

# Лабораторная работа №7

Презентация

---

Устинова В. В.

18 октября 2025

Российский университет дружбы народов, Москва, Россия

## Информация

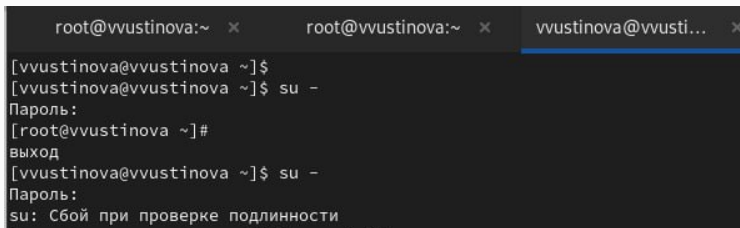
---

- Устинова Виктория Вадимовна
- студент НПИбд-01-24
- Российский университет дружбы народов

Получить навыки работы с журналами мониторинга различных событий в системе.

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 `journald` (см. раздел 7.4.4).

Запустите три вкладки терминала и в каждом из них получите полномочия администратора. В третьей вкладке терминала вернитесь к учётной записи своего пользователя и попробуйте получить полномочия администратора, но введите неправильный пароль

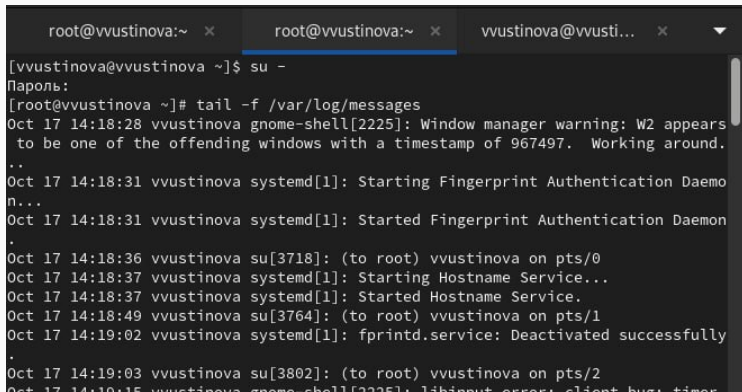


```
root@vvustinova:~ x root@vvustinova:~ x vvustinova@vvusti... x
[vvustinova@vvustinova ~]$
[vvustinova@vvustinova ~]$ su -
Пароль:
[root@vvustinova ~]#
выход
[vvustinova@vvustinova ~]$ su -
Пароль:
su: Сбой при проверке подлинности
```

Рис. 1: Запускаем три терминала и вводим неверный пароль

## Мониторинг журнала системных событий в реальном времени

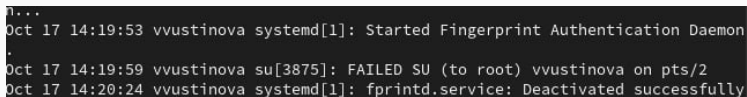
На второй вкладке терминала запустите мониторинг системных событий в реальном времени

A screenshot of a terminal window with three tabs. The active tab is titled 'root@vvustinova:~'. The terminal shows a user switching to root with 'su -', then running 'tail -f /var/log/messages'. The output displays various system messages, including a window manager warning, the start of the fingerprint authentication daemon, and the start of the hostname service. The terminal text is as follows:

```
root@vvustinova:~ x root@vvustinova:~ x vvustinova@vvusti... x
[vvustinova@vvustinova ~]$ su -
Пароль:
[root@vvustinova ~]# tail -f /var/log/messages
Oct 17 14:18:28 vvustinova gnome-shell[2225]: Window manager warning: W2 appears
to be one of the offending windows with a timestamp of 967497. Working around.
..
Oct 17 14:18:31 vvustinova systemd[1]: Starting Fingerprint Authentication Daemo
n...
Oct 17 14:18:31 vvustinova systemd[1]: Started Fingerprint Authentication Daemo
n.
Oct 17 14:18:36 vvustinova su[3718]: (to root) vvustinova on pts/0
Oct 17 14:18:37 vvustinova systemd[1]: Starting Hostname Service...
Oct 17 14:18:37 vvustinova systemd[1]: Started Hostname Service.
Oct 17 14:18:49 vvustinova su[3764]: (to root) vvustinova on pts/1
Oct 17 14:19:02 vvustinova systemd[1]: fprintd.service: Deactivated successfully
.
Oct 17 14:19:03 vvustinova su[3802]: (to root) vvustinova on pts/2
Oct 17 14:19:15 vvustinova gnome-shell[2225]: libinput error: client bug: timer
```

Рис. 2: Запускаем мониторинг

Обратите внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username».

