

Отчет по лабораторной работе №7

Выполнение

---

Власов А.С

18 октября 2025

Российский университет дружбы народов, Москва, Россия

- Власов Артем Сергеевич
- студент НПИбд-01-24
- номер студ. билета 1132246841
- Российский университет дружбы народов
- [1132246841@pfur.ru](mailto:1132246841@pfur.ru)

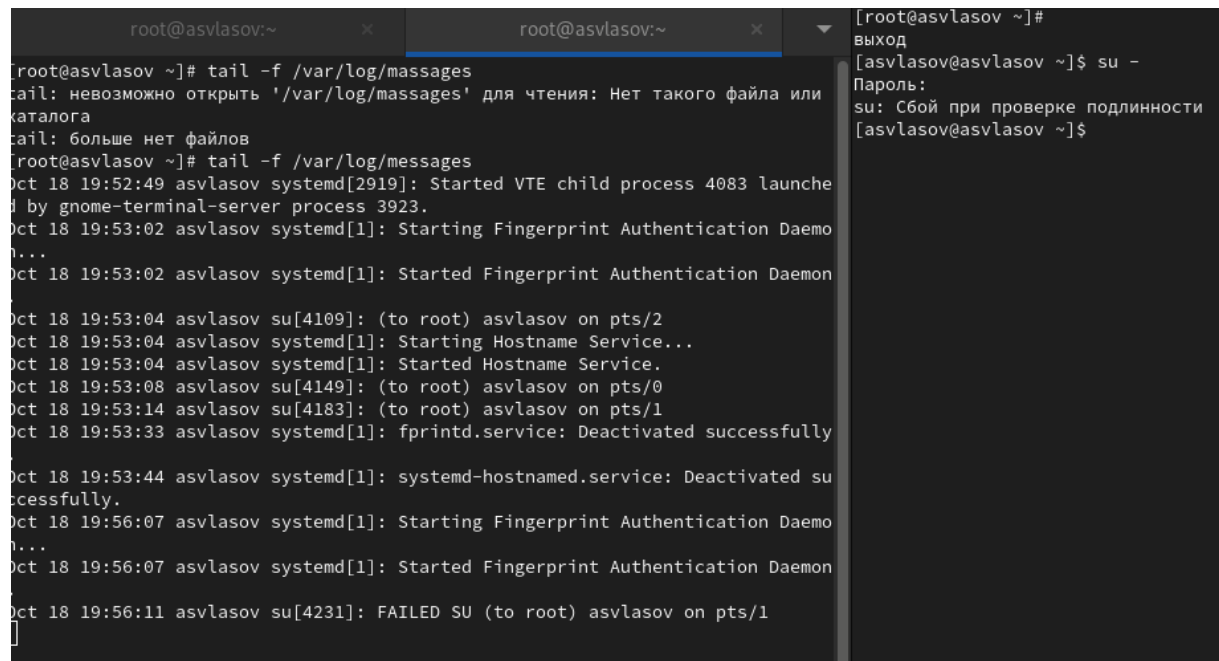
Получить навыки работы с журналами мониторинга различных событий в системе.

Продemonстрировать навыки умения работать с журналом мониторинга событий, созданием файла конфигурации мониторинга, `journald` и `journalctl`.

# Выполнение лабораторной работы

---

Запускаем 3 терминала, открываем во втором журнал мониторинга, на третьем пробуем получить права администратора с неверным паролем.

