

Лабораторная работа 7

Управление журналами операционной системы

Баранов Никита Дмитриевич

- Баранов Никита Дмитриевич
- студент группы НПИбд-02-24
- Российский университет дружбы народов
- 1132242977@pfur.ru

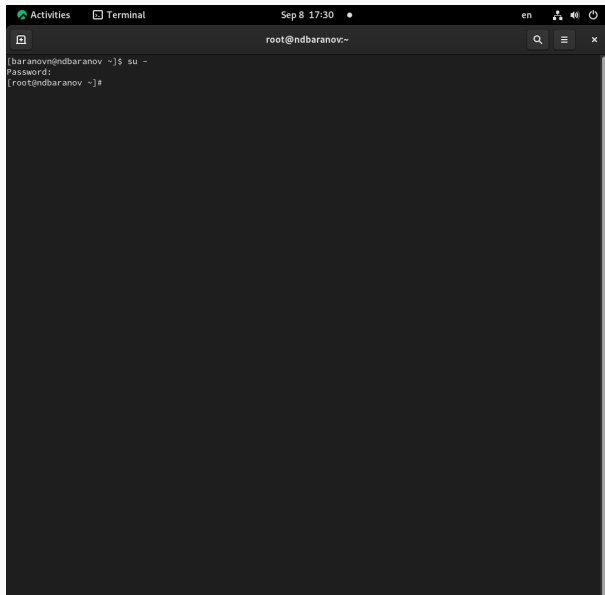


Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

1. Работа с журналом мониторинга событий в реальном времени
2. Создание и настройка конфигурации мониторинга веб-службы
3. Работа с `journalctl`
4. Работа с `journal`

Получение прав администратора



A terminal window titled "Terminal" with a date and time of "Sep 8 17:30". The window shows a user named "baranov" at a host named "ndbaranov" using the "su" command to switch to the root user. The prompt changes from "\$" to "#", indicating successful elevation of privileges.

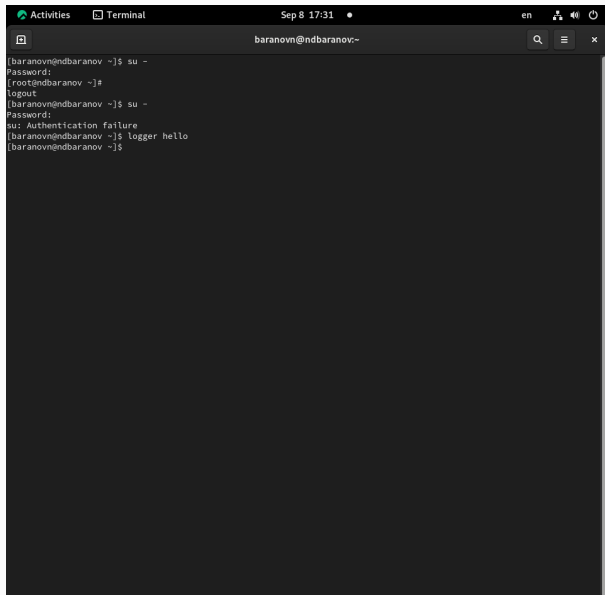
```
[baranov@ndbaranov ~]$ su -  
Password:  
[root@ndbaranov ~]#
```

Мониторинг системных событий

```
Activities Terminal Sep 8 17:31 en [Terminal icon] root@ndbaranov:~ [Search icon] [Menu icon] [Close icon]

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# tail -f /var/log/messages
Sep  8 17:28:21 ndbaranov systemd[1]: Starting Fingerprint Authentication Daemon...
Sep  8 17:28:21 ndbaranov systemd[1]: Started Fingerprint Authentication Daemon.
Sep  8 17:28:23 ndbaranov su[2992]: (to root) baranov on pts/1
Sep  8 17:28:26 ndbaranov systemd[1]: systemd-locale.service: Deactivated successfully.
Sep  8 17:28:26 ndbaranov systemd[2109]: Started Application launched by gnome-shell.
Sep  8 17:28:26 ndbaranov systemd[2109]: Started VTE child process 3041 launched by gnome-terminal-server process 2831.
Sep  8 17:28:31 ndbaranov su[3071]: (to root) baranov on pts/2
Sep  8 17:28:43 ndbaranov geoclue[1773]: Service not used for 60 seconds. Shutting down..
Sep  8 17:28:43 ndbaranov systemd[1]: geoclue.service: Deactivated successfully.
Sep  8 17:28:46 ndbaranov systemd[1]: realmd.service: Deactivated successfully.
Sep  8 17:28:51 ndbaranov systemd[1]: fprintd.service: Deactivated successfully.
Sep  8 17:28:59 ndbaranov PackageKit[1799]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Sep  8 17:28:59 ndbaranov PackageKit[1799]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Sep  8 17:29:01 ndbaranov systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Sep  8 17:29:19 ndbaranov systemd[1]: Starting Fingerprint Authentication Daemon...
Sep  8 17:29:19 ndbaranov systemd[1]: Started Fingerprint Authentication Daemon.
Sep  8 17:29:25 ndbaranov su[3163]: FAILED SU (to root) baranov on pts/0
Sep  8 17:29:44 ndbaranov baranov[3195]: hello
Sep  8 17:29:50 ndbaranov systemd[1]: fprintd.service: Deactivated successfully.
^C
[root@ndbaranov ~]# tail -n 20 /var/log/secure
Sep  8 17:27:30 ndbaranov polkitd[797]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on 0.0.0.0 port 22.
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on :: port 22.
Sep  8 17:27:33 ndbaranov systemd[1174]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Sep  8 17:27:33 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Sep  8 17:27:39 ndbaranov polkitd[797]: Registered Authentication Agent for unix-session:c1 (system bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep  8 17:27:50 ndbaranov gdm-password[2096]: gkr-pam: unable to locate daemon control file
Sep  8 17:27:50 ndbaranov gdm-password[2096]: gkr-pam: stashed password to try later in open session
Sep  8 17:27:50 ndbaranov systemd[2109]: pam_unix(systemd-user:session): session opened for user baranov(uid=1000) by baranov(uid=0)
Sep  8 17:27:50 ndbaranov gdm-password[2096]: pam_unix(gdm-password:session): session opened for user baranov(uid=1000) by baranov(uid=0)
Sep  8 17:27:51 ndbaranov gdm-password[2096]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep  8 17:27:53 ndbaranov polkitd[797]: 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)
Sep  8 17:27:57 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Sep  8 17:27:57 ndbaranov polkitd[797]: 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)
Sep  8 17:28:14 ndbaranov su[2915]: pam_unix(su:session): session opened for user root(uid=0) by baranov(uid=1000)
Sep  8 17:28:14 ndbaranov su[2915]: pam_unix(su:session): session opened for user root(uid=0) by baranov(uid=1000)
```

