

Управление журналами событий в системе

Часть 1

Славинский В.В.

18 октября 2025

Российский университет дружбы народов, Москва, Россия Россия

Информация

..... {.columns align=center} ::: {.column width="70%"}

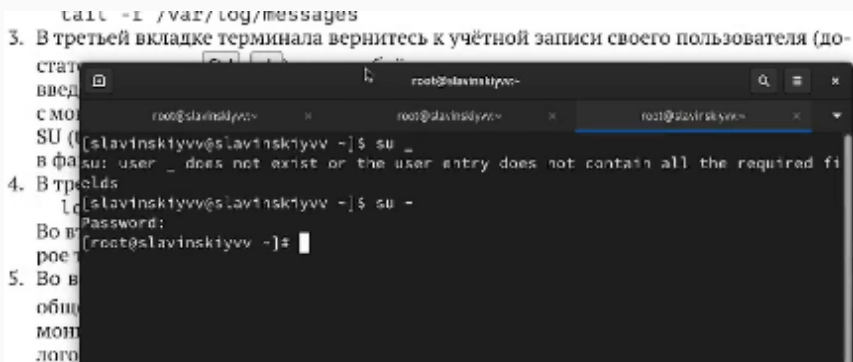
- Славинский Владислав Вадимович
- Студент
- Российский университет дружбы народов
- [1132246169@pfur.ru]

::: ::: {.column width="30%"}

Вводная часть

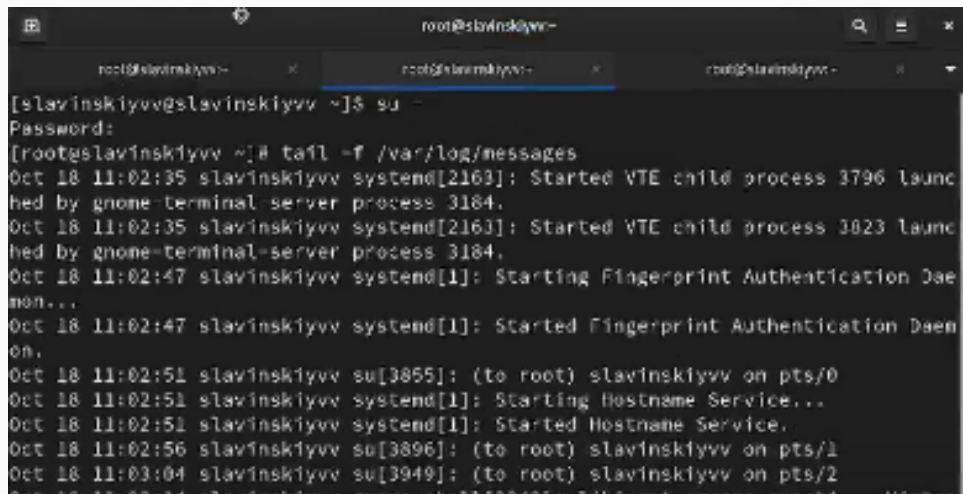
Переход в режим суперпользователя

Запустим три вкладки терминала и в каждом из них получим полномочия администратора



Запуск мониторинга системных событий в реальном времени

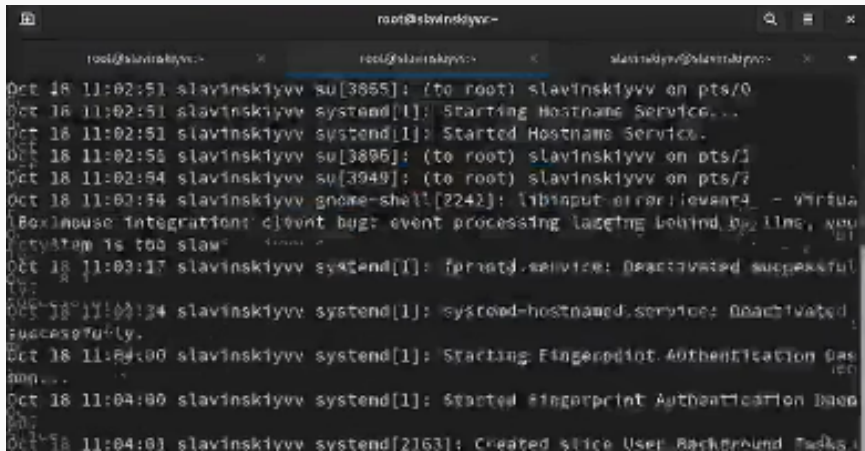
На второй вкладке терминала запустим мониторинг системных событий в реальном времени:
`tail -f /var/log/messages.`

A screenshot of a terminal window with three tabs. The active tab is titled 'root@slavinskiyvv~'. The terminal shows a user switching to root with 'su -', then running 'tail -f /var/log/messages'. The output displays various system events, including the start of VTE child processes, the Fingerprint Authentication Daemon, and Hostname Service, as well as user login attempts.

```
root@slavinskiyvv~  
[slavinskiyvv@slavinskiyvv ~]$ su -  
Password:  
[root@slavinskiyvv ~]# tail -f /var/log/messages  
Oct 18 11:02:35 slavinskiyvv systemd[2163]: Started VTE child process 3796 launched by gnome-terminal-server process 3184.  
Oct 18 11:02:35 slavinskiyvv systemd[2163]: Started VTE child process 3823 launched by gnome-terminal-server process 3184.  
Oct 18 11:02:47 slavinskiyvv systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct 18 11:02:47 slavinskiyvv systemd[1]: Started Fingerprint Authentication Daemon.  
Oct 18 11:02:51 slavinskiyvv su[3855]: (to root) slavinskiyvv on pts/0  
Oct 18 11:02:51 slavinskiyvv systemd[1]: Starting Hostname Service...  
Oct 18 11:02:51 slavinskiyvv systemd[1]: Started Hostname Service.  
Oct 18 11:02:56 slavinskiyvv su[3896]: (to root) slavinskiyvv on pts/1  
Oct 18 11:03:04 slavinskiyvv su[3949]: (to root) slavinskiyvv on pts/2  
Oct 18 11:03:14 slavinskiyvv su[3999]: (to root) slavinskiyvv on pts/3
```

