

# **Лабараторная работа №7**

**Отчет**

Славинский Владислав Вадимович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>21</b>
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>22</b>

# Список иллюстраций

2.1	Переход в режим суперпользователя . . . . .	6
2.2	Запуск мониторинга системных событий в реальном времени . . .	7
2.3	Ввод неверного пароля . . . . .	7
2.4	Logger hello . . . . .	8
2.5	Запуск монитора сообщений безопасности . . . . .	8
2.6	Установка Apache . . . . .	9
2.7	Запуск веб-службы . . . . .	9
2.8	Просмотр журнала с сообщениями об ошибках веб службы . . . . .	10
2.9	Добавление строки в файле конфигурации . . . . .	10
2.10	Создание файла монитора событий веб-службы . . . . .	11
2.11	Перезагрузка конфигурации rsyslogd и веб-службы . . . . .	11
2.12	Создание отдельного файла конфигурации для мониторинга отла- дочной информации . . . . .	12
2.13	Перезапуск rsyslog . . . . .	12
2.14	Запуск мониторинга отладочной информации . . . . .	13
2.15	Ввод команды . . . . .	13
2.16	Содержимое журнала с событиями с момента последнего запуска системы . . . . .	14
2.17	Просмотр журнала без использования пейджера . . . . .	14
2.18	Просмотр журнала в режиме реального времени . . . . .	15
2.19	Использование фильтрации просмотра конкретных параметров журнала . . . . .	15
2.20	Просмотр сыбтия для uid 0 . . . . .	16
2.21	Отображение последних 20 строк журнала . . . . .	16
2.22	Просмотр только сообщений об ошибках . . . . .	17
2.23	Просмотр сообщений за определенный период времени . . . . .	17
2.24	Все сообщения с ошибкой приоритета . . . . .	18
2.25	Вывод детальной информации . . . . .	18
2.26	Дополнительная информация о модуле sshd . . . . .	19
2.27	Создание каталога для хранения записей журнала . . . . .	19
2.28	Корректировка прав доступа . . . . .	19
2.29	Принятие изменений . . . . .	20
2.30	Включение вывода сообщений после перезагрузки . . . . .	20

## **Список таблиц**

# **1 Цель работы**

Получить навыки работы с журналами мониторинга различных событий в системе.

## 2 Выполнение лабораторной работы

Запустим три вкладки терминала и в каждом из них получим полномочия администратора:. (рис. 2.1)

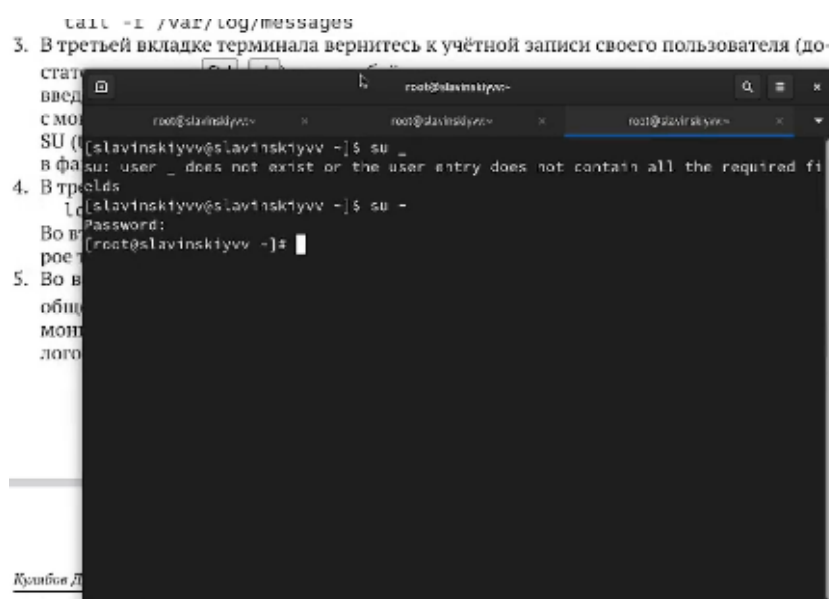
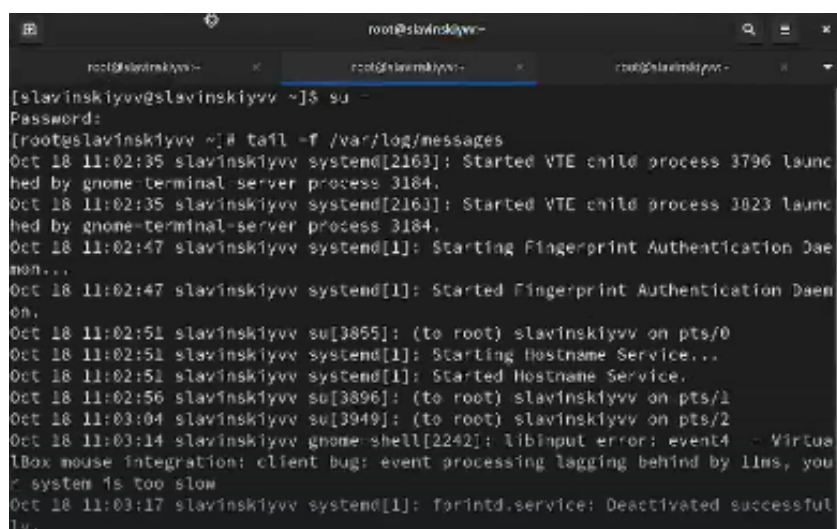


