03 agko systemd[1]: rsyslog.service: Deactivated successfully.
Dec 21 05:17:03 agko systemd[1]: Stopped System Logging Service.
Dec 21 05:17:03 agko systemd[1]: Starting System Logging Service...
Dec 21 05:17:03 agko systemd[1]: Started System Logging Service.
Dec 21 05:17:03 agko rsyslogd[39639]: [origin software="rsyslogd" swVersion="8.2
310.0-4.el9" x-pid="39639" x-info="https://www.rsyslog.com"] start
Dec 21 05:17:03 agko rsyslogd[39639]: imjournal: journal files changed, reloadin
g... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
^[[DDec 21 05:17:55 agko root[39646]: Daemon Debug Message
^C
[root@agko ~]#
```

Рис. 2.11. Открытие второй вкладки терминала и запуск мониторинга отладочной информации.

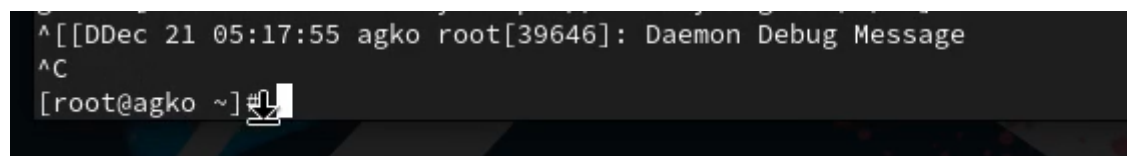
В третьей вкладке терминала введём: **logger -p daemon.debug "Daemon Debug Message"** (Рис. 2.12):



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

Рис. 2.12. Открытие третьей вкладки терминала и ввод команды.

В терминале с мониторингом посмотрим сообщение отладки. Чтобы закрыть трассировку файла журнала, используем Ctrl + c (Рис. 2.13):

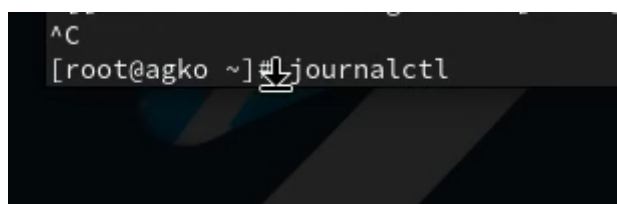


```
^[[DDec 21 05:17:55 agko root[39646]: Daemon Debug Message
^C
[root@agko ~]#
```

Рис. 2.13. 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. 3.1).



```
^C
[root@agko ~]# journalctl
```

Рис. 3.1. Открытие второй вкладки терминала и просмотр содержимого журнала с событиями с момента последнего запуска системы.

Посмотрим содержимое журнала без использования пейджера: **journalctl --no-pager** (Рис. 3.2).

```
bash: q: команда не найдена...
[root@agko ~]# journalctl --no-pager
```

Рис. 3.2. Просмотр содержимого журнала без использования пейджера.

Режим просмотра журнала в реальном времени: **journalctl -f**. Для прерывания просмотра: **Ctrl + c** (Рис. 3.3).

```
[root@agko ~]# journalctl -f
дек 21 05:17:02 agko systemd[1]: Stopping System Logging Service...
дек 21 05:17:03 agko rsyslogd[39616]: [origin software="rsyslogd" swVersion="8.2
310.0-4.el9" x-pid="39616" x-info="https://www.rsyslog.com"] exiting on signal 1
5.
дек 21 05:17:03 agko systemd[1]: rsyslog.service: Deactivated successfully.
дек 21 05:17:03 agko systemd[1]: Stopped System Logging Service.
дек 21 05:17:03 agko systemd[1]: Starting System Logging Service...
дек 21 05:17:03 agko systemd[1]: Started System Logging Service.