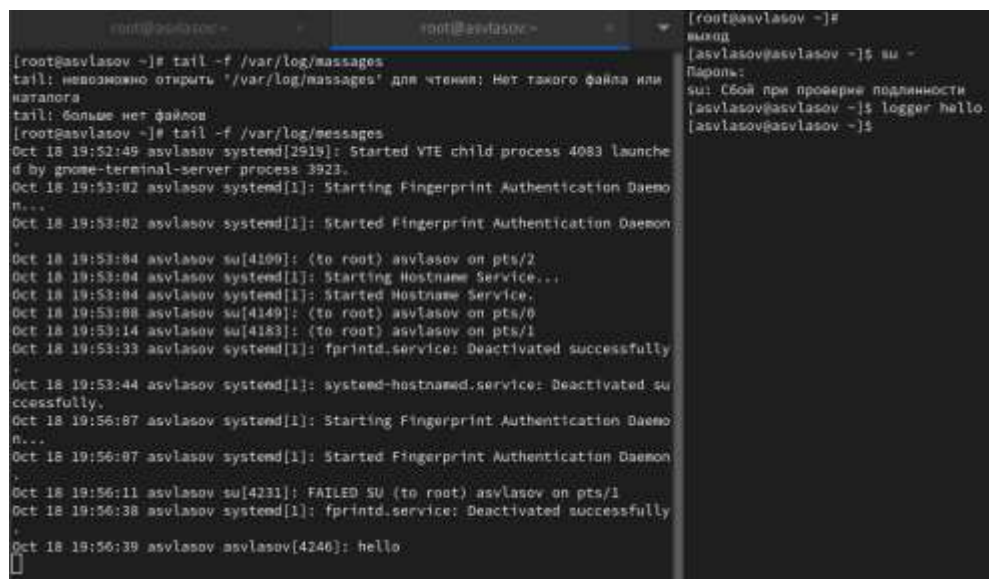


The image shows three terminal windows. The leftmost window is a root terminal with the command `tail -f /var/log/messages` running, displaying system logs. The middle window is also a root terminal with the same command running. The rightmost window is a terminal where a user has switched to root using `su -` and is prompted for a password. The user enters a password, but the system responds with an error: `su: Cбой при проверке подлинности` (su: Authentication check failed).

```
root@asvlasov:~  
[root@asvlasov ~]# tail -f /var/log/messages  
tail: невозможно открыть '/var/log/messages' для чтения: Нет такого файла или каталога  
tail: больше нет файлов  
[root@asvlasov ~]# tail -f /var/log/messages  
Oct 18 19:52:49 asvlasov systemd[2919]: Started VTE child process 4083 launched by gnome-terminal-server process 3923.  
Oct 18 19:53:02 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 18 19:53:02 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
Oct 18 19:53:04 asvlasov su[4109]: (to root) asvlasov on pts/2  
Oct 18 19:53:04 asvlasov systemd[1]: Starting Hostname Service...  
Oct 18 19:53:04 asvlasov systemd[1]: Started Hostname Service.  
Oct 18 19:53:08 asvlasov su[4149]: (to root) asvlasov on pts/0  
Oct 18 19:53:14 asvlasov su[4183]: (to root) asvlasov on pts/1  
Oct 18 19:53:33 asvlasov systemd[1]: fprintd.service: Deactivated successfully  
Oct 18 19:53:44 asvlasov systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Oct 18 19:56:07 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 18 19:56:07 asvlasov systemd[1]: Started Fingerprint Authentication Daemon  
Oct 18 19:56:11 asvlasov su[4231]: FAILED SU (to root) asvlasov on pts/1  
[
```

Рис. 1: Неверный пароль администратора

# Выводим в журнал сообщение hello.



```
root@asvlasov ~# tail -f /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Нет такого файла или каталога
tail: больше нет файлов
[root@asvlasov ~]# tail -f /var/log/messages
Oct 18 19:52:49 asvlasov systemd[2919]: Started VTE child process 4083 launched by gnome-terminal-server process 3923.
Oct 18 19:53:02 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 18 19:53:02 asvlasov systemd[1]: Started Fingerprint Authentication Daemon.
Oct 18 19:53:04 asvlasov su[4100]: (to root) asvlasov on pts/2
Oct 18 19:53:04 asvlasov systemd[1]: Starting Hostname Service...
Oct 18 19:53:04 asvlasov systemd[1]: Started Hostname Service.
Oct 18 19:53:08 asvlasov su[4149]: (to root) asvlasov on pts/0
Oct 18 19:53:14 asvlasov su[4183]: (to root) asvlasov on pts/1
Oct 18 19:53:33 asvlasov systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:53:44 asvlasov systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 18 19:56:07 asvlasov systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 18 19:56:07 asvlasov systemd[1]: Started Fingerprint Authentication Daemon.
Oct 18 19:56:11 asvlasov su[4231]: FAILED SU (to root) asvlasov on pts/1
Oct 18 19:56:38 asvlasov systemd[1]: fprintd.service: Deactivated successfully.
Oct 18 19:56:39 asvlasov asvlasov[4246]: hello
```