Рис. 2.1: Переход в режим суперпользователя

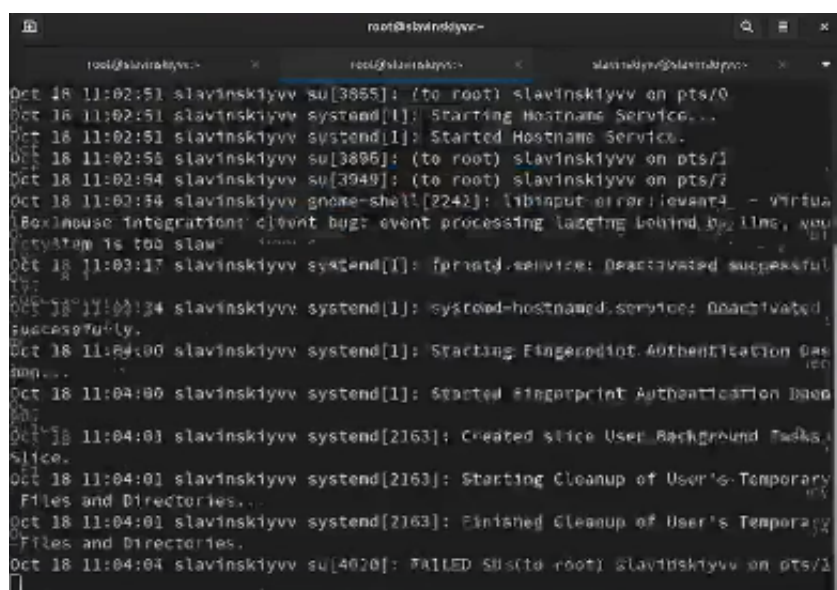
На второй вкладке терминала запустим мониторинг системных событий в реальном времени: `tail -f /var/log/messages`. (рис. 2.2)



```
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 3023 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 gnome-shell[2242]: libinput error: event4 - VirtualBox mouse integration: client bug: event processing lagging behind by 11ms, your system is too slow  
Oct 18 11:03:17 slavinskiyvv systemd[1]: forintd.service: Deactivated successfully.
```

Рис. 2.2: Запуск мониторинга системных событий в реальном времени

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. (рис. 2.3)



```
root@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 11:02:56 slavinskiyvv su[3896]: (to root) slavinskiyvv on pts/1  
Oct 18 11:02:54 slavinskiyvv su[3949]: (to root) slavinskiyvv on pts/2  
Oct 18 11:02:54 slavinskiyvv gnome-shell[2242]: libinput error: event4 - VirtualBox mouse integration: client bug: event processing lagging behind by 11ms, your system is too slow  
Oct 18 11:03:17 slavinskiyvv systemd[1]: forintd.service: Deactivated successfully.  
Oct 18 11:03:17 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 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 SSh(to root) slavinskiyvv on pts/1
```

Рис. 2.3: Ввод неверного пароля

В третьей вкладке терминала из оболочки пользователя введем `logger hello`. (рис. 2.4)