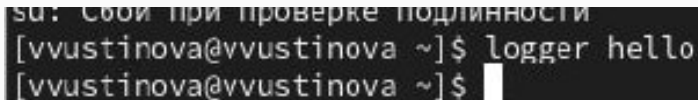
A terminal window with a black background and white text. The text shows system logs for the user 'vvustinova'. The first line is partially cut off. The second line shows 'systemd[1]: Started Fingerprint Authentication Daemon'. The third line shows 'su[3875]: FAILED SU (to root) vvustinova on pts/2'. The fourth line shows 'systemd[1]: fprintd.service: Deactivated successfully'.

```
n...  
Oct 17 14:19:53 vvustinova systemd[1]: Started Fingerprint Authentication Daemon  
.  
Oct 17 14:19:59 vvustinova su[3875]: FAILED SU (to root) vvustinova on pts/2  
Oct 17 14:20:24 vvustinova systemd[1]: fprintd.service: Deactivated successfully
```

**Рис. 3:** Сообщение выведено снизу, из-за того, что пытались ввести пароль неверный



В третьей вкладке терминала из оболочки пользователя введите `logger hello`



```
su: Сбой при проверке подлинности  
[vvustinova@vvustinova ~]$ logger hello  
[vvustinova@vvustinova ~]$
```

Рис. 4: Вводим `logger hello`

## Мониторинг журнала системных событий в реальном времени

Во второй вкладке терминала с мониторингом событий вы увидите сообщение, которое также будет зафиксировано в файле `/var/log/messages`. Запустите мониторинг сообщений безопасности (последние 20 строк)

```
.
Oct 17 14:20:47 vvustinova vvustinova[3900]: hello
^C
[root@vvustinova ~]# tail -n 20 /var/log/secure
Oct 17 14:03:16 vvustinova useradd[907]: failed adding user 'vboxadd', exit code
: 9
Oct 17 14:03:25 vvustinova sshd[1029]: Server listening on 0.0.0.0 port 22.
Oct 17 14:03:25 vvustinova sshd[1029]: Server listening on :: port 22.
Oct 17 14:03:44 vvustinova systemd[1660]: pam_unix(systemd-user:session): sessio
n opened for user gdm(uid=42) by gdm(uid=0)
Oct 17 14:03:45 vvustinova gdm-launch-environment[1655]: pam_unix(gdm-launch-en
vironment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 17 14:03:52 vvustinova polkitd[810]: Registered Authentication Agent for uni
x-session:cl (system bus name :1.29 [/usr/bin/gnome-shell], object path /org/fre
edesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
```

Рис. 5: Отображается hello и выводим 20 строк

В первой вкладке терминала установите Apache. После окончания процесса установки запустите веб-службу

A terminal window with a dark background. The prompt is [root@vvustinova ~]#. The command entered is systemctl enable httpd. The output is Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.

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

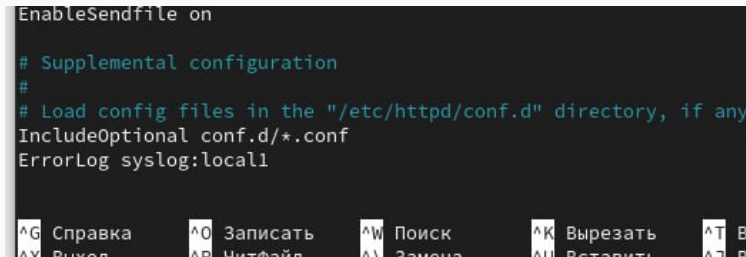
Рис. 6: Устанавливаем и запускаем, все получилось

Во второй вкладке терминала посмотрите журнал сообщений об ошибках веб-службы

```
[root@vvustinova ~]# tail -f /var/log/httpd/error_log
[Fri Oct 17 14:32:17.915820 2025] [core:notice] [pid 35683:tid 35683] SELinux p
olicy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 17 14:32:17.918140 2025] [suexec:notice] [pid 35683:tid 35683] AH01232
: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 17 14:32:18.192492 2025] [lbmethod_heartbeat:notice] [pid 35683:tid 35
683] AH02282: No slotmem from mod_heartbeat
[Fri Oct 17 14:32:18.254280 2025] [mpm_event:notice] [pid 35683:tid 35683] AH00
489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 17 14:32:18.254350 2025] [core:notice] [pid 35683:tid 35683] AH00094:
Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
```