Ошибочный вход и logger



A terminal window titled "Terminal" with a date and time of "Sep 8 17:31". The window shows a user named "baranov" at a host named "ndbaranov". The user attempts to switch to root using "su -", but fails due to an authentication error. They then use "logger hello" to log the event, which succeeds.

```
[baranov@ndbaranov ~]$ su -  
Password:  
[root@ndbaranov ~]#  
logout  
[baranov@ndbaranov ~]$ su -  
Password:  
su: Authentication failure  
[baranov@ndbaranov ~]$ logger hello  
[baranov@ndbaranov ~]$
```

Просмотр логов безопасности

```
Activities Terminal Sep 8 17:31 en [Terminal icon] root@ndbaranov:~ [Search icon] [Menu icon] [Close icon]

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# tail -f /var/log/messages
Sep  8 17:28:21 ndbaranov systemd[1]: Starting Fingerprint Authentication Daemon...
Sep  8 17:28:21 ndbaranov systemd[1]: Started Fingerprint Authentication Daemon.
Sep  8 17:28:23 ndbaranov su[2992]: (to root) baranov on pts/1
Sep  8 17:28:26 ndbaranov systemd[1]: systemd-locale.service: Deactivated successfully.
Sep  8 17:28:26 ndbaranov systemd[2109]: Started Application launched by gnome-shell.
Sep  8 17:28:26 ndbaranov systemd[2109]: Started VTE child process 3041 launched by gnome-terminal-server process 2831.
Sep  8 17:28:31 ndbaranov su[3071]: (to root) baranov on pts/2
Sep  8 17:28:43 ndbaranov geoclue[1773]: Service not used for 60 seconds. Shutting down..
Sep  8 17:28:43 ndbaranov systemd[1]: geoclue.service: Deactivated successfully.
Sep  8 17:28:46 ndbaranov systemd[1]: realmd.service: Deactivated successfully.
Sep  8 17:28:51 ndbaranov systemd[1]: fprintd.service: Deactivated successfully.
Sep  8 17:28:59 ndbaranov PackageKit[1799]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Sep  8 17:28:59 ndbaranov PackageKit[1799]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Sep  8 17:29:01 ndbaranov systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Sep  8 17:29:19 ndbaranov systemd[1]: Starting Fingerprint Authentication Daemon...
Sep  8 17:29:19 ndbaranov systemd[1]: Started Fingerprint Authentication Daemon.
Sep  8 17:29:25 ndbaranov su[3163]: FAILED SU (to root) baranov on pts/0
Sep  8 17:29:44 ndbaranov baranov[3195]: hello
Sep  8 17:29:50 ndbaranov systemd[1]: fprintd.service: Deactivated successfully.
^C
[root@ndbaranov ~]# tail -n 20 /var/log/secure
Sep  8 17:27:30 ndbaranov polkitd[797]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on 0.0.0.0 port 22.
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on :: port 22.
Sep  8 17:27:33 ndbaranov systemd[1174]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Sep  8 17:27:33 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Sep  8 17:27:39 ndbaranov polkitd[797]: Registered Authentication Agent for unix-session:cl (system bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep  8 17:27:50 ndbaranov gdm-password[12096]: gkr-pam: unable to locate daemon control file
Sep  8 17:27:50 ndbaranov gdm-password[12096]: gkr-pam: stashed password to try later in open session
Sep  8 17:27:50 ndbaranov systemd[2109]: pam_unix(systemd-user:session): session opened for user baranov(uid=1000) by baranov(uid=0)
Sep  8 17:27:50 ndbaranov gdm-password[12096]: pam_unix(gdm-password:session): session opened for user baranov(uid=1000) by baranov(uid=0)
Sep  8 17:27:51 ndbaranov gdm-password[12096]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep  8 17:27:53 ndbaranov polkitd[797]: 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)
Sep  8 17:27:57 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Sep  8 17:27:57 ndbaranov polkitd[797]: 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)
Sep  8 17:28:14 ndbaranov su[2915]: pam_unix(su:session): session opened for user root(uid=0) by baranov(uid=1000)
Sep  8 17:28:14 ndbaranov su[2915]: pam_unix(su:session): session opened for user root(uid=0) by baranov(uid=1000)
```