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

Рис. 2.4: Logger hello

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. (рис. 2.5)

```
Oct 18 10:58:34 slavinskiyv gdm-password[2150]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 18 10:58:35 slavinskiyv polkitd[822]: Registered Authentication Agent for unix-session:2 (system bus name :1.69 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 18 10:58:36 slavinskiyv gdm-launch-environment[1215]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 18 10:58:38 slavinskiyv polkitd[822]: Unregistered Authentication Agent for unix-session:cl (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct 18 11:02:51 slavinskiyv su[3855]: pam_unix(su-l:session): session opened for user root(uid=0) by slavinskiyv(uid=1900)
Oct 18 11:02:56 slavinskiyv su[3899]: pam_unix(su-l:session): session opened for user root(uid=0) by slavinskiyv(uid=1900)
Oct 18 11:03:04 slavinskiyv su[3949]: pam_unix(su-l:session): session opened for user root(uid=0) by slavinskiyv(uid=1900)
Oct 18 11:03:55 slavinskiyv su[3949]: pam_unix(su-l:session): session closed for user root
Oct 18 11:04:01 slavinskiyv unix_chkpwd[4029]: password check failed for user (root)
Oct 18 11:04:01 slavinskiyv su[4029]: pam_unix(su-l:auth): authentication failure; logname=slavinskiyv uid=1900 euid=0 tty=/dev/pts/2 ruser=slavinskiyv rhost= user=root
[root@slavinskiyv ~]#
```

Рис. 2.5: Запуск монитора сообщений безопасности

В первой вкладке терминала установим Apache: dnf -y install httpd (рис. 2.6)



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

Рис. 2.6: Установка Apache

После окончания процесса установки запустим веб-службу: `systemctl start httpd`, `systemctl enable httpd`. (рис. 2.7)

```
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!
[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 ~]#
```

Рис. 2.7: Запуск веб-службы

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы: `tail -f /var/log/httpd/error_log`. (рис. 2.8)

```
root@slavinskiyyv-
root@slavinskiyyv-
root@slavinskiyyv-
Oct 18 11:03:84 slavinskiyyv su[3949]: pam_unix(su-l:session): session opened for
r user root(uid=0) by slavinskiyyv(uid=1000)
Oct 18 11:03:55 slavinskiyyv su[3949]: pam_unix(su-l:session): session closed fo
r user root
Oct 18 11:04:81 slavinskiyyv unix_chkpwd[4029]: password check failed for user (
root)
Oct 18 11:04:81 slavinskiyyv su[4820]: pam_unix(su-l:auth): authentication failu
re; logname=slavinskiyyv uid=1000 auid=3 tty=/dev/pts/2 ruser=slavinskiyyv rhost
= user=root
[root@slavinskiyyv ~]# tail -f /var/log/httpd/error_log
[Sat Oct 18 11:07:23.256403 2025] [core:notice] [pid 23688:tid 23688] 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 20683:tid 20683] AH01232:
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using fa80::a90:27ff:falc:13ac6a90s3. Set the 'ServerName' directive glo
bally to suppress this message
[Sat Oct 18 11:07:23.278547 2025] [lbmethod_heartbeat:notice] [pid 28580:tid 285
80] AH02282: No slotmem from mod_heartbeat
[Sat Oct 18 11:07:23.273565 2025] [mpm_event:notice] [pid 23688:tid 23688] AH004
80: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 11:07:23.273585 2025] [core:notice] [pid 23688:tid 23688] AH00394: C
ommand line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.8: Просмотр журнала с сообщениями об ошибках веб службы

В третьей вкладке терминала получим полномочия администратора и в фай-  
ле конфигурации /etc/httpd/conf/httpd.conf в конце добавим следующую строку:  
ErrorLog syslog:local1.(рис. 2.9)