Рис. 7: Смотрим сообщения об ошибках

В третьей вкладке терминала получите полномочия администратора и в файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавьте следующую строку



```
EnableSendfile on

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

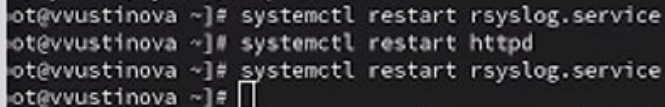
Рис. 8: Открываем файл в редакторе nano и добавляем строку

В каталоге `/etc/rsyslog.d` создайте файл мониторинга событий веб-службы. Открыв его на редактирование, пропишите в нём `local1.* -/var/log/httpd-error.log`

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

**Рис. 9:** Создаем файл и открываем также в редакторе nano и добавляем строку

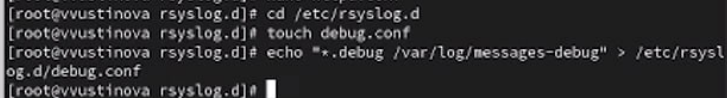
Перейдите в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу

A terminal window with a dark background and light-colored text. It shows four lines of commands entered at a prompt. The first line is 'systemctl restart rsyslog.service', the second is 'systemctl restart httpd', the third is 'systemctl restart rsyslog.service', and the fourth is an empty line with a cursor. The prompt is 'ot@vvustinova ~]#'.

```
ot@vvustinova ~]# systemctl restart rsyslog.service
ot@vvustinova ~]# systemctl restart httpd
ot@vvustinova ~]# systemctl restart rsyslog.service
ot@vvustinova ~]#
```

Рис. 10: Перезагружаем введя команды

В третьей вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации. В этом же терминале введите

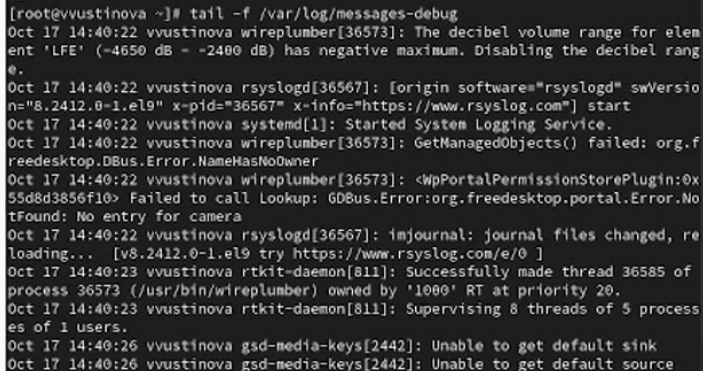
A terminal window with a dark background and light-colored text. The prompt is [root@vvustinova rsyslog.d]#. The user enters 'cd /etc/rsyslog.d', then 'touch debug.conf', then 'echo "\*.\*debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf', and finally another prompt is shown.

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

Рис. 11: Записываем строку в файл и создаем его



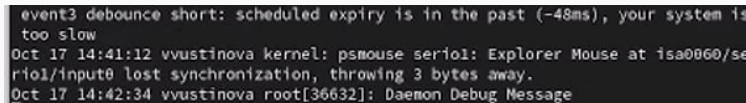
Во второй вкладке терминала запустите мониторинг отладочной информации:

A screenshot of a terminal window with a dark background and light-colored text. The terminal shows the output of the 'tail -f /var/log/messages-debug' command. The output consists of several lines of log messages, including warnings from wireplumber, startup messages from rsyslogd and systemd, error messages from freedesktop, and status messages from rtkit-daemon and gsd-media-keys.