дек 21 05:17:03 agko rsyslogd[39639]: [origin software="rsyslogd" swVersion="8.2
310.0-4.el9" x-pid="39639" x-info="https://www.rsyslog.com"] start
дек 21 05:17:03 agko rsyslogd[39639]: imjournal: journal files changed, reloadin
g... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
дек 21 05:17:55 agko root[39646]: Daemon Debug Message
дек 21 05:19:08 agko PackageKit[39630]: search-file transaction /67_aaeadcee fro
m uid 0 finished with success after 41ms
^C
[root@agko ~]# journal
```

Рис. 3.3. Режим просмотра журнала в реальном времени и прерывание просмотра.

Посмотрим события для UID0: **journalctl _UID=0** (Рис. 3.4).

```
[root@agko ~]# journalctl _UID=0
```

Рис. 3.4. Просмотр событий для UID0.

Для отображения последних 20 строк журнала введём: **journalctl -n 20** (Рис. 3.5).


```
[root@agko ~]# journalctl -n 20
дек 21 05:14:10 agko rsyslogd[39616]: action '*' treated as ':omusrmsg:*' - ple>
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/>
дек 21 05:14:10 agko rsyslogd[39616]: invalid character in selector line - ';te>
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/>
дек 21 05:14:10 agko rsyslogd[39616]: [origin software="rsyslogd" swVersion="8.>
дек 21 05:14:10 agko rsyslogd[39616]: imjournal: journal files changed, reloadi>
дек 21 05:15:36 agko systemd[1]: Starting PackageKit Daemon...
дек 21 05:15:36 agko PackageKit[39630]: daemon start
дек 21 05:15:36 agko systemd[1]: Started PackageKit Daemon.
дек 21 05:15:37 agko PackageKit[39630]: search-file transaction /66_eeadbedb fr>
дек 21 05:17:02 agko systemd[1]: Stopping System Logging Service...
дек 21 05:17:03 agko rsyslogd[39616]: [origin software="rsyslogd" swVersion="8.>
дек 21 05:17:03 agko systemd[1]: rsyslog.service: Deactivated successfully.
дек 21 05:17:03 agko systemd[1]: Stopped System Logging Service.
дек 21 05:17:03 agko systemd[1]: Starting System Logging Service...
дек 21 05:17:03 agko systemd[1]: Started System Logging Service.
дек 21 05:17:03 agko rsyslogd[39639]: [origin software="rsyslogd" swVersion="8.>
дек 21 05:17:03 agko rsyslogd[39639]: imjournal: journal files changed, reloadi>
дек 21 05:17:55 agko root[39646]: Daemon Debug Message
дек 21 05:19:08 agko PackageKit[39630]: search-file transaction /67_aaeadcee fr>