Установка Apache

```
Activities Terminal Sep 8 17:33 en root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                381 B/s | 4.1 kB    00:10
Rocky Linux 9 - AppStream              424 B/s | 4.5 kB    00:10
Rocky Linux 9 - Extras                 277 B/s | 2.9 kB    00:10
Dependencies resolved.
=====
Package      Arch      Version      Repository      Size
=====
Installing:
httpd        x86_64    2.4.62-4.el9    appstream      45 k
Installing dependencies:
apr          x86_64    1.7.0-12.el9_3    appstream      122 k
apr-util     x86_64    1.6.1-23.el9      appstream      94 k
apr-util-bdb x86_64    1.6.1-23.el9      appstream      12 k
httpd-core   x86_64    2.4.62-4.el9      appstream      1.4 M
httpd-filessystem noarch    2.4.62-4.el9      appstream      12 k
httpd-tools  x86_64    2.4.62-4.el9      appstream      78 k
rocky-logos-httpd noarch    90.16-1.el9        appstream      24 k
Installing weak dependencies:
apr-util-openssl x86_64    1.6.1-23.el9      appstream      14 k
mod_http2        x86_64    2.0.26-4.el9      appstream      163 k
mod_lua          x86_64    2.4.62-4.el9      appstream      58 k
=====
Transaction Summary
=====
Install 11 Packages

Total download size: 2.0 M
Installed size: 6.1 M
Downloading Packages:
(1/11): httpd-2.4.62-4.el9.x86_64.rpm                7.8 kB/s | 45 kB    00:05
(2/11): apr-util-bdb-1.6.1-23.el9.x86_64.rpm          2.1 kB/s | 12 kB    00:05
(3/11): httpd-core-2.4.62-4.el9.x86_64.rpm            236 kB/s | 1.4 MB    00:05
(4/11): rocky-logos-httpd-90.16-1.el9.noarch.rpm       80 kB/s | 24 kB    00:00
(5/11): apr-util-1.6.1-23.el9.x86_64.rpm              300 kB/s | 94 kB    00:00
(6/11): httpd-tools-2.4.62-4.el9.x86_64.rpm           1.0 MB/s | 78 kB    00:00
(7/11): mod_lua-2.4.62-4.el9.x86_64.rpm               563 kB/s | 58 kB    00:00
(8/11): apr-util-openssl-1.6.1-23.el9.x86_64.rpm      213 kB/s | 14 kB    00:00
(9/11): mod_http2-2.0.26-4.el9.x86_64.rpm             857 kB/s | 163 kB   00:00
(10/11): httpd-filessystem-2.4.62-4.el9.noarch.rpm      181 kB/s | 12 kB    00:00
(11/11): apr-1.7.0-12.el9_3.x86_64.rpm               888 kB/s | 122 kB   00:00
=====
Total                                           169 kB/s | 2.0 MB    00:12
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
```

Запуск Apache

```
Activities Terminal Sep 8 17:33 en root@ndbaranov:~

(6/11): httpd-tools-2.4.62-4.el9.x86_64.rpm 1.0 MB/s | 78 kB 00:00
(7/11): mod_lua-2.4.62-4.el9.x86_64.rpm 563 kB/s | 58 kB 00:00
(8/11): apr-util-openssl-1.6.1-23.el9.x86_64.rpm 213 kB/s | 14 kB 00:00
(9/11): mod_http2-2.0.26-4.el9.x86_64.rpm 857 kB/s | 163 kB 00:00
(10/11): httpd-fsfilesystem-2.4.62-4.el9.noarch.rpm 181 kB/s | 12 kB 00:00
(11/11): apr-1.7.0-12.el9_3.x86_64.rpm 888 kB/s | 122 kB 00:00
-----
Total 169 kB/s | 2.0 MB 00:12
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : apr-1.7.0-12.el9_3.x86_64 1/11
Installing : apr-util-openssl-1.6.1-23.el9.x86_64 2/11
Installing : apr-util-1.6.1-23.el9.x86_64 3/11
Installing : apr-util-bdb-1.6.1-23.el9.x86_64 4/11
Installing : httpd-tools-2.4.62-4.el9.x86_64 5/11
Running scriptlet: httpd-fsfilesystem-2.4.62-4.el9.noarch 6/11
Installing : httpd-fsfilesystem-2.4.62-4.el9.noarch 6/11
Installing : httpd-core-2.4.62-4.el9.x86_64 7/11
Installing : mod_lua-2.4.62-4.el9.x86_64 8/11
Installing : rocky-logos-httpd-90.16-1.el9.noarch 9/11
Installing : mod_http2-2.0.26-4.el9.x86_64 10/11
Installing : httpd-2.4.62-4.el9.x86_64 11/11
Running scriptlet: httpd-2.4.62-4.el9.x86_64 11/11
Verifying : apr-util-bdb-1.6.1-23.el9.x86_64 1/11
Verifying : httpd-2.4.62-4.el9.x86_64 2/11
Verifying : httpd-core-2.4.62-4.el9.x86_64 3/11
Verifying : apr-util-1.6.1-23.el9.x86_64 4/11
Verifying : rocky-logos-httpd-90.16-1.el9.noarch 5/11
Verifying : httpd-tools-2.4.62-4.el9.x86_64 6/11
Verifying : mod_http2-2.0.26-4.el9.x86_64 7/11
Verifying : mod_lua-2.4.62-4.el9.x86_64 8/11
Verifying : apr-util-openssl-1.6.1-23.el9.x86_64 9/11
Verifying : apr-1.7.0-12.el9_3.x86_64 10/11
Verifying : httpd-fsfilesystem-2.4.62-4.el9.noarch 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.x86_64 httpd-core-2.4.62-4.el9.x86_64
httpd-fsfilesystem-2.4.62-4.el9.noarch httpd-tools-2.4.62-4.el9.x86_64 mod_http2-2.0.26-4.el9.x86_64
mod_lua-2.4.62-4.el9.x86_64 rocky-logos-httpd-90.16-1.el9.noarch

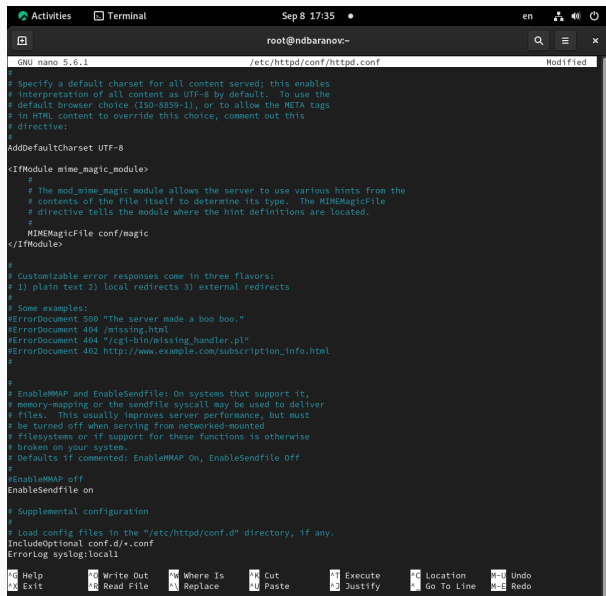
Complete!
[root@ndbaranov ~]# systemctl start httpd
[root@ndbaranov ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ndbaranov ~]#
```