```
[root@vvustinova ~]# tail -f /var/log/messages-debug
Oct 17 14:40:22 vvustinova wireplumber[36573]: The decibel volume range for element 'LFE' (-4650 dB - -2400 dB) has negative maximum. Disabling the decibel range.
Oct 17 14:40:22 vvustinova rsyslogd[36567]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="36567" x-info="https://www.rsyslog.com"] start
Oct 17 14:40:22 vvustinova systemd[1]: Started System Logging Service.
Oct 17 14:40:22 vvustinova wireplumber[36573]: GetManagedObjects() failed: org.freedesktop.DBus.Error.NameHasNoOwner
Oct 17 14:40:22 vvustinova wireplumber[36573]: <WpPortalPermissionStorePlugin:0x55d8d3856f10> Failed to call Lookup: GDBus.Error:org.freedesktop.portal.Error.NotFound: No entry for camera
Oct 17 14:40:22 vvustinova rsyslogd[36567]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 17 14:40:23 vvustinova rtkit-daemon[811]: Successfully made thread 36585 of process 36573 (/usr/bin/wireplumber) owned by '1000' RT at priority 20.
Oct 17 14:40:23 vvustinova rtkit-daemon[811]: Supervising 8 threads of 5 processes of 1 users.
Oct 17 14:40:26 vvustinova gsd-media-keys[2442]: Unable to get default sink
Oct 17 14:40:26 vvustinova gsd-media-keys[2442]: Unable to get default source
```

Рис. 12: Снова запускаем мониторинг

В третьей вкладке терминала введите: `logger -p daemon.debug "Daemon Debug Message"`

A screenshot of a terminal window with a dark background and white text. The text shows three lines of log output. The first line is a kernel message about a debounce short. The second line is a kernel message about a mouse losing synchronization. The third line is a user-level message from the daemon.debug facility.

```
event3 debounce short: scheduled expiry is in the past (-48ms), your system is  
too slow  
Oct 17 14:41:12 vvustinova kernel: psmouse serio1: Explorer Mouse at isa0060/ser  
rio1/input0 lost synchronization, throwing 3 bytes away.  
Oct 17 14:42:34 vvustinova root[36632]: Daemon Debug Message
```

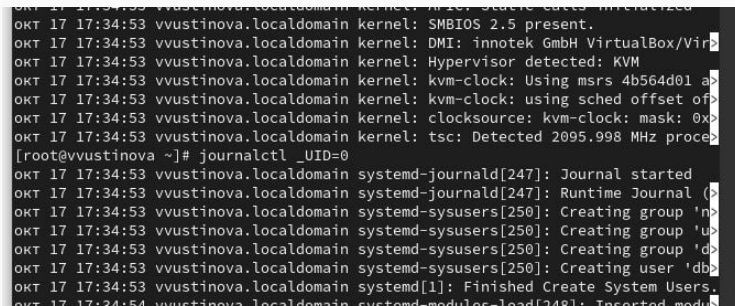
Рис. 13: Переходя на вторую вкладку терминала отображается сразу сообщение

Просмотр содержимого журнала без использования пейджера:

```
окт 17 17:34:53 vvustinova.localdomain kernel: Hypervisor detected: KVM
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: Using msrs 4b564d01 a>
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: using sched offset of>
окт 17 17:34:53 vvustinova.localdomain kernel: clocksource: kvm-clock: mask: 0x>
окт 17 17:34:53 vvustinova.localdomain kernel: tsc: Detected 2095.998 MHz proce>
[root@vvustinova ~]# journalctl --no-pager
окт 17 17:34:53 vvustinova.localdomain kernel: Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-5), GNU ld version 2.35.2-63.el9) #1 SMP PREEMPT_DYNAMIC Fri May 23 22:47:01 UTC 2025
окт 17 17:34:53 vvustinova.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
окт 17 17:34:53 vvustinova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdosl)/vmlinuz-5.14.0-570.17.1.el9_6.x86_64 root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root rd.lvm.lv=rl/swap rhgb quiet
окт 17 17:34:53 vvustinova.localdomain kernel: [Firmware Bug]: TSC doesn't count
```

Рис. 14: Команда : journalctl --no-pager

Режим просмотра журнала в реальном времени: `journalctl -f` и Просмотрите события для UID0: `journalctl _UID=0`