lines 1-20/20 (END)
```

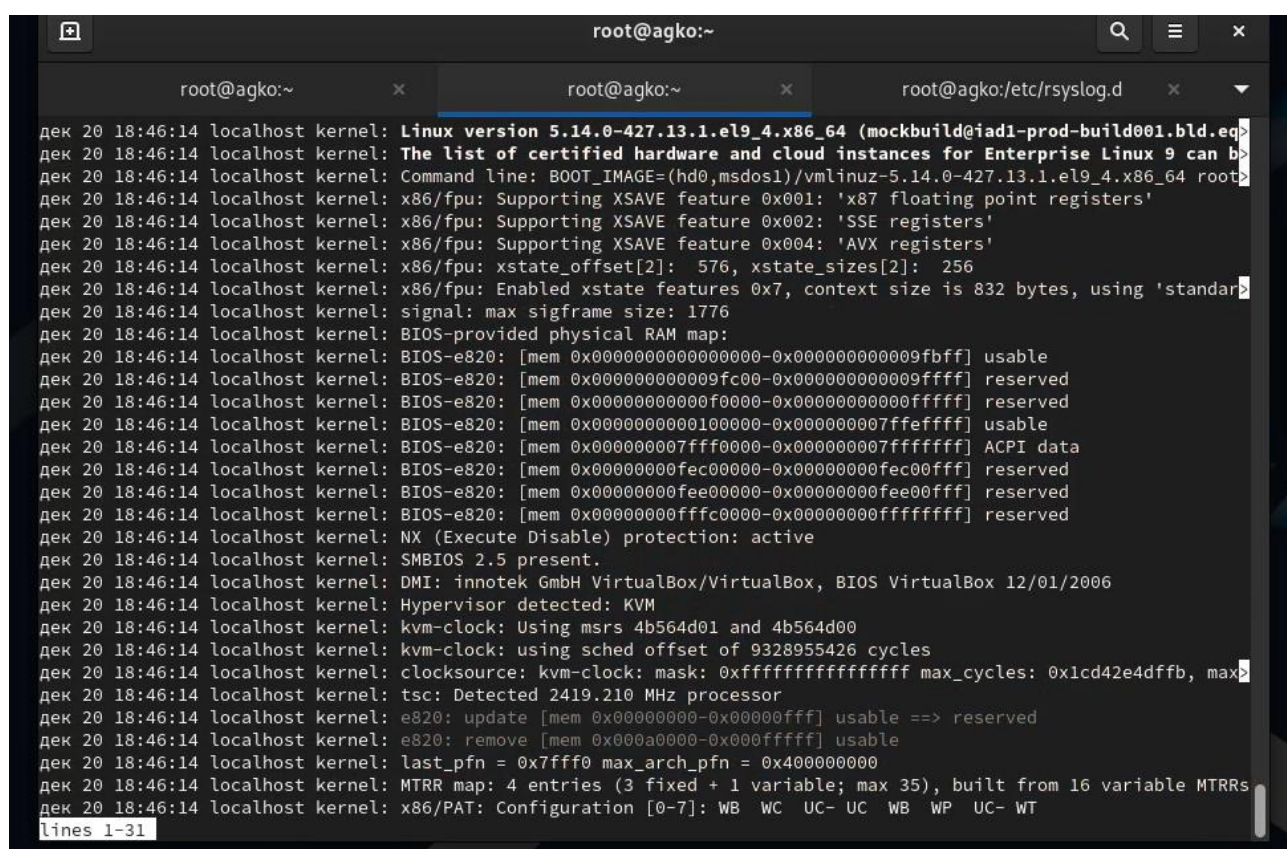
Рис. 3.5. Отображение последних 20 строк журнала.

Для просмотра только сообщений об ошибках введём: **journalctl -p err** (Рис. 3.6).

```
root@agko:~ x root@agko:~ x root@agko:/etc/rsyslog.d x
дек 20 18:46:14 localhost systemd[1]: Invalid DMI field header.
дек 20 18:46:15 localhost kernel: Warning: Unmaintained driver is detected: e1000
дек 20 18:46:16 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported>
дек 20 18:46:16 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
дек 20 18:46:16 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device>
дек 20 18:46:21 localhost systemd[1]: Invalid DMI field header.
дек 20 18:46:21 localhost systemd-fstab-generator[675]: Failed to create unit file '/run/systemd/generator/-.moun>
дек 20 18:46:21 localhost systemd-fstab-generator[675]: Failed to create unit file '/run/systemd/generator/boot.m>
дек 20 18:46:21 localhost systemd-fstab-generator[675]: Failed to create unit file '/run/systemd/generator/dev-ma>
дек 20 18:46:21 localhost systemd[667]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with ex>
дек 20 18:46:25 localhost alsactl[926]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0>
дек 20 18:46:27 localhost kernel: Warning: Unmaintained driver is detected: ip_set
дек 20 18:46:30 vbox rsyslogd[1159]: imjournal: fscanf on state file '/var/lib/rsyslog/imjournal.state' failed |>
дек 20 18:46:30 vbox rsyslogd[1159]: imjournal: ignoring invalid state file /var/lib/rsyslog/imjournal.state [v8.>
дек 20 18:46:50 vbox gdm-password[1981]: gkr-pam: unable to locate daemon control file
дек 20 18:47:01 vbox gdm-wayland-session[1142]: Glib: Source ID 2 was not found when attempting to remove it
дек 20 18:47:01 vbox gdm-launch-environment[1088]: Glib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object)>
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/-.mount',>
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/boot.mount>
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/dev-mapper>
дек 20 18:53:14 vbox systemd[2971]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit s>
дек 20 19:01:23 vbox kernel: md/raid1:md0: Disk failure on sde1, disabling device.