Просмотр error_log Apache

```
Activities Terminal Sep 8 17:34 en
root@ndbaranov:~

Sep  8 17:29:19 ndbaranov systemd[1]: Started Fingerprint Authentication Daemon.
Sep  8 17:29:25 ndbaranov su[3163]: FAILED SU (to root) baranovn on pts/0
Sep  8 17:29:44 ndbaranov baranovn[3195]: hello
Sep  8 17:29:50 ndbaranov systemd[1]: fprintd.service: Deactivated successfully.
^C
[root@ndbaranov ~]# tail -n 20 /var/log/secure
Sep  8 17:27:30 ndbaranov polkitd[797]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on 0.0.0.0 port 22.
Sep  8 17:27:32 ndbaranov sshd[1139]: Server listening on :: port 22.
Sep  8 17:27:33 ndbaranov systemd[1174]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(u
id=0)
Sep  8 17:27:33 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session opened for
user gdm(uid=42) by (uid=0)
Sep  8 17:27:39 ndbaranov polkitd[797]: Registered Authentication Agent for unix-session:cl (system bus name :1.26 [/
usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep  8 17:27:50 ndbaranov gdm-password[2096]: gkr-pam: unable to locate daemon control file
Sep  8 17:27:50 ndbaranov gdm-password[2096]: gkr-pam: stashed password to try later in open session
Sep  8 17:27:50 ndbaranov systemd[2109]: pam_unix(systemd-user:session): session opened for user baranovn(uid=1000) b
y baranovn(uid=0)
Sep  8 17:27:50 ndbaranov gdm-password[2096]: pam_unix(gdm-password:session): session opened for user baranovn(uid=1
000) by baranovn(uid=0)
Sep  8 17:27:51 ndbaranov gdm-password[2096]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep  8 17:27:53 ndbaranov polkitd[797]: Registered Authentication Agent for unix-session:2 (system bus name :1.69 [/u
sr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep  8 17:27:57 ndbaranov gdm-launch-environment[1169]: pam_unix(gdm-launch-environment:session): session closed for
user gdm
Sep  8 17:27:57 ndbaranov polkitd[797]: 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)
Sep  8 17:28:14 ndbaranov su[2915]: pam_unix(su-l:session): session opened for user root(uid=0) by baranovn(uid=1000)
Sep  8 17:28:23 ndbaranov su[2992]: pam_unix(su-l:session): session opened for user root(uid=0) by baranovn(uid=1000)
Sep  8 17:28:31 ndbaranov su[3071]: pam_unix(su-l:session): session opened for user root(uid=0) by baranovn(uid=1000)
Sep  8 17:29:03 ndbaranov su[2915]: pam_unix(su-l:session): session closed for user root
Sep  8 17:29:23 ndbaranov unix_chkpwd[3171]: password check failed for user (root)
Sep  8 17:29:23 ndbaranov su[3163]: pam_unix(su-l:auth): authentication failure; logname=baranovn uid=1000 euid=0 tty
=/dev/pts/0 ruser=baranovn rhost= user=root
[root@ndbaranov ~]# tail -f /var/log/httpd/error_log
[Mon Sep 08 17:33:25.441545 2025] [core:notice] [pid 3716:tid 3716] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Mon Sep 08 17:33:25.445342 2025] [suexec:notice] [pid 3716:tid 3716] AH01232: suEXEC mechanism enabled (wrapper: /us
r/sbin/suexec)
AH00558: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fe2a:f035
::%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Mon Sep 08 17:33:25.613000 2025] [lbmethod:heartbeat:notice] [pid 3716:tid 3716] AH02282: No slotmem from mod_heartm
onitor
[Mon Sep 08 17:33:25.634291 2025] [mpm_event:notice] [pid 3716:tid 3716] AH00489: Apache/2.4.62 (Rocky Linux) configu
red -- resuming normal operations
[Mon Sep 08 17:33:25.634400 2025] [core:notice] [pid 3716:tid 3716] AH00094: Command line: '/usr/sbin/httpd -D FOREGR
OUND'
^C
[root@ndbaranov ~]#
```

Настройка ErrorLog в httpd.conf



The screenshot shows a terminal window with the nano text editor open, editing the file /etc/httpd/conf/httpd.conf. The user is root@ndbaranov.~. The editor shows the following configuration:

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default. To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8

<IfModule mime_magic_module>
#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
MIMEMagicFile conf/magic
</IfModule>