```
окт 17 17:34:53 vvustinova.localdomain kernel: ACPI: Static calls initialized
окт 17 17:34:53 vvustinova.localdomain kernel: SMBIOS 2.5 present.
окт 17 17:34:53 vvustinova.localdomain kernel: DMI: innotek GmbH VirtualBox/Vir
окт 17 17:34:53 vvustinova.localdomain kernel: Hypervisor detected: KVM
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: Using msrs 4b564d01 a>
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: using sched offset of>
окт 17 17:34:53 vvustinova.localdomain kernel: clocksource: kvm-clock: mask: 0x>
окт 17 17:34:53 vvustinova.localdomain kernel: tsc: Detected 2095.998 MHz proce>
[root@vvustinova ~]# journalctl _UID=0
окт 17 17:34:53 vvustinova.localdomain systemd-journald[247]: Journal started
окт 17 17:34:53 vvustinova.localdomain systemd-journald[247]: Runtime Journal (>
окт 17 17:34:53 vvustinova.localdomain systemd-sysusers[250]: Creating group 'n>
окт 17 17:34:53 vvustinova.localdomain systemd-sysusers[250]: Creating group 'u>
окт 17 17:34:53 vvustinova.localdomain systemd-sysusers[250]: Creating group 'd>
окт 17 17:34:53 vvustinova.localdomain systemd-sysusers[250]: Creating user 'db>
окт 17 17:34:53 vvustinova.localdomain systemd[1]: Finished Create System Users.
окт 17 17:34:54 vvustinova.localdomain systemd-modules-load[248]: Inserted modu>
```

Рис. 15: сверху просмотр в реальном времени снизу события UID0

# Использование journalctl

Для отображения последних 20 строк журнала введите и Для просмотра только сообщений об ошибках введите

```
приоритета, [root@vvustinova ~]# journalctl -n 20
офт 17 17:38:27 vvustinova.localdomain systemd[1]: Started Hostname Service.
зуйте      офт 17 17:38:36 vvustinova.localdomain su[3584]: (to root) vvustinova on pts/1
офт 17 17:38:36 vvustinova.localdomain su[3584]: pam_unix(su-l:session): session
дуле sshd в офт 17 17:38:44 vvustinova.localdomain su[3620]: (to root) vvustinova on pts/0
офт 17 17:38:44 vvustinova.localdomain su[3620]: pam_unix(su-l:session): session
офт 17 17:38:51 vvustinova.localdomain PackageKit[1957]: update-packages transac
офт 17 17:38:54 vvustinova.localdomain systemd[1]: fprintd.service: Deactivated
г в оператив офт 17 17:38:54 vvustinova.localdomain PackageKit[1957]: get-updates transactio
лько до перез офт 17 17:38:54 vvustinova.localdomain PackageKit[1957]: get-updates transactio
олините следую офт 17 17:38:54 vvustinova.localdomain packagekitd[1957]: Failed to get cache f
нистратора. офт 17 17:38:54 vvustinova.localdomain packagekitd[1957]: Failed to get cache f
офт 17 17:38:54 vvustinova.localdomain packagekitd[1957]: Failed to get cache f
log/journal офт 17 17:38:54 vvustinova.localdomain packagekitd[1957]: Failed to get cache f
офт 17 17:38:55 vvustinova.localdomain PackageKit[1957]: get-details transactio
ournal      офт 17 17:38:55 vvustinova.localdomain PackageKit[1957]: get-updates transactio
офт 17 17:39:14 vvustinova.localdomain systemd[1]: systemd-hostnamed.service: D
офт 17 17:41:49 vvustinova.localdomain systemd[2286]: Created Slice User Backgr
офт 17 17:41:49 vvustinova.localdomain systemd[2286]: Starting Cleanup of User's
офт 17 17:41:49 vvustinova.localdomain systemd[2286]: Finished Cleanup of User's
офт 17 17:42:21 vvustinova.localdomain gnome-shell[2382]: libinput error: clien
[root@vvustinova ~]# journalctl -p err
офт 17 17:34:53 vvustinova.localdomain kernel: Warning: Deprecated Hardware is
офт 17 17:34:53 vvustinova.localdomain systemd[1]: Invalid DMX field header.
```

Рис. 16: Смотрим последние 20 строк и сообщения об ошибках

ля просмотра всех сообщений со вчерашнего дня введите `journalctl--since yesterday`. Если вы хотите показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используйте `journalctl--since yesterday -p err`