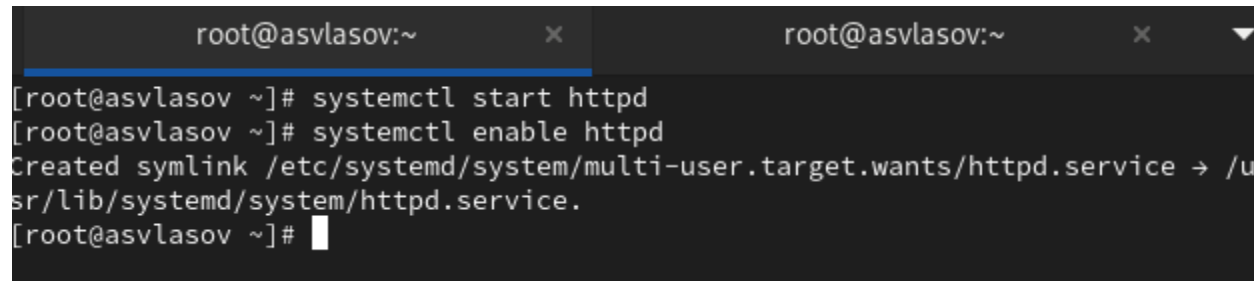
Рис. 2: Сообщение

## Открываем 20 последних строчек журнала.

```
[root@asvlasov ~]# tail -n 20 /var/log/secure
Oct 18 19:18:35 asvlasov useradd[1905]: failed adding user 'vboxadd', exit code: 9
Oct 18 19:18:35 asvlasov useradd[1906]: failed adding user 'vboxadd', exit code: 9
Oct 18 19:18:44 asvlasov systemd[2459]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 18 19:18:45 asvlasov gdm-launch-environment[2454]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 18 19:18:49 asvlasov polkitd[798]: Registered Authentication Agent for unix-session:c1 (system bus name :1.25 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: unable to locate daemon control file
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: stashed password to try later in open session
Oct 18 19:19:24 asvlasov systemd[2919]: pam_unix(systemd-user:session): session opened for user asvlasov(uid=1000) by asvlasov(uid=0)
Oct 18 19:19:24 asvlasov gdm-password[2898]: pam_unix(gdm-password:session): session opened for user asvlasov(uid=1000) by asvlasov(uid=0)
Oct 18 19:19:24 asvlasov gdm-password[2898]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 18 19:19:28 asvlasov polkitd[798]: Registered Authentication Agent for unix-session:2 (system bus name :1.71 [/usr/bin/gnome-shell], object path /org/fr
```

Рис. 3: 20 строчек

## Устанавливаем и запускаем httpd.



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

Рис. 4: httpd



# Смотрим логи ошибок httpd.

```
[root@asvlasov ~]# tail -f /var/log/httpd/error_log
[Sat Oct 18 20:18:18.880510 2025] [core:notice] [pid 17160:tid 17160] SELinux
policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 20:18:18.884071 2025] [suexec:notice] [pid 17160:tid 17160] AH0123
2: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Oct 18 20:18:18.953597 2025] [lbmethod_heartbeat:notice] [pid 17160:tid 1
7160] AH02282: No slotmem from mod_heartbeat
[Sat Oct 18 20:18:18.966719 2025] [mpm_event:notice] [pid 17160:tid 17160] AH0
0489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 20:18:18.966841 2025] [core:notice] [pid 17160:tid 17160] AH00094:
Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 5: Логи ошибок

Заходим в файл конфигурации и дописываем строчку.