```
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

ErrorLog syslog:local1
```

Рис. 2.9: Добавление строки в файле конфигурации

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. (рис. 2.10)

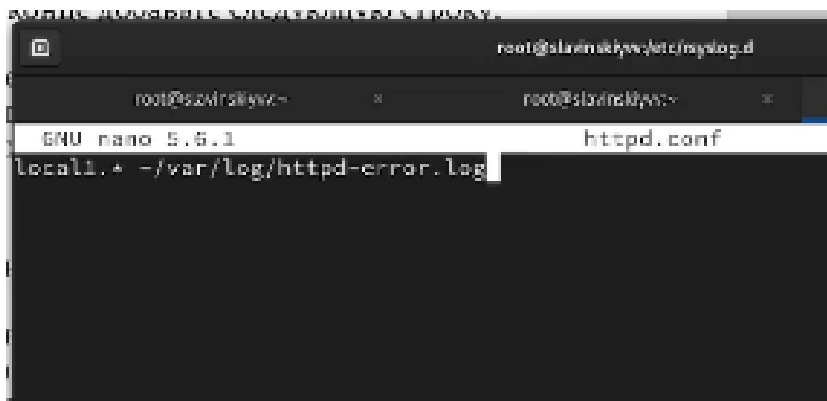


Рис. 2.10: Создание файла монитора событий веб-службы

Перейдем в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу: `systemctl restart rsyslog.service, systemctl restart httpd`. (рис. 2.11)

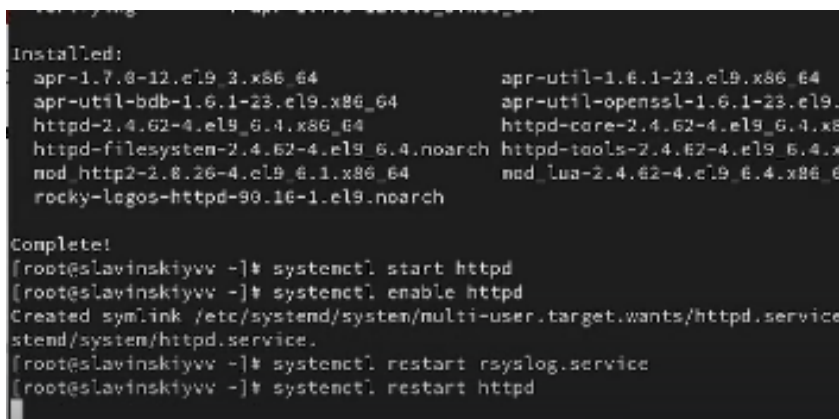


Рис. 2.11: Перезагрузка конфигурации rsyslogd и веб-службы

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`. (рис. 2.12)

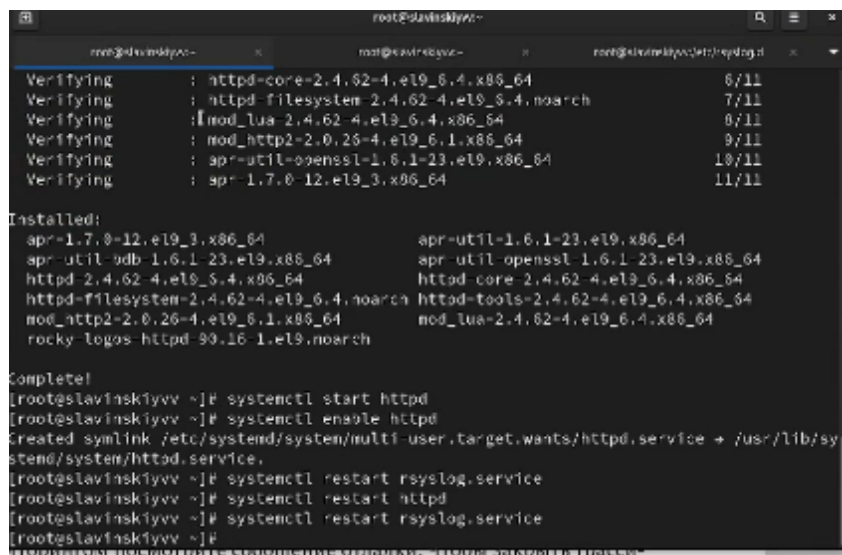
```

[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]# 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]#

```

Рис. 2.12: Создание отдельного файла конфигурации для мониторинга отладочной информации

В первой вкладке терминала снова перезапустим rsyslog: `systemctl restart rsyslog.service`. (рис. 2.13)



```

root@slavinskiyvv ~
root@slavinskiyvv ~
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 : 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