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# 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 network-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:local
```

At the bottom of the terminal, there is a row of keyboard shortcuts for nano:

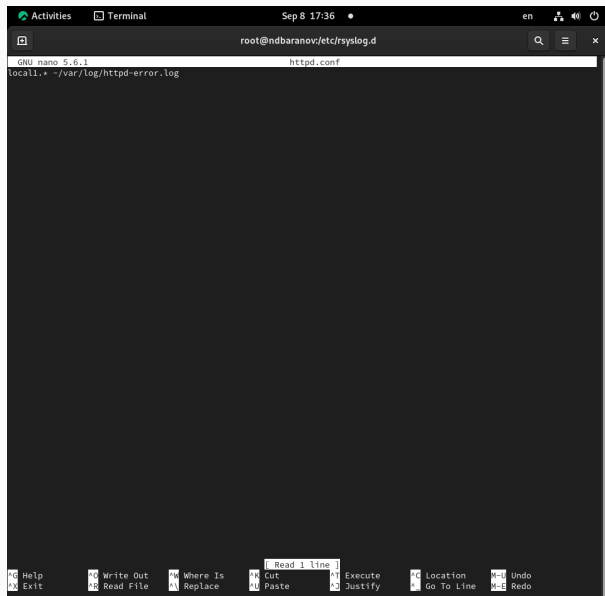
⌘ Help	⌘ Write Out	⌘ Where Is	⌘ Cut	⌘ Execute	⌘ Location	⌘ Undo
⌘ Exit	⌘ Read File	⌘ Replace	⌘ Paste	⌘ Justify	⌘ Go To Line	⌘ Redo

Создание конфигурации rsyslog

```
Activities Terminal Sep 8 17:36 en
root@ndbaranov:/etc/rsyslog.d

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]#
logout
[baranov@ndbaranov ~]$ su -
Password:
su: Authentication failure
[baranov@ndbaranov ~]$ logger hello
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# nano /etc/httpd/conf/httpd.conf
[root@ndbaranov ~]# nano /etc/httpd/conf/httpd.conf
[root@ndbaranov ~]# cd /etc/rsyslog.d
[root@ndbaranov rsyslog.d]# touch httpd.conf
[root@ndbaranov rsyslog.d]# nano httpd.conf
[root@ndbaranov rsyslog.d]#
```

Настройка правил local1



The screenshot shows a terminal window with the title bar "Activities Terminal" and the date/time "Sep 8 17:36". The terminal prompt is "root@ndbaranov:/etc/rsyslog.d". A nano text editor is open, editing the file "httpd.conf". The editor's status bar at the bottom shows "GNU nano 5.6.1" and the current file path "httpd.conf". The terminal output shows the command "local1.* -/var/log/httpd-error.log" being entered. The nano editor's menu bar at the bottom includes: "G Help", "X Exit", "O Write Out", "R Read File", "W Where Is", "A Replace", "C Cut", "U Paste", "J Read 1 line", "E Execute", "O Justify", "C Location", "G Go To Line", "U Undo", "R Redo".

```
root@ndbaranov:/etc/rsyslog.d
GNU nano 5.6.1 httpd.conf
local1.* -/var/log/httpd-error.log
```

Перезапуск служб

```
Activities Terminal Sep 8 17:37 en root@ndbaranov:~

(8/11): apr-util-openssl-1.6.1-23.el9.x86_64.rpm                213 kB/s | 14 kB    00:00
(9/11): mod_http2-2.0.26-4.el9.x86_64.rpm                    857 kB/s | 163 kB  00:00
(10/11): httpd-filesystem-2.4.62-4.el9.noarch.rpm             181 kB/s | 12 kB   00:00
(11/11): apr-1.7.0-12.el9_3.x86_64.rpm                       888 kB/s | 122 kB  00:00
-----
Total                                                         169 kB/s | 2.0 MB  00:12

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing :                                                                 1/1
  Installing : apr-1.7.0-12.el9_3.x86_64                                  1/11
  Installing : apr-util-openssl-1.6.1-23.el9.x86_64                     2/11
  Installing : apr-util-1.6.1-23.el9.x86_64                             3/11
  Installing : apr-util-bdb-1.6.1-23.el9.x86_64                         4/11
  Installing : httpd-tools-2.4.62-4.el9.x86_64                          5/11
  Running scriptlet: httpd-filesystem-2.4.62-4.el9.noarch                6/11
  Installing : httpd-filesystem-2.4.62-4.el9.noarch                     6/11
  Installing : httpd-core-2.4.62-4.el9.x86_64                           7/11
  Installing : mod_lua-2.4.62-4.el9.x86_64                              8/11
  Installing : rocky-logos-httpd-90.16-1.el9.noarch                     9/11
  Installing : mod_http2-2.0.26-4.el9.x86_64                           10/11
  Installing : httpd-2.4.62-4.el9.x86_64                                11/11
  Running scriptlet: httpd-2.4.62-4.el9.x86_64                           11/11
  Verifying   : apr-util-bdb-1.6.1-23.el9.x86_64                        1/11
  Verifying   : httpd-2.4.62-4.el9.x86_64                               2/11
  Verifying   : httpd-core-2.4.62-4.el9.x86_64                         3/11
  Verifying   : apr-util-1.6.1-23.el9.x86_64                           4/11
  Verifying   : rocky-logos-httpd-90.16-1.el9.noarch                     5/11
  Verifying   : httpd-tools-2.4.62-4.el9.x86_64                         6/11
  Verifying   : mod_http2-2.0.26-4.el9.x86_64                           7/11
  Verifying   : mod_lua-2.4.62-4.el9.x86_64                             8/11
  Verifying   : apr-util-openssl-1.6.1-23.el9.x86_64                   9/11
  Verifying   : apr-1.7.0-12.el9_3.x86_64                              10/11
  Verifying   : httpd-filesystem-2.4.62-4.el9.noarch                    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.x86_64      httpd-core-2.4.62-4.el9.x86_64
  httpd-filesystem-2.4.62-4.el9.noarch  httpd-tools-2.4.62-4.el9.x86_64  mod_http2-2.0.26-4.el9.x86_64
  mod_lua-2.4.62-4.el9.x86_64      rocky-logos-httpd-90.16-1.el9.noarch