```
323 <IfModule mime_magic_module>
324 #
325 # The mod_mime_magic module allows the server to use various hints f
326 # contents of the file itself to determine its type. The MIMEMagicF
327 # directive tells the module where the hint definitions are located.
328 #
329 MIMEMagicFile conf/magic
330 </IfModule>
331
332 #
333 # Customizable error responses come in three flavors:
334 # 1) plain text 2) local redirects 3) external redirects
335 #
336 # Some examples:
337 #ErrorDocument 500 "The server made a boo boo."
338 #ErrorDocument 404 /missing.html
339 #ErrorDocument 404 "/cgi-bin/missing_handler.pl"
340 #ErrorDocument 482 http://www.example.com/subscription_info.html
341 #
342 #
343 #
344 # EnableMMAP and EnableSendfile: On systems that support it,
345 # memory-mapping or the sendfile syscall may be used to deliver
346 # files. This usually improves server performance, but must
347 # be turned off when serving from networked-mounted
348 # filesystems or if support for these functions is otherwise
349 # broken on your system.
350 # Defaults if commented: EnableMMAP On, EnableSendfile Off
351 #
352 #EnableMMAP off
353 #EnableSendfile on
354
355 # Supplemental configuration
356 #
357 # Load config files in the "/etc/httpd/conf.d" directory, if any.
358 IncludeOptional conf.d/*.conf
359
360 ErrorLog syslog:locali
```

Рис. 6: Изменение файла конфигурации

Создаем новый файл конфигурации и заполняем его.

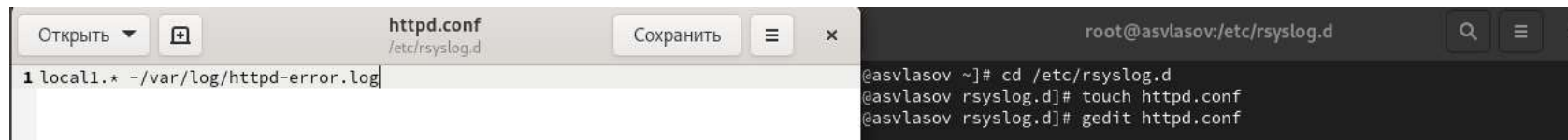
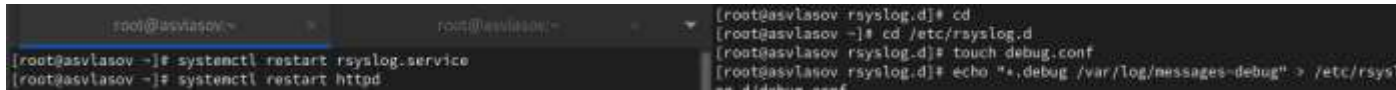


Рис. 7: Новый файл конфигурации

Перезапускаем сервисы и дописываем строчку в файл конфигурации debug.conf.

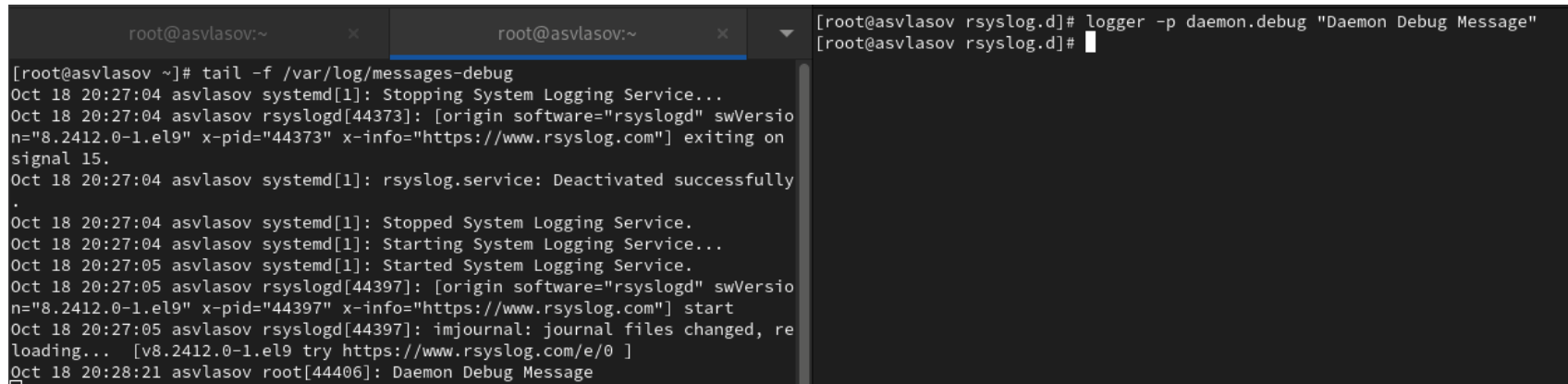