дек 20 19:01:23 vbox kernel: md/raid1:md0: Operation continuing on 1 devices.
дек 20 19:05:34 vbox kernel: md/raid1:md0: Disk failure on sde1, disabling device.
дек 20 19:05:34 vbox kernel: md/raid1:md0: Operation continuing on 1 devices.
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/-.mount',>
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/boot.moun>
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/dev-mappe>
дек 21 04:08:41 agko systemd[36146]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>
дек 21 05:08:09 agko systemd[38804]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>
дек 21 05:08:09 agko systemd-fstab-generator[38812]: Failed to create unit file '/run/systemd/generator/-.mount',>
lines 1-31
```

Рис. 3.6. Просмотр только сообщений об ошибках.

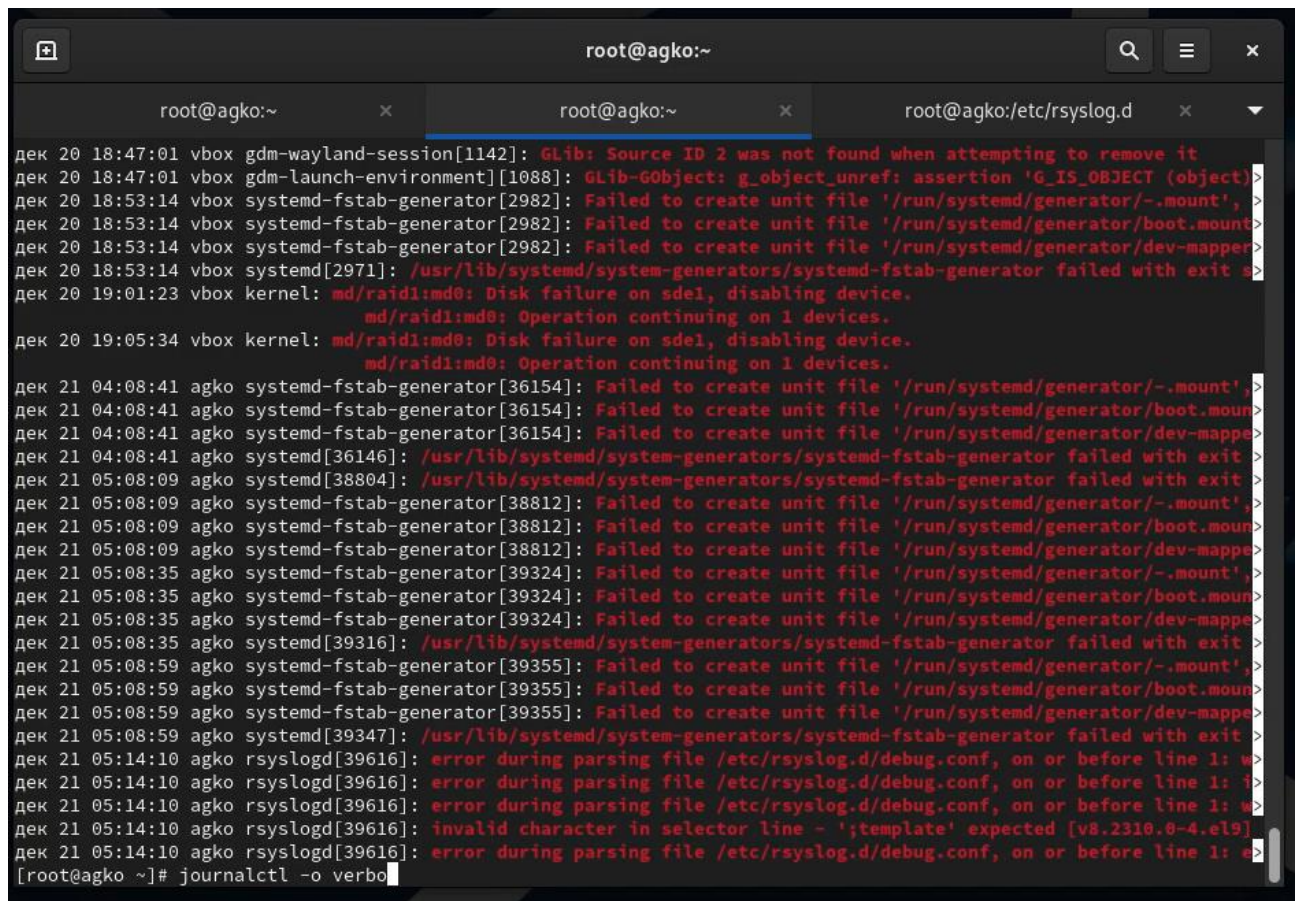
Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, мы можем использовать параметры `--since` и `--until`. Обе опции принимают параметр времени в формате `YYYY-MM-DD hh:mm:ss`. Кроме того, мы можем использовать `yesterday`, `today` и `tomorrow` в качестве параметров. Например, для просмотра всех сообщений со вчерашнего дня введём: **`journalctl --since yesterday`** (Рис. 3.7).