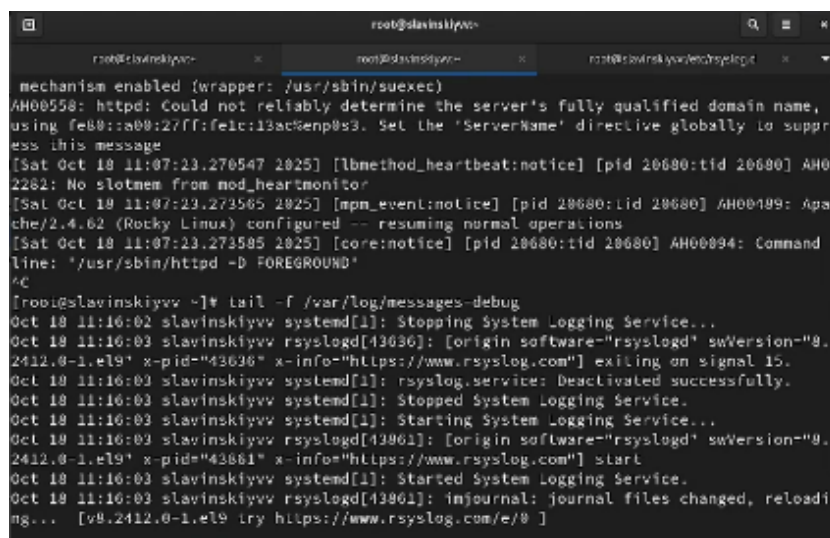
Installed:
apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64
apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.62-4.el9_6.4.x86_64  httpd-core-2.4.62-4.el9_6.4.x86_64
httpd-filesystem-2.4.62-4.el9_6.4.noarch  httpd-tools-2.4.62-4.el9_6.4.x86_64
mod_http2-2.0.26-4.el9_6.1.x86_64  mod_lua-2.4.62-4.el9_6.4.x86_64
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/sy
stemd/systemd/httpd.service.
[root@slavinskiyvv ~]# systemctl restart rsyslog.service
[root@slavinskiyvv ~]# systemctl restart httpd
[root@slavinskiyvv ~]# systemctl restart rsyslog.service
[root@slavinskiyvv ~]#

```

Рис. 2.13: Перезапуск rsyslog

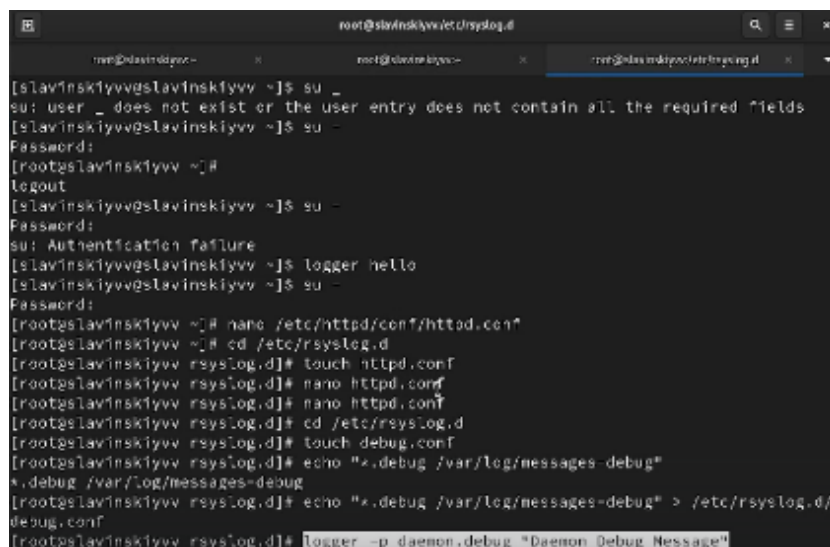
Во второй вкладке терминала запустим мониторинг отладочной информации: `tail -f /var/log/messages-debug`. (рис. 2.14)



```
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 10 11:07:23.270547 2025] [lbmethod_heartbeat:notice] [pid 20680:tfd 20680] AH0  
2282: No slotmem from mod_heartbeat  
[Sat Oct 10 11:07:23.273585 2025] [mpm_event:notice] [pid 20680:lid 20680] AH00189: Aps  
che/2.4.62 (Rocky Linux) configured -- resuming normal operations  
[Sat Oct 10 11:07:23.273585 2025] [core:notice] [pid 20680:tfd 20680] AH00994: Command  
line: '/usr/sbin/httpd -D FOREGROUND'  
^C  
[root@slavinskiyvv ~]# tail -f /var/log/messages-debug  
Oct 10 11:16:02 slavinskiyvv systemd[1]: Stopping System Logging Service...  
Oct 10 11:16:03 slavinskiyvv rsyslogd[43836]: [origin software="rsyslogd" swVersion="9.  
2412.0-1.el9" x-pid="43836" x-info="https://www.rsyslog.com"] exiting on signal 15.  
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[43861]: [origin software="rsyslogd" swVersion="9.  
2412.0-1.el9" x-pid="43861" x-info="https://www.rsyslog.com"] start  
Oct 10 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.  
Oct 10 11:16:03 slavinskiyvv rsyslogd[43861]: imjournal: journal files changed, reloadi  
ng... [v9.2412.0-1.el9 try https://www.rsyslog.com/e/9 ]
```

Рис. 2.14: Запуск мониторинга отладочной информации

В третьей вкладке терминала введем: `logger -p daemon.debug "Daemon Debug Message"`. (рис. 2.15)