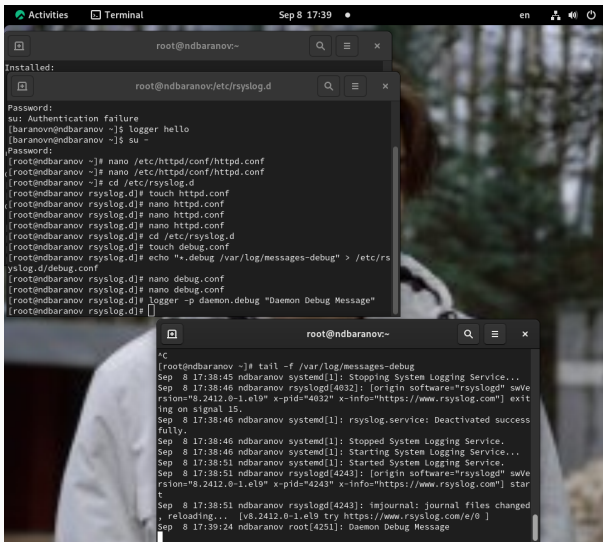
Complete!
[root@ndbaranov ~]# systemctl start httpd
[root@ndbaranov ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ndbaranov ~]# systemctl restart rsyslog.service
[root@ndbaranov ~]# systemctl restart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

Создание debug.conf

```
Activities Terminal Sep 8 17:38 en
root@ndbaranov:/etc/rsyslog.d

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


Тестирование debug-сообщений



The screenshot shows a terminal window with the following commands and output:

```
root@ndbaranov:~# nano /etc/rsyslog.d
root@ndbaranov:~# nano /etc/rsyslog.d
root@ndbaranov:~# cd /etc/rsyslog.d
root@ndbaranov:~# touch httpd.conf
root@ndbaranov:~# nano httpd.conf
root@ndbaranov:~# nano httpd.conf
root@ndbaranov:~# cd /etc/rsyslog.d
root@ndbaranov:~# touch debug.conf
root@ndbaranov:~# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@ndbaranov:~# nano debug.conf
root@ndbaranov:~# nano debug.conf
root@ndbaranov:~# logger -p daemon.debug "Daemon Debug Message"
root@ndbaranov:~#
```

Below the first terminal window, a second terminal window shows the output of the `tail -f /var/log/messages-debug` command:

```
^C
[root@ndbaranov:~]# tail -f /var/log/messages-debug
Sep  8 17:38:45 ndbaranov systemd[1]: Stopping System Logging Service...
Sep  8 17:38:46 ndbaranov rsyslogd[4032]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4032" x-info="https://www.rsyslog.com"] exiting on signal 15.
Sep  8 17:38:46 ndbaranov systemd[1]: rsyslog.service: Deactivated successfully.
Sep  8 17:38:46 ndbaranov systemd[1]: Stopped System Logging Service.
Sep  8 17:38:46 ndbaranov systemd[1]: Starting System Logging Service...
Sep  8 17:38:51 ndbaranov systemd[1]: Started System Logging Service.
Sep  8 17:38:51 ndbaranov rsyslogd[4243]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4243" x-info="https://www.rsyslog.com"] starting
Sep  8 17:38:51 ndbaranov rsyslogd[4243]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Sep  8 17:39:24 ndbaranov root[4251]: Daemon Debug Message
```

journalctl: просмотр журнала

```
Activities Terminal Sep 8 17:40 en
root@ndbaranov:~
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.r
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be v
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/o
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009fffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dfffff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dffffffffff] ACPI data
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec000000-0x00000000fec00ffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee000000-0x00000000fee00ffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fff000000-0x00000000fffffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000001000000000-0x000000011fffffff] usable
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
Sep 08 17:27:19 ndbaranov kernel: SMBIOS 2.5 present.
Sep 08 17:27:19 ndbaranov kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 08 17:27:19 ndbaranov kernel: Hypervisor detected: KVM
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: using sched offset of 8893561305 cycles
Sep 08 17:27:19 ndbaranov kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_id
Sep 08 17:27:19 ndbaranov kernel: tsc: Detected 3593.376 MHz processor
Sep 08 17:27:19 ndbaranov kernel: e820: update [mem 0x000000000-0x00000ffff] usable ==> reserved
Sep 08 17:27:19 ndbaranov kernel: e820: remove [mem 0x000a00000-0x000ffffff] usable
Sep 08 17:27:19 ndbaranov kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 08 17:27:19 ndbaranov kernel: MTRR map: 3 entries (3 fixed + 0 variable; max 19), built from 8 variable MTRRs
Sep 08 17:27:19 ndbaranov kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Sep 08 17:27:19 ndbaranov kernel: CPU MTRRs all blank - virtualized system.
Sep 08 17:27:19 ndbaranov kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
Sep 08 17:27:19 ndbaranov kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
Sep 08 17:27:19 ndbaranov kernel: RAMDISK: [mem 0x30cda000-0x34664fff]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Early table checksum verification disabled
Sep 08 17:27:19 ndbaranov kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
Sep 08 17:27:19 ndbaranov kernel: ACPI: XSDT 0x0000000000000030 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
Sep 08 17:27:19 ndbaranov kernel: ACPI: FACP 0x00000000000000f0 0000f4 (v04 VBOX VBOXFACP 00000001 ASL 00000001)
Sep 08 17:27:19 ndbaranov kernel: ACPI: DSDT 0x0000000000000310 002353 (v02 VBOX VBOXBIOS 00000002 VBOX 000298f4)
Sep 08 17:27:19 ndbaranov kernel: ACPI: FACS 0x0000000000000200 000040
Sep 08 17:27:19 ndbaranov kernel: ACPI: FACS 0x0000000000000200 000040
Sep 08 17:27:19 ndbaranov kernel: ACPI: APIC 0x0000000000000240 00006C (v02 VBOX VBOXAPIC 00000001 ASL 00000001)
Sep 08 17:27:19 ndbaranov kernel: ACPI: SSDT 0x00000000000002B0 00005F (v01 VBOX VBOXCPU0 00000002 VBOX 000298f4)
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving FACP table memory at [mem 0xdffff00f0-0xdffff01e3]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving DSDT table memory at [mem 0xdffff0310-0xdffff2662]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving FACS table memory at [mem 0xdffff0200-0xdffff023f]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving FACS table memory at [mem 0xdffff0200-0xdffff023f]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving APIC table memory at [mem 0xdffff0240-0xdffff02ab]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving SSDT table memory at [mem 0xdffff02b0-0xdffff030e]
Sep 08 17:27:19 ndbaranov kernel: No NUMA configuration found
Sep 08 17:27:19 ndbaranov kernel: Faking a node at [mem 0x0000000000000000-0x000000011fffffff]
lines 1-49
```

journalctl: просмотр полей