```
окт 17 17:34:53 vvustinova.localdomain kernel: Hypervisor detected: KVM
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: Using msrs 4b564d01 a>
окт 17 17:34:53 vvustinova.localdomain kernel: kvm-clock: using sched offset of>
окт 17 17:34:53 vvustinova.localdomain kernel: clocksource: kvm-clock: mask: 0x>
окт 17 17:34:53 vvustinova.localdomain kernel: tsc: Detected 2095.998 MHz proce>
[root@vvustinova ~]# journalctl --since yesterday -p err
окт 17 17:34:53 vvustinova.localdomain kernel: Warning: Deprecated Hardware is >
окт 17 17:34:53 vvustinova.localdomain systemd[1]: Invalid DMI field header.
окт 17 17:34:57 vvustinova.localdomain kernel: Warning: Unmaintained driver is >
окт 17 17:35:01 vvustinova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
окт 17 17:35:01 vvustinova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
окт 17 17:35:01 vvustinova.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERRO>
окт 17 17:35:11 vvustinova.localdomain systemd[1]: Invalid DMI field header.
окт 17 17:35:18 vvustinova.localdomain alsactl[829]: alsa-lib main.c:1554:(snd_>
окт 17 17:35:26 vvustinova.localdomain kernel: Warning: Unmaintained driver is >
окт 17 17:35:39 vvustinova.localdomain setroubleshoot[894]: SELinux запрещает />
окт 17 17:35:47 vvustinova.localdomain systemd[1]: Failed to start vboxadd.serv>
окт 17 17:35:47 vvustinova.localdomain systemd[1]: Failed to start vboxadd-serv>
```

Рис. 17: Смотрим события прошлого дня

## Использование journalctl

Если вам нужна детальная информация, то используйте `journalctl -o verbose` Для просмотра дополнительной информации о модуле `sshd` введите

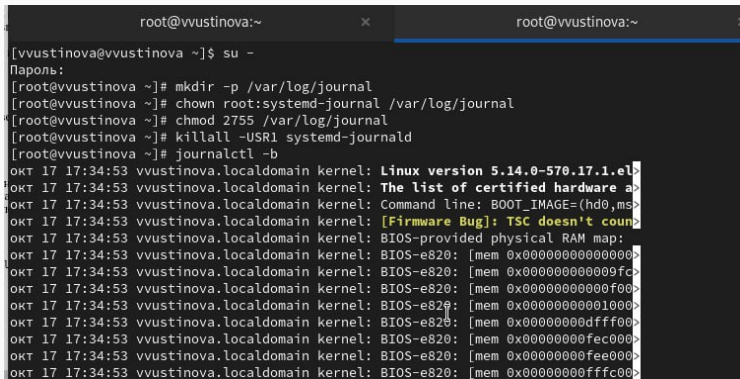
```

Fri 2025-10-17 17:34:53.666807 MSK [s=a7792966206f436882a1654d8bbf9ec8;i=2;b=f4>
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=f41a4104cc3c4bf49c04b4be3bf49d71
  _MACHINE_ID=580d4f7e5f63408eb20cbd7b314c132a
  _HOSTNAME=vvustinova.localdomain
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of certified hardware and cloud instances for Enterprise L>
Fri 2025-10-17 17:34:53.666816 MSK [s=a7792966206f436882a1654d8bbf9ec8;i=3;b=f4>
[root@vvustinova ~]# journalctl _SYSTEMD_UNIT=sshd.service
окт 17 17:35:29 vvustinova.localdomain sshd[1023]: Server listening on 0.0.0.0 >
окт 17 17:35:29 vvustinova.localdomain sshd[1023]: Server listening on :: port >
[root@vvustinova ~]#
```

Рис. 18: Выполняем команды

## Постоянный журнал journald

Создайте каталог, скорректируйте права доступа, Для принятия изменений необходимо или перезагрузить систему, чтобы видеть сообщения журнала с момента последней перезагрузки, используйте



```
root@vvustinova:~  
[vvustinova@vvustinova ~]$ su -  
Пароль:  
[root@vvustinova ~]# mkdir -p /var/log/journal  
[root@vvustinova ~]# chown root:systemd-journal /var/log/journal  
[root@vvustinova ~]# chmod 2755 /var/log/journal  
[root@vvustinova ~]# killall -USR1 systemd-journald  
[root@vvustinova ~]# journalctl -b  
окт 17 17:34:53 vvustinova.localdomain kernel: Linux version 5.14.0-570.17.1.el>  
окт 17 17:34:53 vvustinova.localdomain kernel: The list of certified hardware a>  
окт 17 17:34:53 vvustinova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,ms>  
окт 17 17:34:53 vvustinova.localdomain kernel: [Firmware Bug]: TSC doesn't coun>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-provided physical RAM map:  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x000000000000000>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000000009fc>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x000000000000f00>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000001000>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000dffff00>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000fec000>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000fee000>  
окт 17 17:34:53 vvustinova.localdomain kernel: BIOS-e820: [mem 0x00000000fffc00>
```

Рис. 19: Выполняем все перечисленные команды



Получить навыки работы с журналами мониторинга различных событий в системе.