```
root@slavinskiyvv /etc/rsyslog.d  
[slavinskiyvv@slavinskiyvv ~]$ su -  
su: user _ does not exist or the user entry does not contain all the required fields  
[slavinskiyvv@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 "x.debug /var/log/messages-debug"  
x.debug /var/log/messages-debug  
[root@slavinskiyvv rsyslog.d]# echo "x.debug /var/log/messages-debug" > /etc/rsyslog.d/  
debug.conf  
[root@slavinskiyvv rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
```

Рис. 2.15: Ввод команды

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: `journalctl`. (рис. 2.16)





```
root@slavinskiyvv:~# journalctl -f
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 11:16:03 slavinskiyvv systemd[1]: Stopping 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"] 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
ng... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 18 11:17:08 slavinskiyvv root[43881]: Daemon Debug Message
```

Рис. 2.18: Просмотр журнала в режиме реального времени

Для использования фильтрации просмотра конкретных параметров журнала введем `journalctl` и дважды нажмем клавишу `tab`. (рис. 2.19)

```
root@slavinskiyvv:~# journalctl
Oct 18 18:58:22 slavinskiyvv kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockb
Oct 18 18:58:22 slavinskiyvv kernel: The list of certified hardware and cloud instances
Oct 18 18:58:22 slavinskiyvv kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.1
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-provided physical RAM map:
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000000f000-0x00000000000
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x000000000000f000-0x00000000000
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000001
Oct 18 18:58:22 slavinskiyvv kernel: NX (Execute Disable) protection: active
Oct 18 18:58:22 slavinskiyvv kernel: APIC: Static calls initialized
Oct 18 18:58:22 slavinskiyvv kernel: SMBIOS 2.5 present.
Oct 18 18:58:22 slavinskiyvv kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vir
Oct 18 18:58:22 slavinskiyvv kernel: Hypervisor detected: KVM
Oct 18 18:58:22 slavinskiyvv kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
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: 0xffffffffffffff
Oct 18 18:58:22 slavinskiyvv kernel: tsc: Detected 2684.004 MHz processor
Oct 18 18:58:22 slavinskiyvv kernel: c820: update [mem 0x00000000-0x000000ff] usable ->
lines 1-23
```

Рис. 2.19: Использование фильтрации просмотра конкретных параметров журнала

Посмотрим события для `UID0`: `journalctl _UID=0`. (рис. 2.20)

```
root@slavinskiyvv:~# journalctl -u systemd-journald[264]: Journal started
Oct 10 10:58:22 slavinskiyvv systemd-journald[264]: Runtime Journal (/run/log/journal/10000000000000000000000000000000)
Oct 10 10:58:22 slavinskiyvv systemd-sysusers[267]: Creating group 'nobody' with GID 65534.
Oct 10 10:58:22 slavinskiyvv systemd-sysusers[267]: Creating group 'users' with GID 1000.
Oct 10 10:58:22 slavinskiyvv systemd-modules-load[265]: Inserted module 'fuse'.
Oct 10 10:58:22 slavinskiyvv systemd-sysusers[267]: Creating group 'dbus' with GID 288.
Oct 10 10:58:22 slavinskiyvv systemd-modules-load[265]: Module 'msr' is built in.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Load Kernel Modules.
Oct 10 10:58:22 slavinskiyvv systemd-sysusers[267]: Creating user 'dbus' (System Bus User).
Oct 10 10:58:22 slavinskiyvv systemd[1]: Starting Apply Kernel Variables...
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Create System Users.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Starting Create Static Device Nodes in /dev.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Starting Create Volatile Files and Directories.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Apply Kernel Variables.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Create Static Device Nodes in /dev.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Create Volatile Files and Directories.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished Setup Virtual Console.
Oct 10 10:58:22 slavinskiyvv systemd[1]: dracut ask for additional cmdline parameters.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Starting dracut cmdline hook...
Oct 10 10:58:22 slavinskiyvv dracut-cmdline[205]: dracut 9.6 (Blue Oxyx) dracut-cmdline hook.
Oct 10 10:58:22 slavinskiyvv dracut-cmdline[205]: Using kernel command line parameters: root=UUID=10000000000000000000000000000000 dracut=
Oct 10 10:58:22 slavinskiyvv systemd[1]: Finished dracut cmdline hook.
Oct 10 10:58:22 slavinskiyvv systemd[1]: Starting dracut pre-udev hook...
lines 1-23
```

Рис. 2.20: Просмотр сыбтия для uid 0

Для отображения последних 20 строк журнала введем: journalctl -n 20.(рис. 2.21)