```
Activities Terminal Sep 8 17:41 en root@ndbaranov:~
.AUDIT_LOGINID=
.AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
COMMAND=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
DBUS_BROKER_MESSAGE_DESTINATION=
DBUS_BROKER_MESSAGE_INTERFACE=
DBUS_BROKER_MESSAGE_MEMBER=
DBUS_BROKER_MESSAGE_PATH=
DBUS_BROKER_MESSAGE_SERIAL=
DBUS_BROKER_MESSAGE_SIGNATURE=
DBUS_BROKER_MESSAGE_TYPE=
DBUS_BROKER_MESSAGE_UNIX_FDS=
DBUS_BROKER_METRICS_DISPATCH_AVG=
DBUS_BROKER_METRICS_DISPATCH_COUNT=
DBUS_BROKER_METRICS_DISPATCH_MAX=
DBUS_BROKER_METRICS_DISPATCH_MIN=
DBUS_BROKER_METRICS_DISPATCH_STDEV=
DBUS_BROKER_POLICY_TYPE=
DBUS_BROKER_RECEIVER_SECURITY_LABEL=
DBUS_BROKER_RECEIVER_UNIQUE_NAME=
DBUS_BROKER_RECEIVER_WELL_KNOWN_NAME_@=
DBUS_BROKER_SENDER_SECURITY_LABEL=
DBUS_BROKER_SENDER_UNIQUE_NAME=
DBUS_BROKER_TRANSMIT_ACTION=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
ERRNO=
_EXIT_CODE=
EXIT_STATUS=
_GID=
GLIB_DOMAIN=
GLIB_OLD_LOG_API=
_HOSTNAME=
INITRD_USEC=
--More--
_KERNEL_SUBSYSTEM=
KERNEL_USEC=
LEADER=
LIMIT=
LIMIT_PRETTY=
_MACHINE_ID=
MAX_USE=
MAX_USE_PRETTY=
MESSAGE=
MESSAGE_ID=
NM_DEVICE=
NM_LOG_DOMAINS=
NM_LOG_LEVEL=
_PID=
PRIORITY=
REALMD_OPERATION=
_RUNTIME_SCOPE=
SEAT_ID=
_SELINUX_CONTEXT=
SESSION_ID=
_SOURCE_MONOTONIC_TIMESTAMP=
_SOURCE_REALTIME_TIMESTAMP=
SSSD_DOMAIN=
SSSD_PRG_NAME=
_STREAM_ID=
SYSLOG_FACILITY=
SYSLOG_IDENTIFIER=
SYSLOG_PID=
SYSLOG_RAW=
SYSLOG_TIMESTAMP=
_SYSTEMD_CGROUP=
_SYSTEMD_INVOCATION_ID=
_SYSTEMD_OWNER_UID=
_SYSTEMD_SESSION=
_SYSTEMD_SLICE=
_SYSTEMD_UNIT=
_SYSTEMD_USER_SLICE=
_SYSTEMD_USER_UNIT=
_THREAD_ID=
TID=
TIMESTAMP_BOOTTIME=
TIMESTAMP_MONOTONIC=
TRANSPORT=
_UDEV_DEVLINK=
_UDEV_DEVNODE=
_UDEV_SYSNAME=
_UID=
UNIT=
UNIT_RESULT=
```

journalctl: фильтрация по UID