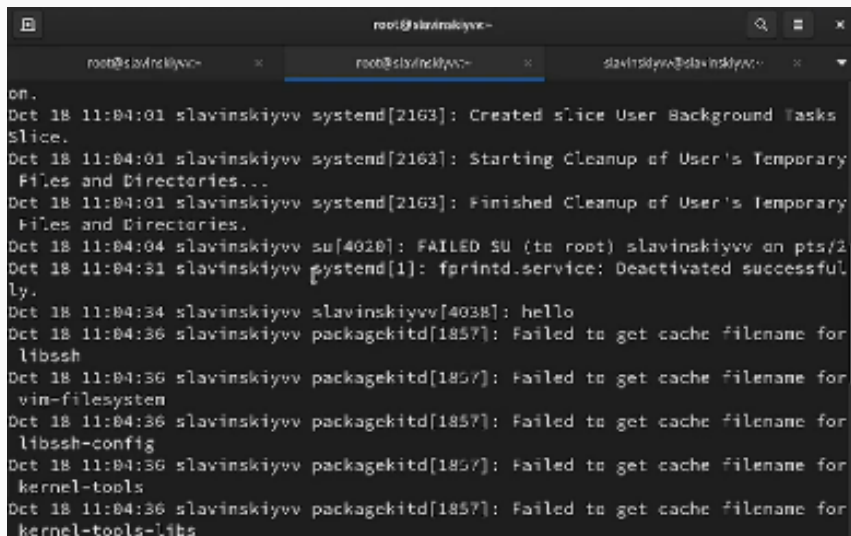
Ввод неверного пароля

В третьей вкладке терминала вернемся к учётной записи своего пользователя. Попробуем войти в режим суперпользователя, но при этом введем неправильный пароль и посмотрим вторую вкладку терминала.



```
root@slavinskiyvv:~  
root@slavinskiyvv:~  
slavinskiyvv@slavinskiyvv:~  
Oct 18 11:02:51 slavinskiyvv su[3855]: (to root) slavinskiyvv on pts/0  
Oct 18 11:02:51 slavinskiyvv systemd[1]: Starting Hostname Service...  
Oct 18 11:02:51 slavinskiyvv systemd[1]: Started Hostname Service.  
Oct 18 11:02:55 slavinskiyvv su[3895]: (to root) slavinskiyvv on pts/1  
Oct 18 11:02:54 slavinskiyvv su[3949]: (to root) slavinskiyvv on pts/2  
Oct 18 11:03:54 slavinskiyvv gnome-shell[2242]: libinput error: event4 - Virtual  
Box/ouse integration: client bug: event processing lagging behind by 2 line, you  
r system is too slow  
Oct 18 11:03:17 slavinskiyvv systemd[1]: formatd.service: Deactivated successful  
ly.  
Oct 18 11:03:34 slavinskiyvv systemd[1]: systemd-hostnamed.service: Deactivated  
successfully.  
Oct 18 11:04:00 slavinskiyvv systemd[1]: Starting Fingerprint Authentication Daemon  
...  
Oct 18 11:04:00 slavinskiyvv systemd[1]: Started Fingerprint Authentication Daemon  
...  
Oct 18 11:04:01 slavinskiyvv systemd[2163]: Created slice User Background Tasks...
```

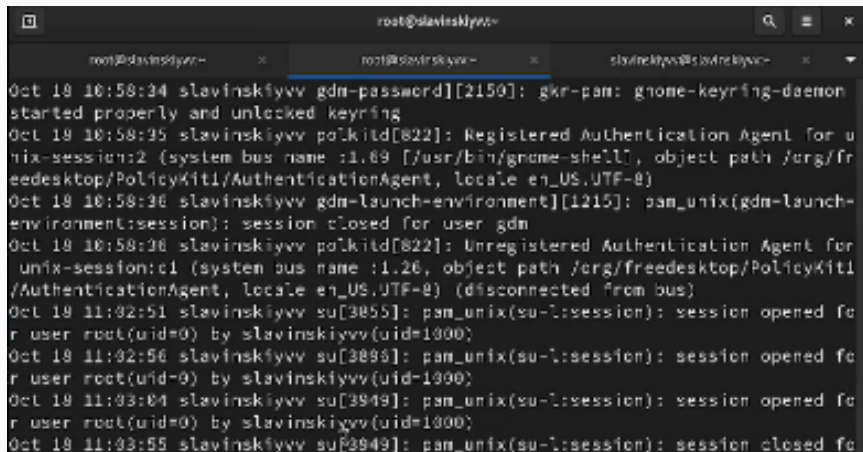
В третьей вкладке терминала из оболочки пользователя введем logger hello.



```
root@slavinskiyvv:~  
root@slavinskiyvv:~  
slavinskiyvv@slavinskiyvv:~  
on.  
Oct 18 11:04:01 slavinskiyvv systemd[2163]: Created slice User Background Tasks  
Slice.  
Oct 18 11:04:01 slavinskiyvv systemd[2163]: Starting Cleanup of User's Temporary  
Files and Directories...  
Oct 18 11:04:01 slavinskiyvv systemd[2163]: Finished Cleanup of User's Temporary  
Files and Directories.  
Oct 18 11:04:04 slavinskiyvv su[4020]: FAILED SU (to root) slavinskiyvv on pts/2  
Oct 18 11:04:31 slavinskiyvv systemd[1]: fprintd.service: Deactivated successful  
ly.  
Oct 18 11:04:34 slavinskiyvv slavinskiyvv[4038]: hello  
Oct 18 11:04:36 slavinskiyvv packagekitd[1857]: Failed to get cache filename for  
libssh  
Oct 18 11:04:36 slavinskiyvv packagekitd[1857]: Failed to get cache filename for  
vim-filesystem  
Oct 18 11:04:36 slavinskiyvv packagekitd[1857]: Failed to get cache filename for  
libssh-config  
Oct 18 11:04:36 slavinskiyvv packagekitd[1857]: Failed to get cache filename for  
kernel-tools  
Oct 18 11:04:36 slavinskiyvv packagekitd[1857]: Failed to get cache filename for  
kernel-tools-lints
```


Запуск монитора сообщений безопасности

Во второй вкладке терминала с мониторингом остановите 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`.



```
root@slavinskiyvv ~  
root@slavinskiyvv ~  
slavinskiyvv@slavinskiyvv ~  
Oct 19 10:58:34 slavinskiyvv gdm-password[2150]: gkr-pam: gnome-keyring-daemon  
started properly and unlocked keyring  
Oct 19 10:58:35 slavinskiyvv polkitd[822]: Registered Authentication Agent for u  
nix-session:2 (system bus name :1.69 [/usr/bin/gnome-shell], object path /org/fr  
eedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)  
Oct 19 10:58:36 slavinskiyvv gdm-launch-environment[1215]: pam_unix(gdm-launch-  
environment:session): session closed for user gdm  
Oct 19 10:58:36 slavinskiyvv polkitd[822]: Unregistered Authentication Agent for  
unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1  
/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)  
Oct 19 11:32:51 slavinskiyvv su[3855]: pam_unix(su-l:session): session opened fo  
r user root(uid=0) by slavinskiyvv(uid=1000)  
Oct 19 11:32:56 slavinskiyvv su[3896]: pam_unix(su-l:session): session opened fo  
r user root(uid=0) by slavinskiyvv(uid=1000)  
Oct 19 11:33:04 slavinskiyvv su[3949]: pam_unix(su-l:session): session opened fo  
r user root(uid=0) by slavinskiyvv(uid=1000)  
Oct 19 11:33:55 slavinskiyvv su[3949]: pam_unix(su-l:session): session closed fo
```

В первой вкладке терминала установим Apache: `dnf -y install httpd`.

```
[slavinskiyvv@slavinskiyvv ~]$ su -  
[root@slavinskiyvv ~]# dnf -y install httpd  
Extra Packages for Enterprise Linux 9 - x86_64 16 kB/s | 10 kB 80:00  
Extra Packages for Enterprise Linux 9 - x86_64 7.9 MB/s | 20 MB 80:02
```