```
[root@slavinskiyvv ~]# journalctl -n 20
Oct 10 11:14:01 slavinskiyvv rsyslogd[43636]: [origin software="rsyslogd" swVersion="8.24.0" module="imjournal" provide="pr"]
Oct 10 11:14:01 slavinskiyvv rsyslogd[43636]: imjournal: journal files changed, reloaded.
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" swVersion="8.24.0" module="imjournal" provide="pr"]
Oct 10 11:16:03 slavinskiyvv rsyslogd[43636]: imjournal: journal files changed, reloaded.
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[43661]: [origin software="rsyslogd" swVersion="8.24.0" module="imjournal" provide="pr"]
Oct 10 11:16:03 slavinskiyvv rsyslogd[43661]: imjournal: journal files changed, reloaded.
Oct 10 11:16:03 slavinskiyvv systemd[1]: Started System Logging Service.
Oct 10 11:16:03 slavinskiyvv rsyslogd[43661]: [origin software="rsyslogd" swVersion="8.24.0" module="imjournal" provide="pr"]
Oct 10 11:16:03 slavinskiyvv rsyslogd[43661]: imjournal: journal files changed, reloaded.
Oct 10 11:17:08 slavinskiyvv root[43861]: Daemon Debug Message
lines 1-28/20 (END)
```

Рис. 2.21: Отображение последних 20 строк журнала

Для просмотра только сообщений об ошибках введем: journalctl -p err.(рис. 2.22)





-p err.(рис. 2.24)

```
Oct 18 18:58:22 slavinskiyvv kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS V1.0
Oct 18 18:58:22 slavinskiyvv kernel: Hypervisor detected: KVM
Oct 18 18:58:22 slavinskiyvv kernel: kvm-clock: Using msrs 4b564d01 and 4b564d03
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: 0xffffffffffffff
Oct 18 18:58:22 slavinskiyvv kernel: tsc: Detected 2984.064 MHz processor
Oct 18 18:58:22 slavinskiyvv kernel: e820: update [mem 0x88300000-0x88300000] usable
[root@slavinskiyvv ~]# journalctl --since yesterday -p err
Oct 18 18:58:22 slavinskiyvv kernel: RETbleed: WARNING: Spectre v2 mitigation leaves
Oct 18 18:58:22 slavinskiyvv kernel: Warning: Unmaintained driver is detected: el800
Oct 18 18:58:23 slavinskiyvv kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems
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_table
Oct 18 18:58:25 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip6_table
Oct 18 18:58:25 slavinskiyvv kernel: Warning: Unmaintained driver is detected: ip_set
Oct 18 18:58:34 slavinskiyvv gdm-password[2150]: gkr-pam: unable to locate daemon con
Oct 18 18:58:35 slavinskiyvv systemd[2153]: Failed to start Application launched by gdm
Oct 18 18:58:35 slavinskiyvv systemd[2153]: Failed to start Application launched by gdm
Oct 18 18:58:35 slavinskiyvv systemd[2153]: Failed to start Application launched by gdm
Oct 18 18:58:35 slavinskiyvv gdm-launch-environment[1215]: GLib-GObject: g_object_unref
```

Рис. 2.24: Все сообщения с ошибкой приоритета

Если нам нужна детальная информация, то будем использовать journalctl -o verbose.(рис. 2.25)