```
root@asvlasov:~# systemctl restart rsyslog.service
root@asvlasov:~# systemctl restart httpd

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

Рис. 8: debug

Затем отправляем сообщение в другой журнал мониторинга.



```
root@asvlasov:~ x root@asvlasov:~ x [root@asvlasov rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
[root@asvlasov rsyslog.d]#

[root@asvlasov ~]# tail -f /var/log/messages-debug
Oct 18 20:27:04 asvlasov systemd[1]: Stopping System Logging Service...
Oct 18 20:27:04 asvlasov rsyslogd[44373]: [origin software="rsyslogd" swVersio
n="8.2412.0-1.el9" x-pid="44373" x-info="https://www.rsyslog.com"] exiting on
signal 15.
Oct 18 20:27:04 asvlasov systemd[1]: rsyslog.service: Deactivated successfully
.
Oct 18 20:27:04 asvlasov systemd[1]: Stopped System Logging Service.
Oct 18 20:27:04 asvlasov systemd[1]: Starting System Logging Service...
Oct 18 20:27:05 asvlasov systemd[1]: Started System Logging Service.
Oct 18 20:27:05 asvlasov rsyslogd[44397]: [origin software="rsyslogd" swVersio
n="8.2412.0-1.el9" x-pid="44397" x-info="https://www.rsyslog.com"] start
Oct 18 20:27:05 asvlasov rsyslogd[44397]: imjournal: journal files changed, re
loading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 20:28:21 asvlasov root[44406]: Daemon Debug Message
```

Рис. 9: Сообщение в журнале

# Начинаем работу с journalctl. Смотрим журнал в реальном времени.

```
[root@asvlasov ~]# journalctl -f
bash: journalctl: команда не найдена...
[root@asvlasov ~]# journalctl -f
окт 18 20:27:04 asvlasov.localdomain systemd[1]: Stopped System Logging Service.
окт 18 20:27:04 asvlasov.localdomain systemd[1]: Starting System Logging Service...
окт 18 20:27:05 asvlasov.localdomain systemd[1]: Started System Logging Service.
окт 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="44397" x-info="https://www.rsyslog.com"]
start
окт 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
окт 18 20:28:21 asvlasov.localdomain root[44406]: Daemon Debug Message
окт 18 20:29:25 asvlasov.localdomain systemd[1]: Starting PackageKit Daemon...
окт 18 20:29:25 asvlasov.localdomain PackageKit[44417]: daemon start
окт 18 20:29:25 asvlasov.localdomain systemd[1]: Started PackageKit Daemon.
окт 18 20:29:26 asvlasov.localdomain PackageKit[44417]: search-file transaction /1089_eabbeccc from uid 0 finished with success after 501ms
```