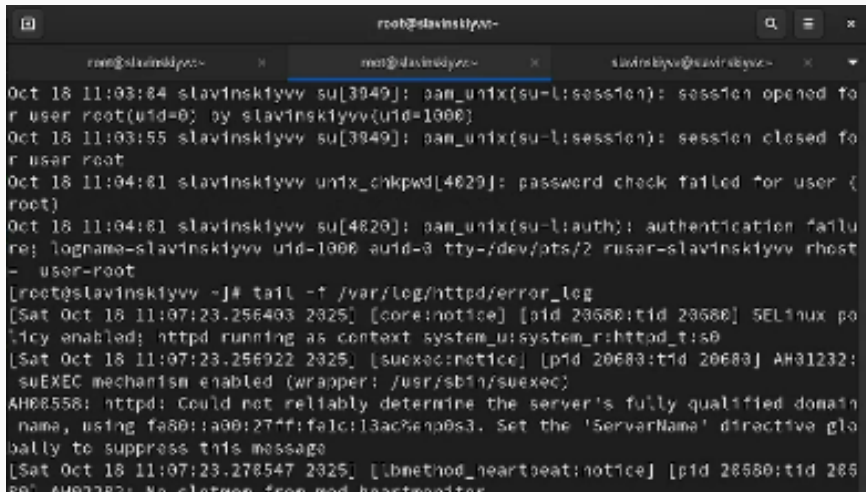
Запуск веб-службы

После окончания процесса установки запустим веб-службу: `systemctl start httpd`, `systemctl enable httpd`.

```
root@slavtrakepc:~#  
Verifying : httpd-2.4.62-4.el9_6.4.x86_64 3/11  
Verifying : apr-util-1.6.1-23.el9.x86_64 4/11  
Verifying : rocky-logos-httpd-98.16-1.el9.noarch 5/11  
Verifying : httpd-core-2.4.62-4.el9_6.4.x86_64 6/11  
Verifying : httpd-filesystem-2.4.62-4.el9_6.4.noarch 7/11  
Verifying : mod_lua-2.4.62-4.el9_6.4.x86_64 8/11  
Verifying : mod_http2-2.0.26-4.el9_6.1.x86_64 9/11  
Verifying : apr-util-openssl-1.6.1-23.el9.x86_64 10/11  
Verifying : apr-1.7.0-12.el9_3.x86_64 11/11  
Installed:  
  apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64  
  apr-util-bdb-1.6.1-23.el9.x86_64  apr-util-openssl-1.6.1-23.el9.x86_64  
  httpd-2.4.62-4.el9_6.4.x86_64  httpd-core-2.4.62-4.el9_6.4.x86_64  
  httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x86_64  
  mod_http2-2.0.26-4.el9_6.1.x86_64  mod_lua-2.4.62-4.el9_6.4.x86_64  
  rocky-logos-httpd-98.16-1.el9.noarch  
Complete!
```

Просмотр журнала с сообщениями об ошибках веб службы

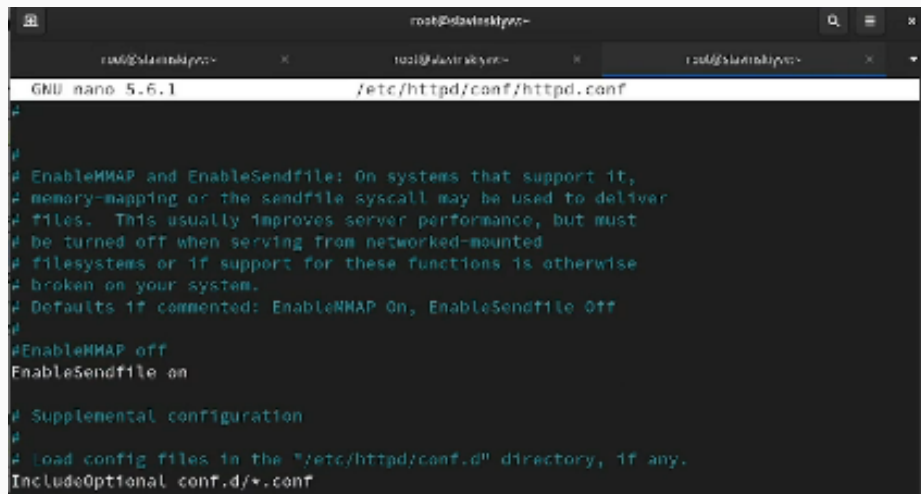
Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: `tail -f /var/log/httpd/error_log`.



```
root@slavinskiyvv:~  
root@slavinskiyvv:~  
root@slavinskiyvv:~  
Oct 18 11:03:54 slavinskiyvv su[3949]: pam_unix(su-l:session): session opened for  
r user root(uid=0) by slavinskiyvv(uid=1000)  
Oct 18 11:03:55 slavinskiyvv su[3949]: pam_unix(su-l:session): session closed fo  
r user root  
Oct 18 11:04:51 slavinskiyvv unix_chkpwd[4629]: password check failed for user (  
root)  
Oct 18 11:04:51 slavinskiyvv su[4629]: pam_unix(su-l:auth): authentication failu  
re; logname=slavinskiyvv uid=1000 auid=0 tty=/dev/pts/2 ruser=slavinskiyvv rhost  
= user=root  
[root@slavinskiyvv ~]# tail -f /var/log/httpd/error_log  
[Sat Oct 18 11:07:23.256403 2025] [core:notice] [pid 28680:tid 28680] 5ELinux po  
licy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Sat Oct 18 11:07:23.256922 2025] [suexec:notice] [pid 20680:tid 20680] AH01232:  
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
AH00558: httpd: Could not reliably determine the server's fully qualified domain  
name, using f80::a00:27ff:fc1c:13ac8eap0s3. Set the 'ServerName' directive glo  
bally to suppress this message  
[Sat Oct 18 11:07:23.278547 2025] [lbmethod:heartbeat:notice] [pid 28680:tid 286  
80] AH02282: No cluster from mod_heartbeat
```

Добавление строки в файле конфигурации

В третьей вкладке терминала получим полномочия администратора и в файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавим следующую строку: `ErrorLog syslog:local1`.

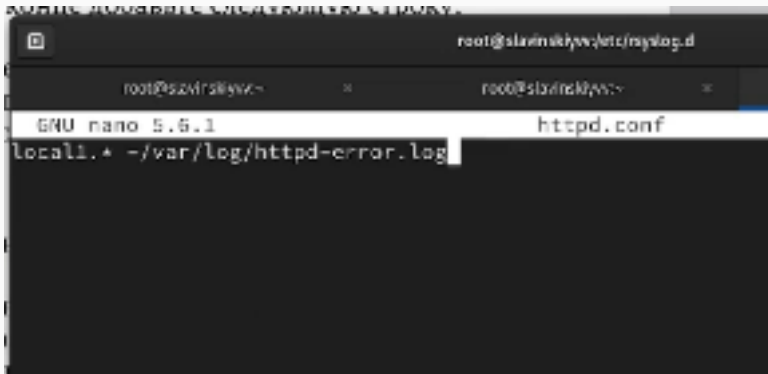


```
root@slave1sklyov-
root@slave1sklyov-
root@slave1sklyov-
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files.  This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

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

Создание файла монитора событий веб-службы

В каталоге `/etc/rsyslog.d` создадим файл мониторинга событий веб-службы: `cd /etc/rsyslog.d`, `touch httpd.conf`. Потом пропишем в нем `local1.* -/var/log/httpd-error.log`. Эта строка позволит отправлять все сообщения, получаемые для объекта `local1` в файл `/var/log/httpd-error.log`.



Перезагрузка конфигурации rsyslogd и веб-службы

Перейдем в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу: `systemctl restart rsyslog.service`, `systemctl restart httpd`.

```
Installed:
  apr-1.7.8-12.el9_3.x86_64          apr-util-1.6.1-23.el9.x86_64
  apr-util-bdb-1.6.1-23.el9.x86_64  apr-util-openssl-1.6.1-23.el9.
  httpd-2.4.62-4.el9_6.4.x86_64     httpd-core-2.4.62-4.el9_6.4.x8
  httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x
  mod_http2-2.8.26-4.el9_6.1.x86_64  mod_lua-2.4.62-4.el9_6.4.x86_6
  rocky-logos-httpd-90.16-1.el9.noarch