```
root@agko:~  
дек 20 18:46:14 localhost kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.e  
дек 20 18:46:14 localhost kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be  
дек 20 18:46:14 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x86_64 root  
дек 20 18:46:14 localhost kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'  
дек 20 18:46:14 localhost kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'  
дек 20 18:46:14 localhost kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'  
дек 20 18:46:14 localhost kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256  
дек 20 18:46:14 localhost kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard  
дек 20 18:46:14 localhost kernel: signal: max sigframe size: 1776  
дек 20 18:46:14 localhost kernel: BIOS-provided physical RAM map:  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000fffff] reserved  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000007ffeffff] usable  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x000000000007fff0000-0x000000000007ffffff] ACPI data  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved  
дек 20 18:46:14 localhost kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000ffffff] reserved  
дек 20 18:46:14 localhost kernel: NX (Execute Disable) protection: active  
дек 20 18:46:14 localhost kernel: SMBIOS 2.5 present.  
дек 20 18:46:14 localhost kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006  
дек 20 18:46:14 localhost kernel: Hypervisor detected: KVM  
дек 20 18:46:14 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
дек 20 18:46:14 localhost kernel: kvm-clock: using sched offset of 9328955426 cycles  
дек 20 18:46:14 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max  
дек 20 18:46:14 localhost kernel: tsc: Detected 2419.210 MHz processor  
дек 20 18:46:14 localhost kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved  
дек 20 18:46:14 localhost kernel: e820: remove [mem 0x000a0000-0x000ffff] usable  
дек 20 18:46:14 localhost kernel: last_pfn = 0x7fff0 max_arch_pfn = 0x400000000  
дек 20 18:46:14 localhost kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35), built from 16 variable MTRRs  
дек 20 18:46:14 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT  
lines 1-31
```

Рис. 3.7. Просмотр всех сообщений со вчерашнего дня.

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. 3.8).



```
root@agko:~  
дек 20 18:47:01 vbox gdm-wayland-session[1142]: GLib: Source ID 2 was not found when attempting to remove it  
дек 20 18:47:01 vbox gdm-launch-environment[1088]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object)'  
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/-.mount',>  
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/boot.mount>  
дек 20 18:53:14 vbox systemd-fstab-generator[2982]: Failed to create unit file '/run/systemd/generator/dev-mapper>  
дек 20 18:53:14 vbox systemd[2971]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit s>  
дек 20 19:01:23 vbox kernel: md/raid1:md0: Disk failure on sde1, disabling device.  
дек 20 19:01:23 vbox kernel: md/raid1:md0: Operation continuing on 1 devices.  
дек 20 19:05:34 vbox kernel: md/raid1:md0: Disk failure on sde1, disabling device.  
дек 20 19:05:34 vbox kernel: md/raid1:md0: Operation continuing on 1 devices.  