Рис. 10: Журнал в реальном времени

Затем смотрим строки связанные с UID 0, последние 20 строк журнала и строки с ошибками.

```
[root@asvlasov ~]# journalctl _UID=0
OCT 18 19:17:58 asvlasov.localdomain systemd-journald[244]: Journal started
OCT 18 19:17:58 asvlasov.localdomain systemd-journald[244]: Runtime Journal (>
OCT 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'n>
OCT 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'u>
OCT 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating group 'u>
OCT 18 19:17:58 asvlasov.localdomain systemd-sysusers[246]: Creating user 'db>
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Starting Create Volatile Fil>
OCT 18 19:17:58 asvlasov.localdomain systemd-modules-load[245]: Inserted modu>
OCT 18 19:17:58 asvlasov.localdomain systemd-modules-load[245]: Module 'msr' >
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Load Kernel Modules.>
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Starting Apply Kernel Variab>
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Apply Kernel Variab>
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Create Static Devi>
OCT 18 19:17:58 asvlasov.localdomain systemd[1]: Finished Create Volatile Fil>
OCT 18 19:17:59 asvlasov.localdomain systemd[1]: Finished Setup Virtual Conso>
OCT 18 19:17:59 asvlasov.localdomain systemd[1]: dracut ask for additional cm>
OCT 18 19:17:59 asvlasov.localdomain systemd[1]: Starting dracut cmdline hook>
OCT 18 19:17:59 asvlasov.localdomain dracut-cmdline[262]: dracut-9.6 (Blue On>
```

Рис. 11: Журнал

```
[root@asvlasov ~]# journalctl -n 20
OCT 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Consumed 2.9s
OCT 18 20:23:55 asvlasov.localdomain systemd[1]: Starting The Apache HTTP Serv
OCT 18 20:23:55 asvlasov.localdomain httpd[44382]: Syntax error on line 1 of
OCT 18 20:23:55 asvlasov.localdomain httpd[44382]: Invalid command 'Errorlog'.
OCT 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Main process
OCT 18 20:23:55 asvlasov.localdomain systemd[1]: httpd.service: Failed with r
OCT 18 20:23:55 asvlasov.localdomain systemd[1]: Failed to start the Apache S
OCT 18 20:27:04 asvlasov.localdomain systemd[1]: Stopping System Logging Serv
OCT 18 20:27:04 asvlasov.localdomain rsyslogd[44373]: [origin software="rsysla
OCT 18 20:27:04 asvlasov.localdomain systemd[1]: rsyslog.service: Deactivat
OCT 18 20:27:04 asvlasov.localdomain systemd[1]: Stopped System Logging Servi
OCT 18 20:27:04 asvlasov.localdomain systemd[1]: Starting System Logging Serv
OCT 18 20:27:05 asvlasov.localdomain systemd[1]: Started System Logging Servi
OCT 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: [origin software="rsysl
OCT 18 20:27:05 asvlasov.localdomain rsyslogd[44397]: !journal: journal file
OCT 18 20:28:21 asvlasov.localdomain root[44406]: Daemon Output Message
OCT 18 20:29:25 asvlasov.localdomain systemd[1]: Starting PackageKit Daemon...
OCT 18 20:29:25 asvlasov.localdomain PackageKit[44417]: Daemon Start
OCT 18 20:29:25 asvlasov.localdomain systemd[1]: Started PackageKit Daemon.
OCT 18 20:29:36 asvlasov.localdomain PackageKit[44417]: search-file transacti

[root@asvlasov ~]# journalctl -p err
OCT 18 20:17:56 asvlasov.localdomain kernel: WARNING: Repetated hardware is
OCT 18 20:17:58 asvlasov.localdomain systemd[1]: Invalid SMD file header:
OCT 18 20:17:59 asvlasov.localdomain kernel: WARNING: Uninitialized device io
OCT 18 20:18:00 asvlasov.localdomain kernel: ceph: 0000-0000-0000-0000-0000-0000-0000-0000
```