Complete!
[root@slavinskiyvv ~]# systemctl start httpd
[root@slavinskiyvv ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service
to /usr/lib/systemd/system/httpd.service.
[root@slavinskiyvv ~]# systemctl restart rsyslog.service
[root@slavinskiyvv ~]# systemctl restart httpd
```

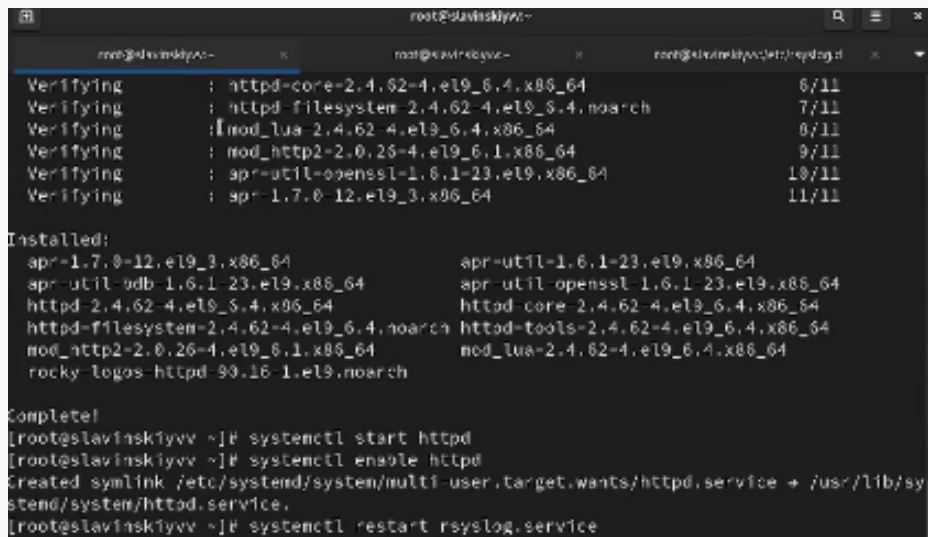
Создание отдельного файла конфигурации для мониторинга отладочной информации

В третьей вкладке терминала создадим отдельный файл конфигурации для мониторинга отладочной информации: `cd /etc/rsyslog.d, touch debug.conf`. И в этом же терминале введем `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf`.

```
[slavinskiyvv@slavinskiyvv ~]$ logger hello
[slavinskiyvv@slavinskiyvv ~]$ su -
Password:
[root@slavinskiyvv ~]# nano /etc/httpd/conf/httpd.conf
[root@slavinskiyvv ~]# cd /etc/rsyslog.d
[root@slavinskiyvv rsyslog.d]# touch httpd.conf
[root@slavinskiyvv rsyslog.d]# nano httpd.conf
[root@slavinskiyvv rsyslog.d]# nano httpd.conf
[root@slavinskiyvv rsyslog.d]# cd /etc/rsyslog.d
[root@slavinskiyvv rsyslog.d]# touch debug.conf
[root@slavinskiyvv rsyslog.d]# echo "*.debug /var/log/messages-debug"
*.debug /var/log/messages-debug
[root@slavinskiyvv rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/
debug.conf
[root@slavinskiyvv rsyslog.d]#
```


Перезапуск rsyslog

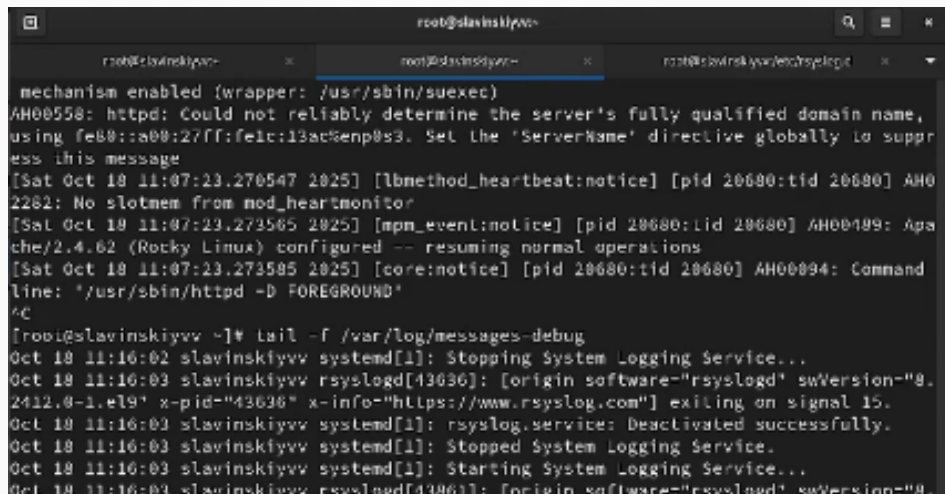
В первой вкладке терминала снова перезапустим rsyslogd: `systemctl restart rsyslog.service`.



```
root@slavinskiyvv:~  
Verifying      : httpd-core-2.4.62-4.el9_6.4.x86_64          6/11  
Verifying      : httpd-filesystem-2.4.62-4.el9_6.4.noarch    7/11  
Verifying      : httpd-mod_lua-2.4.62-4.el9_6.4.x86_64      8/11  
Verifying      : httpd-mod_http2-2.0.26-4.el9_6.1.x86_64    9/11  
Verifying      : apr-util-openssl-1.6.1-23.el9.x86_64       10/11  
Verifying      : apr-1.7.0-12.el9_3.x86_64                  11/11  
  
Installed:  
apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64  
apr-util-openssl-1.6.1-23.el9.x86_64  
httpd-2.4.62-4.el9_6.4.x86_64  httpd-core-2.4.62-4.el9_6.4.x86_64  
httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x86_64  
mod_http2-2.0.26-4.el9_6.1.x86_64  mod_lua-2.4.62-4.el9_6.4.x86_64  
rocky-logos-httpd-90.16-1.el9.noarch  
  
Complete!  
[root@slavinskiyvv ~]# systemctl start httpd  
[root@slavinskiyvv ~]# systemctl enable httpd  
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.  
[root@slavinskiyvv ~]# systemctl restart rsyslog.service
```

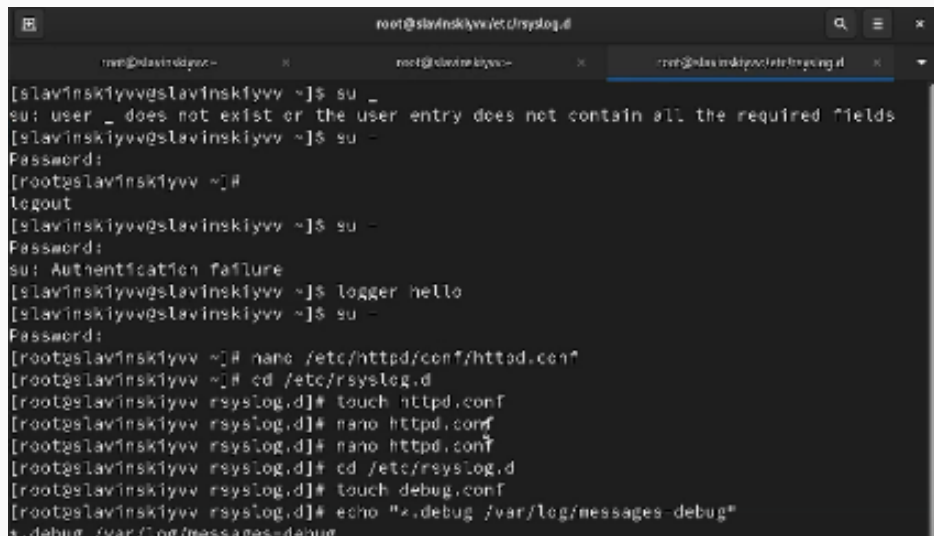
Запуск мониторинга отладочной информации

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