```
Oct 18 19:58:36 slavinskiyvv gdm-launch-environment[1215]: GLib-GObject: g_object_unref
[root@slavinskiyvv ~]# journalctl -o verbose
Sat 2025-10-18 18:58:22.284536 M5K [s-e4f84208efcd4c51893a2495af66d3fa;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=bd69652ae92748ae8b335d52b3b91df
_HOSTNAME=slavinskiyvv
_RUNTIME_SCOPE=initrd
Sat 2025-10-18 18:58:22.284552 M5K [s-e4f84208efcd4c51893a2495af66d3fa;1-2;b-22be8349b2
_SOURCE_MONOTONIC_TIMESTAMP=3
_TRANSPORT=kernel
_PRIORITY=5
_SYSLOG_FACILITY=0
_SYSLOG_IDENTIFIER=kernel
_BOOT_ID=22be8049b5d0413494ceebab1ad45aff
_MACHINE_ID=bd69652ae92748ae8b335d52b3b91df
_HOSTNAME=slavinskiyvv
_RUNTIME_SCOPE=initrd
```

Рис. 2.25: Вывод детальной информации

Для просмотра дополнительной информации о модуле sshd введем: journalctl \_SYSTEMD\_UNIT=sshd.service(рис. 2.26)



Для принятия изменений нам необходимо или перезагрузить систему (перезапустить службу `systemd-journald` недостаточно), или использовать команду: `killall -USR1 systemd-journald`. (рис. 2.29)

```

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. 2.29: Принятие изменений

Журнал systemd теперь постоянный. Если мы хотим видеть сообщения журнала с момента последней перезагрузки, то используем: `journalctl -b` (рис. 2.30)

```
root@slavinskiyyv-  
mem@slavinskiyyv-- root@slavinskiyyv-- root@slavinskiyyv-/etc/initramfs-tools root@slavinskiyyv--  
  
Oct 10 10:58:22 slavinskiyyv kernel: The list of certified hardware and cloud instance  
Oct 10 10:58:22 slavinskiyyv kernel: Command line: BOOT_IMAGE=(hd0,msofst)/vm-linux-5.1  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS provided physical RAM map:  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x830068300e830008-0xe830068300e9f007]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x830068300e83c008-0xe830068300e9f007]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x830068300e83f008-0xe830068300e9f007]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x830068300e830008-0xe830068300dffffb]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x83006830dff0008-0xe83006830dfffbfb]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x83006830fec30008-0xe8300683fecbfbb]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x83006830fee30008-0xe8300683feebfbb]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x83006830fff0008-0xe8300683fffffbfb]  
Oct 10 10:58:22 slavinskiyyv kernel: BIOS-e820: [mem 0x830068310ef30008-0xe83006821fffffb]  
Oct 10 10:58:22 slavinskiyyv kernel: NX (Execute Disable) protection: active  
Oct 10 10:58:22 slavinskiyyv kernel: APIC: Static calls initialized  
Oct 10 10:58:22 slavinskiyyv kernel: SMBIOS 2.5 present,  
Oct 10 10:58:22 slavinskiyyv kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS Vir  
Oct 10 10:58:22 slavinskiyyv kernel: Hypervisor detected: KVM  
Oct 10 10:58:22 slavinskiyyv kernel: kvm-clock: Using msrc 4b564d01 and 4b564d06  
Oct 10 10:58:22 slavinskiyyv kernel: kvm-clock: using sched offset of 4946798051 cycles  
Oct 10 10:58:22 slavinskiyyv kernel: clocksource: kvm-clock: mask: 0xfffffffffffcffff  
Oct 10 10:58:22 slavinskiyyv kernel: tsc: Detected 2904.304 MHz processor  
Oct 10 10:58:22 slavinskiyyv kernel: e820: update [mem 8x0068300e-8x006830ffb] usable ->  
  
[root@slavinskiyyv ~]#
```

Рис. 2.30: Включение вывода сообщений после перезагрузки

## **3 Выводы**

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

## 4 Ответы на контрольные вопросы

1. `/etc/rsyslog.conf`
2. `/var/log/secure`
3. Еженедельная ротация
4. `*.info /var/log/messages`
5. `tail -f` - для `rsyslog`, а для `journald` `journalctl -f`
6. `journalctl -since "09:00:00" -until "15:00:00"`
7. `journalctl -b`
8. `mkdir -p /var/log/journal, chown root:systemd-journal /var/log/journal, chmod 2755 /var/log/journal, killall -USR1 systemd-journald`