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/-.mount'>  
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/boot.moun>  
дек 21 04:08:41 agko systemd-fstab-generator[36154]: Failed to create unit file '/run/systemd/generator/dev-mappe>  
дек 21 04:08:41 agko systemd[36146]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>  
дек 21 05:08:09 agko systemd[38804]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>  
дек 21 05:08:09 agko systemd-fstab-generator[38812]: Failed to create unit file '/run/systemd/generator/-.mount'>  
дек 21 05:08:09 agko systemd-fstab-generator[38812]: Failed to create unit file '/run/systemd/generator/boot.moun>  
дек 21 05:08:09 agko systemd-fstab-generator[38812]: Failed to create unit file '/run/systemd/generator/dev-mappe>  
дек 21 05:08:35 agko systemd-fstab-generator[39324]: Failed to create unit file '/run/systemd/generator/-.mount'>  
дек 21 05:08:35 agko systemd-fstab-generator[39324]: Failed to create unit file '/run/systemd/generator/boot.moun>  
дек 21 05:08:35 agko systemd-fstab-generator[39324]: Failed to create unit file '/run/systemd/generator/dev-mappe>  
дек 21 05:08:35 agko systemd[39316]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>  
дек 21 05:08:59 agko systemd-fstab-generator[39355]: Failed to create unit file '/run/systemd/generator/-.mount'>  
дек 21 05:08:59 agko systemd-fstab-generator[39355]: Failed to create unit file '/run/systemd/generator/boot.moun>  
дек 21 05:08:59 agko systemd-fstab-generator[39355]: Failed to create unit file '/run/systemd/generator/dev-mappe>  
дек 21 05:08:59 agko systemd[39347]: /usr/lib/systemd/system-generators/systemd-fstab-generator failed with exit>  
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/debug.conf, on or before line 1: u>  
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/debug.conf, on or before line 1: f>  
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/debug.conf, on or before line 1: u>  
дек 21 05:14:10 agko rsyslogd[39616]: invalid character in selector line - 'template' expected [v8.2310.0-4.el9]>  
дек 21 05:14:10 agko rsyslogd[39616]: error during parsing file /etc/rsyslog.d/debug.conf, on or before line 1: u>  
[root@agko ~]# journalctl -o verbo
```

Рис. 3.8. Просмотр сообщений с ошибкой приоритета, которые были зафиксированы со вчерашнего дня. Просмотр детальной информации.

Для просмотра дополнительной информации о модуле sshd введём: **journalctl _SYSTEMD_UNIT=sshd.service** (Рис. 3.9).



```
SYSLOG_IDENTIFIER=kernel  
[root@agko ~]# journalctl _SYSTEMD_UNIT=sshd.service  
дек 20 18:46:28 localhost.localdomain sshd[1060]: Server listening on 0.0.0.0 port 22.  
дек 20 18:46:28 localhost.localdomain sshd[1060]: Server listening on :: port 22.  
[root@agko ~]# journalctl -o verbose
```

Рис. 3.9. 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. 4).

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

Рис. 4. 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.

Ответы на контрольные вопросы:

1. Какой файл используется для настройки `rsyslogd`? **`/etc/rsyslog.conf`**
2. В каком файле журнала `rsyslogd` содержатся сообщения, связанные с аутентификацией? **`/var/log/secure`**
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов? **Неделя**
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**

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00? **journalctl _PID=1 -since “2022-02-01 09:00:00” –until “2022-02-01 15:00:00”**

7. Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы? **journalctl -b**

8. Какая процедура позволяет сделать журнал journald постоянным?

Запустите терминал и получите полномочия администратора: **su –**

Создайте каталог для хранения записей журнала: **mkdir -p /var/log/journal**

Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию:

chown root:systemd-journal /var/log/journal

chmod 2755 /var/log/journal

Для принятия изменений необходимо или перезагрузить систему (перезапустить службу systemd-journald недостаточно), или использовать команду: **killall -USR1 systemd-journald**

(1-4 задание в последнем блоке)

Вывод:

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