```
root@slavinskiyvv ~  
mechanism enabled (wrapper: /usr/sbin/suexec)  
AH00558: httpd: Could not reliably determine the server's fully qualified domain name,  
using fe80::a00:27ff:fe1c:13ac:enp0s3. Set the 'ServerName' directive globally to suppress this message  
[Sat Oct 18 11:07:23.270547 2025] [lbmethod_heartbeat:notice] [pid 20680:tid 20680] AH02282: No slotmem from mod_heartbeat  
[Sat Oct 18 11:07:23.273565 2025] [mpm_event:notice] [pid 20680:tid 20680] AH00499: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations  
[Sat Oct 18 11:07:23.273595 2025] [core:notice] [pid 20680:tid 20680] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'  
^C  
[root@slavinskiyvv ~]# tail -f /var/log/messages-debug  
Oct 18 11:16:02 slavinskiyvv systemd[1]: Stopping System Logging Service...  
Oct 18 11:16:03 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="43636" x-info="https://www.rsyslog.com"] exiting on signal 15.  
Oct 18 11:16:03 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully.  
Oct 18 11:16:03 slavinskiyvv systemd[1]: Stopped System Logging Service.  
Oct 18 11:16:03 slavinskiyvv systemd[1]: Starting System Logging Service...  
Oct 18 11:16:03 slavinskiyvv rsyslogd[43961]: [origin software="rsyslogd" swVersion="8.
```

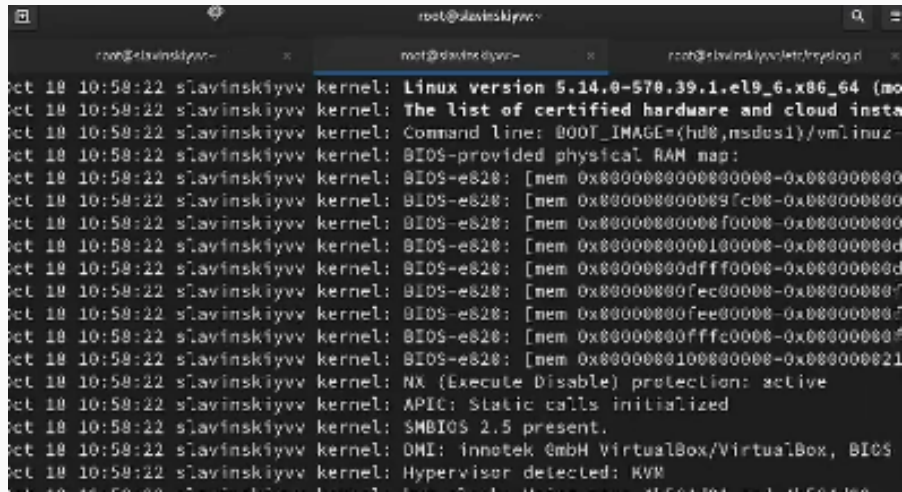
В третьей вкладке терминала введем: `logger -p daemon.debug "Daemon Debug Message"`.



```
root@slavinskiyvv:~# su _
su: user _ does not exist or the user entry does not contain all the required fields
root@slavinskiyvv:~# su -
Password:
[root@slavinskiyvv ~]#
logout
[slavinskiyvv@slavinskiyvv ~]$ su -
Password:
su: Authentication failure
[slavinskiyvv@slavinskiyvv ~]$ logger hello
[slavinskiyvv@slavinskiyvv ~]$ su -
Password:
[root@slavinskiyvv ~]# nano /etc/httpd/conf/httpd.conf
[root@slavinskiyvv ~]# cd /etc/rsyslog.d
[root@slavinskiyvv rsyslog.d]# touch httpd.conf
[root@slavinskiyvv rsyslog.d]# nano httpd.conf
[root@slavinskiyvv rsyslog.d]# nano httpd.conf
[root@slavinskiyvv rsyslog.d]# cd /etc/rsyslog.d
[root@slavinskiyvv rsyslog.d]# touch debug.conf
[root@slavinskiyvv rsyslog.d]# echo "*.debug /var/log/messages-debug"
*.debug /var/log/messages-debug
```

Содержимое журнала с событиями с момента последнего запуска системы

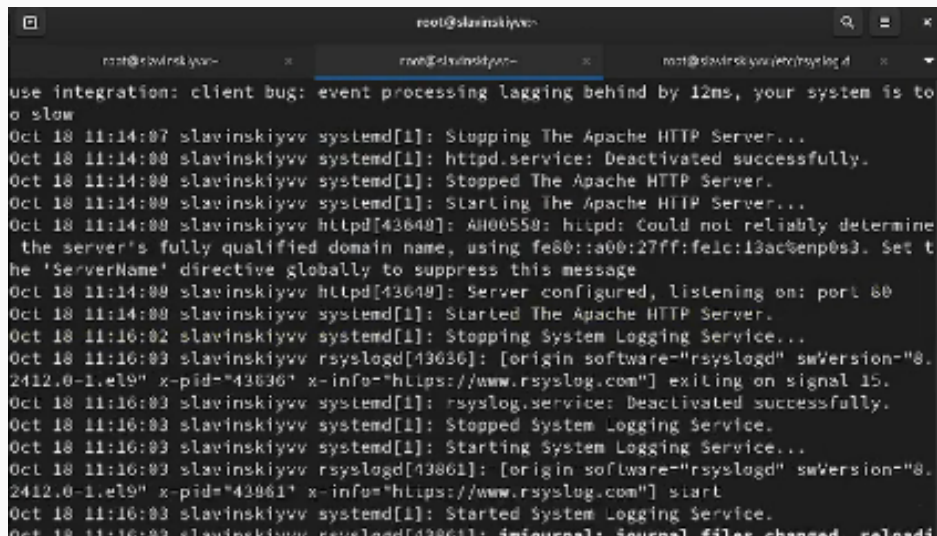
Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: `journalctl`.



```
root@slavinskiyvv:~  
root@slavinskiyvv:~  
root@slavinskiyvv:~  
oct 18 10:58:22 slavinskiyvv kernel: Linux version 5.14.0-578.39.1.el9_6.x86_64 (mo  
oct 18 10:58:22 slavinskiyvv kernel: The list of certified hardware and cloud insta  
oct 18 10:58:22 slavinskiyvv kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-provided physical RAM map:  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x00000000000089fc00-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x00000000000dfff0000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000  
oct 18 10:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000021  
oct 18 10:58:22 slavinskiyvv kernel: NX (Execute Disable) protection: active  
oct 18 10:58:22 slavinskiyvv kernel: APIC: Static calls initialized  
oct 18 10:58:22 slavinskiyvv kernel: SMBIOS 2.5 present.  
oct 18 10:58:22 slavinskiyvv kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS  
oct 18 10:58:22 slavinskiyvv kernel: Hypervisor detected: KVM  
oct 18 10:58:22 slavinskiyvv kernel: kexec-tools: Unified kernel image loaded at 0x00000000
```

Просмотр журнала без использования пейджера

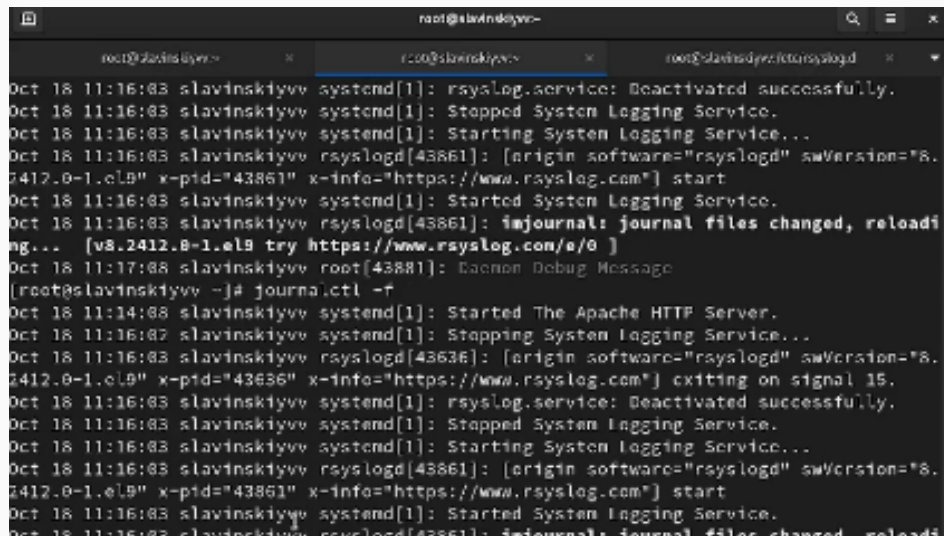
Просмотр содержимого журнала без использования пейджера: `journalctl -no-pager`.

A screenshot of a terminal window with a dark background and light-colored text. The window title is 'root@slavinskiyvv'. The terminal shows a series of system logs. The first line is a warning: 'use integration: client bug: event processing lagging behind by 12ms, your system is too slow'. Subsequent lines show the stopping and starting of the Apache HTTP Server and the System Logging Service (rsyslogd). The logs include timestamps like 'Oct 18 11:14:07' and 'Oct 18 11:16:02', along with process IDs and service names. The terminal output is as follows:

```
root@slavinskiyvv-
root@slavinskiyvv-
root@slavinskiyvv-jeh/rsyslog.d
use integration: client bug: event processing lagging behind by 12ms, your system is too slow
Oct 18 11:14:07 slavinskiyvv systemd[1]: Stopping The Apache HTTP Server...
Oct 18 11:14:08 slavinskiyvv systemd[1]: httpd.service: Deactivated successfully.
Oct 18 11:14:08 slavinskiyvv systemd[1]: Stopped The Apache HTTP Server.
Oct 18 11:14:08 slavinskiyvv systemd[1]: Starting The Apache HTTP Server...
Oct 18 11:14:08 slavinskiyvv httpd[43648]: AH00558: httpd: Could not reliably determine
the server's fully qualified domain name, using fe80::a00:27ff:fe1c:13ac%enp0s3. Set the
'ServerName' directive globally to suppress this message
Oct 18 11:14:08 slavinskiyvv httpd[43648]: Server configured, listening on: port 80
Oct 18 11:14:08 slavinskiyvv systemd[1]: Started The Apache HTTP Server.
Oct 18 11:16:02 slavinskiyvv systemd[1]: Stopping System Logging Service...
Oct 18 11:16:03 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="43636" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 11:16:03 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Stopped System Logging Service.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Starting System Logging Service...
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="43861" x-info="https://www.rsyslog.com"] start
Oct 18 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: imjournal: journal files changed, reloadi
```

Просмотр журнала в режиме реального времени

Режим просмотра журнала в реальном времени: `journalctl -f`.

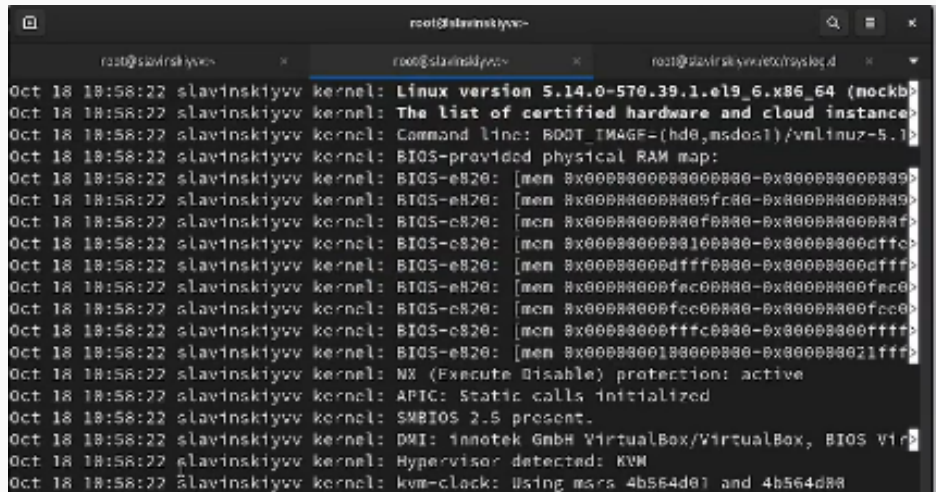


The screenshot shows a terminal window with three tabs. The active tab is titled `root@slavinskiyvv`. The terminal displays a series of system logs from `systemd` and `rsyslogd`. The logs show the process of deactivating and starting the System Logging Service, followed by the start of `rsyslogd`. A key log entry is `imjournal: journal files changed, reloading...`, which is highlighted in red in the original image. Below this, a user enters the command `journalctl -f` to follow the logs in real-time. The logs continue to show the start of the Apache HTTP Server and the stopping of the System Logging Service.

```
Oct 18 11:16:03 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Stopped System Logging Service.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Starting System Logging Service...
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="43861" x-info="https://www.rsyslog.com"] start
Oct 18 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: imjournal: journal files changed, reloadi
ng... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 11:17:08 slavinskiyvv root[43881]: Daemon Debug Message
[root@slavinskiyvv ~]# journalctl -f
Oct 18 11:14:08 slavinskiyvv systemd[1]: Started The Apache HTTP Server.
Oct 18 11:16:02 slavinskiyvv systemd[1]: Stopping System Logging Service...
Oct 18 11:16:03 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="43636" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 11:16:03 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Stopped System Logging Service.
Oct 18 11:16:03 slavinskiyvv systemd[1]: Starting System Logging Service...
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: [origin software="rsyslogd" swVersion="8.
2412.0-1.el9" x-pid="43861" x-info="https://www.rsyslog.com"] start
Oct 18 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 18 11:16:03 slavinskiyvv rsyslogd[43861]: imjournal: journal files changed, reloadi
```

Использование фильтрации просмотра конкретных параметров журнала

Для использования фильтрации просмотра конкретных параметров журнала введем `journalctl` и дважды нажмем клавишу `tab`.



```
root@slavinskiyvm:~# journalctl
Oct 18 18:58:22 slavinskiyvm kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockb>
Oct 18 18:58:22 slavinskiyvm kernel: The list of certified hardware and cloud instance>
Oct 18 18:58:22 slavinskiyvm kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.1>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-provided physical RAM map:
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Oct 18 18:58:22 slavinskiyvm kernel: NX (Execute Disable) protection: active
Oct 18 18:58:22 slavinskiyvm kernel: APIC: Static calls initialized
Oct 18 18:58:22 slavinskiyvm kernel: SMBIOS 2.5 present.
Oct 18 18:58:22 slavinskiyvm kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Virb
Oct 18 18:58:22 slavinskiyvm kernel: Hypervisor detected: KVM
Oct 18 18:58:22 slavinskiyvm kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
```

Просмотр сыбтия для uid 0

Посмотрим события для UID0: journalctl _UID=0.