# Смотрим все ошибки со вчерашнего дня. Просмотр детальной информации

```
[root@asvlasov ~]# journalctl --since yesterday -p err
окт 18 19:17:58 asvlasov.localdomain kernel: Warning: Deprecated Hardware is >
окт 18 19:17:58 asvlasov.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:17:59 asvlasov.localdomain kernel: Warning: Unmaintained driver is >
окт 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERR0>
окт 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERR0>
окт 18 19:18:00 asvlasov.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERR0>
окт 18 19:18:06 asvlasov.localdomain systemd[1]: Invalid DMI field header.
окт 18 19:18:09 asvlasov.localdomain alsactl[828]: alsa-lib main.c:1554:(snd_>
окт 18 19:18:11 asvlasov.localdomain kernel: Warning: Unmaintained driver is >
окт 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd.serv>
окт 18 19:18:44 asvlasov.localdomain systemd[1]: Failed to start vboxadd-serv>
окт 18 19:19:24 asvlasov.localdomain gdm-password[2898]: gkr-pam: unable to >
окт 18 19:19:26 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
окт 18 19:19:29 asvlasov.localdomain systemd[2919]: Failed to start Applicati>
окт 18 19:19:32 asvlasov.localdomain gdm-wayland-session[2476]: GLib: Source >
окт 18 19:19:32 asvlasov.localdomain gdm-launch-environment[2454]: GLib-GObj>
окт 18 20:23:55 asvlasov.localdomain systemd[1]: Failed to start The Apache H>
```

Рис. 13: Ошибки с определенной даты

```
[root@asvlasov ~]# journalctl -o verbose
Sat 2025-10-18 19:17:58.677082 MSK [s=8cb80feba247454eb5b61aff96174f65;i=1;b=
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 5.14.0-576.37.1.el9_6.x86_64 (mockbuild@iad1-prod-b
  _BOOT_ID=63c468765c994298a15e6a96f1a71195
  _MACHINE_ID=632ddcdda5794c52ad928429cbc91d0b
  _HOSTNAME=asvlasov.localdomain
  _RUNTIME_SCOPE=initrd
Sat 2025-10-18 19:17:58.677102 MSK [s=8cb80feba247454eb5b61aff96174f65;i=2;b=
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
```

Рис. 14: Детальная информация



## Просмотр дополнительной информации о модуле sshd.

```
[root@asvlasov ~]# journalctl _SYSTEM_UNIT=sshd.service  
-- No entries --
```

Рис. 15: sshd

Создаем каталог для хранения записей журнала, задаем ему права, принимаем изменения командой. Теперь журнал постоянный.

```
[root@asvlasov ~]# mkdir -p /var/log/journal
[root@asvlasov ~]# chown root:systemd-journal /var/lo
local/ lock/ log/
[root@asvlasov ~]# chown root:systemd-journal /var/log/journal
[root@asvlasov ~]# chmod 2755 /var/log/journal
[root@asvlasov ~]# killall -USR1 systemd-journald
[root@asvlasov ~]# journalctl -b
окт 18 19:17:58 asvlasov.localdomain kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.3
окт 18 19:17:58 asvlasov.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem
окт 18 19:17:58 asvlasov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev/mapper/r1_vbox-root ro resu
окт 18 19:17:58 asvlasov.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-provided physical RAM map:
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000bfff] usable
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000bfc00-0x00000000000009ffff] reserved
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000ffff] reserved
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x000000000000100000-0x000000000000dffff] usable
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dffffffffff] ACPI data
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffc00ffff] reserved
окт 18 19:17:58 asvlasov.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011ffffffffff] usable
окт 18 19:17:58 asvlasov.localdomain kernel: NX (Execute Disable) protection: active
окт 18 19:17:58 asvlasov.localdomain kernel: APIC: Static calls initialized
окт 18 19:17:58 asvlasov.localdomain kernel: SMBIOS 2.5 present.
окт 18 19:17:58 asvlasov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
окт 18 19:17:58 asvlasov.localdomain kernel: Hypervisor detected: KVM
окт 18 19:17:58 asvlasov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
окт 18 19:17:58 asvlasov.localdomain kernel: kvm-clock: using sched offset of 8190943666 cycles
окт 18 19:17:58 asvlasov.localdomain kernel: clocksource: kvm-clock: mask 0xffffffffffffffff max_cycles=1000000000000000.000000 max_delta_ns=1000000000000000.000000
```

Рис. 16: Создание постоянного журнала

Мы научились работать с журналами мониторинга событий в системе.