```
root@slavinskiyvm:~# journalctl _UID=0
Oct 10 10:58:22 slavinskiyvm systemd-journald[264]: Journal started
Oct 10 10:58:22 slavinskiyvm systemd-journald[264]: Runtime Journal (/run/log/journal/00000000000000000000000000000000)
Oct 10 10:58:22 slavinskiyvm systemd-sysusers[267]: Creating group 'nobody' with UID 65534
Oct 10 10:58:22 slavinskiyvm systemd-sysusers[267]: Creating group 'users' with UID 1000
Oct 10 10:58:22 slavinskiyvm systemd-modules-load[265]: Inserted module 'fuse'
Oct 10 10:58:22 slavinskiyvm systemd-sysusers[267]: Creating group 'dbus' with GID 215
Oct 10 10:58:22 slavinskiyvm systemd-modules-load[265]: Module 'msr' is built in
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Load Kernel Modules.
Oct 10 10:58:22 slavinskiyvm systemd-sysusers[267]: Creating user 'dbus' (System Message Bus)
Oct 10 10:58:22 slavinskiyvm systemd[1]: Starting Apply Kernel Variables...
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Create System Users.
Oct 10 10:58:22 slavinskiyvm systemd[1]: Starting Create Static Device Nodes in /dev
Oct 10 10:58:22 slavinskiyvm systemd[1]: Starting Create Volatile Files and Directories
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Apply Kernel Variables.
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Create Static Device Nodes in /dev
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Create Volatile Files and Directories
Oct 10 10:58:22 slavinskiyvm systemd[1]: Finished Setup Virtual Console.
Oct 10 10:58:22 slavinskiyvm systemd[1]: dracut ask for additional cmdline parameters
Oct 10 10:58:22 slavinskiyvm systemd[1]: Starting dracut cmdline hook...
Oct 10 10:58:22 slavinskiyvm dracut-cmdline[205]: dracut-9.6 (Blue Onyx) dracut-cmdline
Oct 10 10:58:22 slavinskiyvm dracut-cmdline[205]: Using kernel command line parameters
```

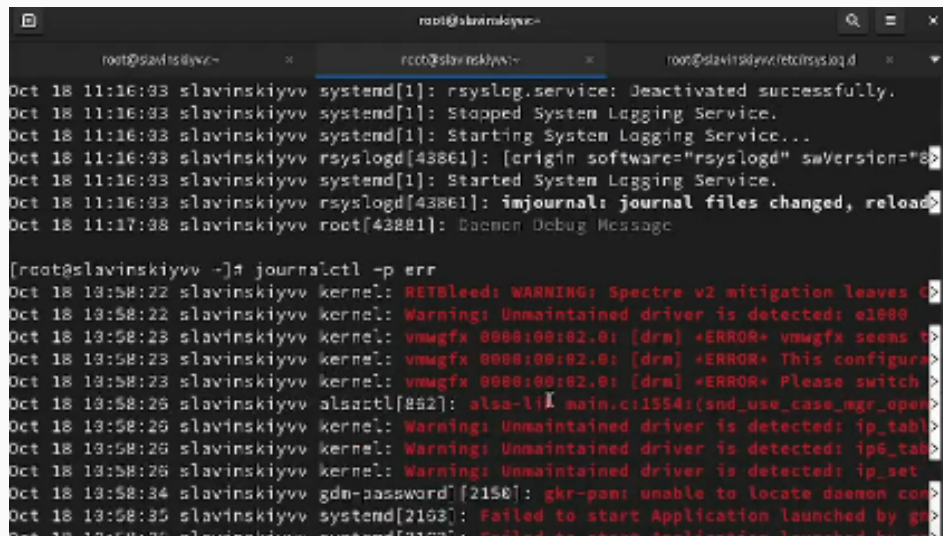

Отображение последних 20 строк журнала

Для отображения последних 20 строк журнала введем: `journalctl -n 20`.

```
[root@slavinskiyvv ~]# journalctl -n 20
Oct 10 11:14:01 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersio
Oct 10 11:14:01 slavinskiyvv rsyslogd[43636]: injournal: journal files changed, re
Oct 10 11:14:01 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 10 11:14:06 slavinskiyvv gnome-shell[2242]: libinput error: event4 - VirtualE
Oct 10 11:14:07 slavinskiyvv systemd[1]: Stopping The Apache HTTP Server...
Oct 10 11:14:08 slavinskiyvv systemd[1]: httpd.service: Deactivated successfully.
Oct 10 11:14:08 slavinskiyvv systemd[1]: Stopped The Apache HTTP Server.
Oct 10 11:14:08 slavinskiyvv systemd[1]: Starting The Apache HTTP Server...
Oct 10 11:14:08 slavinskiyvv httpd[43640]: AH00550: httpd: Could not reliably dete
Oct 10 11:14:08 slavinskiyvv httpd[43640]: Server configured, listening on: port 8
Oct 10 11:14:08 slavinskiyvv systemd[1]: Started The Apache HTTP Server.
Oct 10 11:16:02 slavinskiyvv systemd[1]: Stopping System Logging Service...
Oct 10 11:16:03 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersio
Oct 10 11:16:03 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully
Oct 10 11:16:03 slavinskiyvv systemd[1]: Stopped System Logging Service.
Oct 10 11:16:03 slavinskiyvv systemd[1]: Starting System Logging Service...
Oct 10 11:16:03 slavinskiyvv rsyslogd[43061]: [origin software="rsyslogd" swVersio
Oct 10 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 10 11:16:03 slavinskiyvv rsyslogd[43061]: injournal: journal files changed, re
```

Просмотр только сообщений об ошибках

Для просмотра только сообщений об ошибках введем: `journalctl -p err`.



```
root@slavinskiyvv:~  
root@slavinskiyvv:~  
root@slavinskiyvv:~/etc/rsyslog.d  
Oct 18 11:16:33 slavinskiyvv systemd[1]: rsyslog.service: Deactivated successfully.  
Oct 18 11:16:33 slavinskiyvv systemd[1]: Stopped System Logging Service.  
Oct 18 11:16:33 slavinskiyvv systemd[1]: Starting System Logging Service...  
Oct 18 11:16:33 slavinskiyvv rsyslogd[43861]: [origin software="rsyslogd" swVersion="8.24.0"]  
Oct 18 11:16:33 slavinskiyvv systemd[1]: Started System Logging Service.  
Oct 18 11:16:33 slavinskiyvv rsyslogd[43861]: imjournal: journal files changed, reload  
Oct 18 11:17:38 slavinskiyvv root[43881]: Daemon Debug Message  
  
[root@slavinskiyvv ~]# journalctl -p err  
Oct 18 13:58:22 slavinskiyvv kernel: RETbleed: WARNING: Spectre v2 mitigation leaves  
Oct 18 13:58:22 slavinskiyvv kernel: Warning: Unmaintained driver is detected: el1880  
Oct 18 13:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to  
Oct 18 13:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configura  
Oct 18 13:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch  
Oct 18 13:58:26 slavinskiyvv alsactl[252]: alsa-lib main.c:1554:(snd_use_case_mgr_open)  
Oct 18 13:58:26 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip_table  
Oct 18 13:58:26 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip6_tab  
Oct 18 13:58:26 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip_set  
Oct 18 13:58:34 slavinskiyvv gdm-password[2158]: gkr-pam: unable to locate daemon con  
Oct 18 13:58:35 slavinskiyvv systemd[2163]: Failed to start Application launched by g  
Oct 18 13:58:36 slavinskiyvv systemd[2163]: Failed to start Application launched by g
```


Все сообщения с ошибкой приоритета

Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то мы используем: `journalctl -since yesterday -p err`.

```
Oct 18 18:58:22 slavinskiyvv kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Virb
Oct 18 18:58:22 slavinskiyvv kernel: Hypervisor detected: KVM
Oct 18 18:58:22 slavinskiyvv kernel: kvm-clock: Using msrs 4b564d01 and 4b564d83
Oct 18 18:58:22 slavinskiyvv kernel: kvm-clock: using sched offset of 4846798051 cycles
Oct 18 18:58:22 slavinskiyvv kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff b
Oct 18 18:58:22 slavinskiyvv kernel: tsc: Detected 2984.064 MHz processor
Oct 18 18:58:22 slavinskiyvv kernel: e820: update [mem 0x88300000-0x883006fff] usable ->

[roct@slavinskiyvv ~]# journalctl --since yesterday -p err
Oct 18 18:58:22 slavinskiyvv kernel: RETbleed: WARNING: Spectre v2 mitigation leaves C
Oct 18 18:58:22 slavinskiyvv kernel: Warning: Unmaintained driver is detected: el000
Oct 18 18:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to
Oct 18 18:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configura
Oct 18 18:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch
Oct 18 18:58:25 slavinskiyvv alsactl[862]: alsa-lib main.c:1554:(snd_use_case_mgr_open)
Oct 18 18:58:25 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip_tabl
Oct 18 18:58:25 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip6_tab
Oct 18 18:58:25 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip6_tab
```

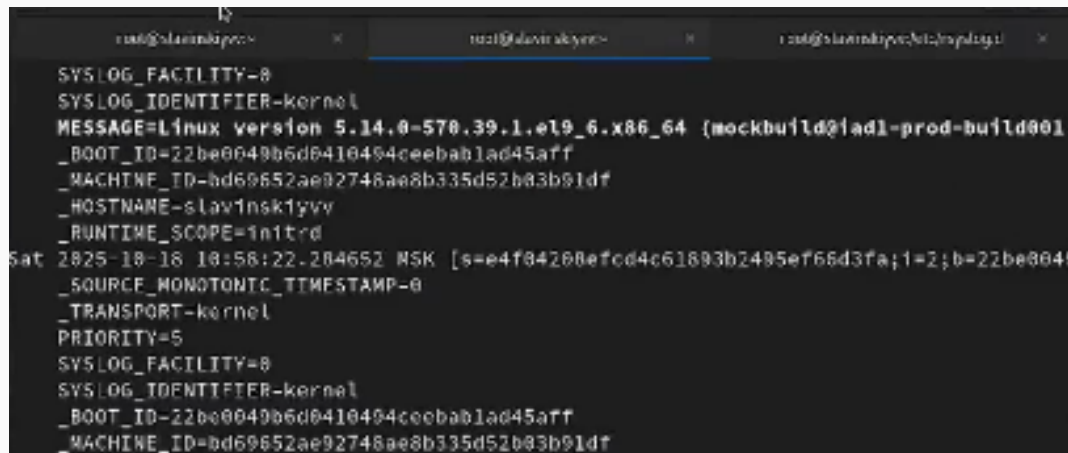
Вывод детальной информации

Если нам нужна детальная информация, то будем использовать `journalctl -o verbose`.

```
Oct 18 10:58:36 slavinskiyvv gdm-launch-environment[1215]: GLib-GObject: g_object_unref:
[root@slavinskiyvv ~]# journalctl -o verbose
Sat 2025-10-18 10:58:22.284536 M5K [s-e4f84208efcd4c51893b2405ef66d3fa;1-1;b-22be8349b2
_SOURCE_MONOTONIC_TIMESTAMP=3
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.b
_BOOT_ID=22be8049b5d0413494ceebab1ad45aff
_MACHINE_ID=bd69652ae92748ae8b335d52b83b91df
_HOSTNAME=slavinskiyvv
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 10:58:22.284552 M5K [s-e4f84208efcd4c51893b2405ef66d3fa;1-2;b-22be8349b2
_SOURCE_MONOTONIC_TIMESTAMP=3
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
_BOOT_ID=22be8049b5d0413494ceebab1ad45aff
```

Дополнительная информация о модуле sshd

Для просмотра дополнительной информации о модуле sshd введем: `journalctl _SYSTEMD_UNIT=sshd.service`.

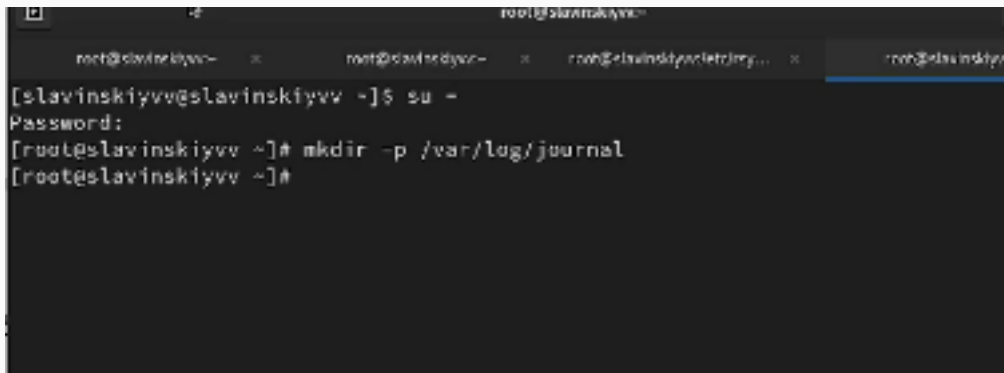
A terminal window with three tabs. The active tab shows the output of the command 'journalctl _SYSTEMD_UNIT=sshd.service'. The output displays system logs for the sshd service, including kernel messages about the Linux version (5.14.0-570.39.1.el9_6.x86_64), machine ID, hostname (slavinsk1yvv), and runtime scope (initrd). The logs are timestamped 'Sat 2025-10-18 10:58:22 -04652 MSK'.

```

SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001
_BOOT_ID=22be0040b6d0410494ceebab1ad45aff
_MACHINE_ID=bd69652ae92748ae8b335d52b03b91df
_HOSTNAME=slavinsk1yvv
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 10:58:22 -04652 MSK [s=e4f04208efcd4c61893b2495ef66d3fa;1=2;b=22be004
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=22be0040b6d0410494ceebab1ad45aff
_MACHINE_ID=bd69652ae92748ae8b335d52b03b91df
```

Создание каталога для хранения записей журнала

Запустим терминал и получим полномочия администратора. Затем создадим каталог для хранения записей журнала: `mkdir -p /var/log/journal`.

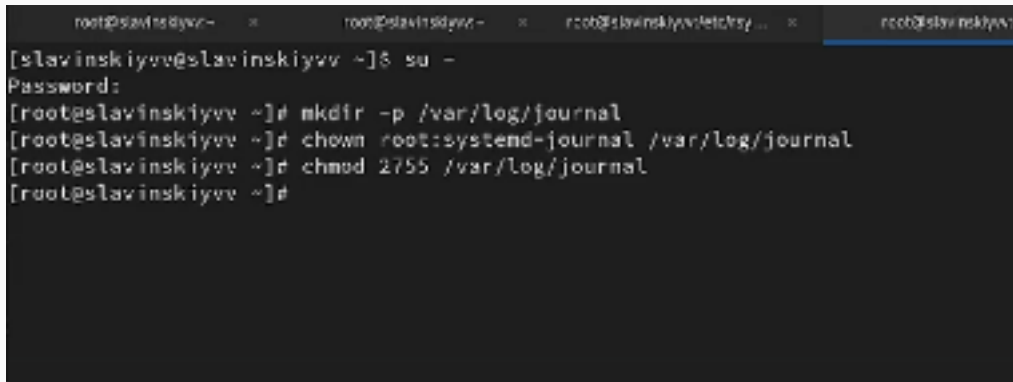


```
root@slavinskiyvv:~  
root@slavinskiyvv ~]$ su -  
Password:  
[root@slavinskiyvv ~]# mkdir -p /var/log/journal  
[root@slavinskiyvv ~]#
```

Рис. 27: sc27

Корректировка прав доступа

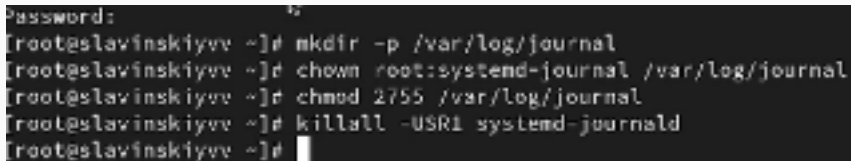
Скорректируем права доступа для каталога `/var/log/journal`, чтобы `journal` смог записывать в него информацию: `chown root: systemd-journal /var/log/journal, chmod 2755 /var/log/journal`.



```
root@slavinskiyvv ~  
[slavinskiyvv@slavinskiyvv ~]$ su -  
Password:  
[root@slavinskiyvv ~]# mkdir -p /var/log/journal  
[root@slavinskiyvv ~]# chown root:systemd-journal /var/log/journal  
[root@slavinskiyvv ~]# chmod 2755 /var/log/journal  
[root@slavinskiyvv ~]#
```

Рис. 28: sc28

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

A terminal window with a dark background and light-colored text. The prompt is [root@slavinskiyvv ~]#. The commands entered are: mkdir -p /var/log/journal, chown root:systemd-journal /var/log/journal, chmod 2755 /var/log/journal, and killall -USR1 systemd-journald. The output of the last command is a small white square.

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

Рис. 29: sc29