```
Activities Terminal Sep 8 17:42 en
root@ndbaranov:~

GLIB_DOMAIN=_UDEV_SYSNAME=
GLIB_OLD_LOG_API=_UID=
_HOSTNAME=_UNIT=
INITRD_USEC=_UNIT_RESULT=

(root@ndbaranov ~) # journalctl _UID=0
Sep 08 17:27:19 ndbaranov systemd-journald[247]: Journal started
Sep 08 17:27:19 ndbaranov systemd-journald[247]: Runtime Journal (/run/log/journal/ce5436fdb891482c88cb03327500575e)
Sep 08 17:27:19 ndbaranov systemd-sysusers[249]: Creating group 'nobody' with GID 65534.
Sep 08 17:27:19 ndbaranov systemd-sysusers[249]: Creating group 'users' with GID 100.
Sep 08 17:27:19 ndbaranov systemd-sysusers[249]: Creating group 'dbus' with GID 81.
Sep 08 17:27:19 ndbaranov systemd-sysusers[249]: Creating user 'dbus' (System Message Bus) with UID 81 and GID 81.
Sep 08 17:27:19 ndbaranov systemd-modules-load[248]: Inserted module 'fuse'
Sep 08 17:27:19 ndbaranov systemd-modules-load[248]: Module 'msr' is built in
Sep 08 17:27:19 ndbaranov systemd[1]: Starting Create Volatile Files and Directories...
Sep 08 17:27:19 ndbaranov systemd[1]: Finished Load Kernel Modules.
Sep 08 17:27:19 ndbaranov systemd[1]: Starting Apply Kernel Variables...
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Create Static Device Nodes in /dev.
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Apply Kernel Variables.
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Create Volatile Files and Directories.
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Setup Virtual Console.
Sep 08 17:27:20 ndbaranov systemd[1]: dracut ask for additional cmdline parameters was skipped because no trigger co
Sep 08 17:27:20 ndbaranov systemd[1]: Starting dracut cmdline hook...
Sep 08 17:27:20 ndbaranov dracut-cmdline[264]: dracut-9.6 (Blue Onyx) dracut-057-88.git20250311.e19.6
Sep 08 17:27:20 ndbaranov dracut-cmdline[264]: Using kernel command line parameters: BOOT_IMAGE=(hd0,msdos1)/vmlin
Sep 08 17:27:20 ndbaranov systemd[1]: Finished dracut cmdline hook.
Sep 08 17:27:20 ndbaranov systemd[1]: Starting dracut pre-udev hook...
Sep 08 17:27:20 ndbaranov systemd[1]: Finished dracut pre-udev hook.
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Rule-based Manager for Device Events and Files...
Sep 08 17:27:20 ndbaranov systemd-udevd[379]: Using default interface naming scheme 'rhel-9.0'.
Sep 08 17:27:20 ndbaranov systemd[1]: Started Rule-based Manager for Device Events and Files.
Sep 08 17:27:20 ndbaranov systemd[1]: dracut pre-trigger hook was skipped because no trigger condition checks were m
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Coldplug All udev Devices...
Sep 08 17:27:20 ndbaranov systemd[1]: sys-module-fuse-devices: Failed to enqueue SYSTEMD_WANTS= job, ignoring: Unit s
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Coldplug All udev Devices.
Sep 08 17:27:20 ndbaranov systemd[1]: nm-initrd.service was skipped because of an unset condition check (ConditionPa
Sep 08 17:27:20 ndbaranov systemd[1]: Reached target Network.
Sep 08 17:27:20 ndbaranov systemd[1]: nm-wait-online-initrd.service was skipped because of an unset condition check
Sep 08 17:27:20 ndbaranov systemd[1]: Starting dracut initqueue hook...
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Show Plymouth Boot Screen...
Sep 08 17:27:20 ndbaranov systemd[1]: Received SIGRTMIN-20 from PID 392 (plymouthd).
Sep 08 17:27:20 ndbaranov systemd[1]: Started Show Plymouth Boot Screen.
Sep 08 17:27:20 ndbaranov systemd[1]: Dispatch Password Requests to Console Directory Watch was skipped because of a
Sep 08 17:27:20 ndbaranov systemd[1]: Started Forward Password Requests to Plymouth Directory Watch.
Sep 08 17:27:20 ndbaranov systemd[1]: Reached target Path Units.
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: Scanning devices sda2 for LVM logical volumes rl/root
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/swap
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/root linear
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/swap linear
Sep 08 17:27:22 ndbaranov systemd[1]: Found device /dev/mapper/rl-root.
Sep 08 17:27:22 ndbaranov systemd[1]: Reached target Initrd Root Device.
```

journalctl: последние записи

```
Activities Terminal Sep 8 17:42 en [Icons] root@ndbaranov:~

Sep 08 17:27:20 ndbaranov systemd[1]: Finished dracut pre-udev hook.
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Rule-based Manager for Device Events and Files...
Sep 08 17:27:20 ndbaranov systemd-udevd[379]: Using default interface naming scheme 'rhel-9.0'.
Sep 08 17:27:20 ndbaranov systemd[1]: Started Rule-based Manager for Device Events and Files.
Sep 08 17:27:20 ndbaranov systemd[1]: dracut pre-trigger hook was skipped because no trigger condition checks were m
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Coldplug All udev Devices...
Sep 08 17:27:20 ndbaranov systemd[1]: sys-module-fuse.device: Failed to enqueue SYSTEMD_WANTS= job, ignoring: Unit s
Sep 08 17:27:20 ndbaranov systemd[1]: Finished Coldplug All udev Devices.
Sep 08 17:27:20 ndbaranov systemd[1]: nm-initrd.service was skipped because of an unmet condition check (ConditionPa
Sep 08 17:27:20 ndbaranov systemd[1]: Reached target Network.
Sep 08 17:27:20 ndbaranov systemd[1]: nm-wait-online-initrd.service was skipped because of an unmet condition check
Sep 08 17:27:20 ndbaranov systemd[1]: Starting dracut initqueue hook...
Sep 08 17:27:20 ndbaranov systemd[1]: Starting Show Plymouth Boot Screen...
Sep 08 17:27:20 ndbaranov systemd[1]: Received SIGRTMIN+20 from PID 392 (plymouthd).
Sep 08 17:27:20 ndbaranov systemd[1]: Started Show Plymouth Boot Screen.
Sep 08 17:27:20 ndbaranov systemd[1]: Dispatch Password Requests to Console Directory Watch was skipped because of a
Sep 08 17:27:20 ndbaranov systemd[1]: Started Forward Password Requests to Plymouth Directory Watch.
Sep 08 17:27:20 ndbaranov systemd[1]: Reached target Path Units.
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: Scanning devices sda2 for LVM logical volumes rl/root
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/swap
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/root linear
Sep 08 17:27:22 ndbaranov dracut-initqueue[499]: rl/swap linear
Sep 08 17:27:22 ndbaranov systemd[1]: Found device /dev/mapper/rl-root.
Sep 08 17:27:22 ndbaranov systemd[1]: Reached target Initrd Root Device.
Sep 08 17:27:22 ndbaranov systemd[1]: Found device /dev/mapper/rl-swap.
Sep 08 17:27:22 ndbaranov systemd[1]: Starting Resume from hibernation using device /dev/mapper/rl-swap...
Sep 08 17:27:22 ndbaranov systemd-hibernate-resume[535]: Could not resume from '/dev/mapper/rl-swap' (253:1).
Sep 08 17:27:22 ndbaranov systemd[1]: systemd-hibernate-resume@dev-mapper-rl\x2dswap.service: Deactivated successful
[root@ndbaranov ~]# journalctl -n 20
Sep 08 17:37:20 ndbaranov systemd[1]: Starting The Apache HTTP Server...
Sep 08 17:37:25 ndbaranov httpd[4041]: AH00558: httpd: Could not reliably determine the server's fully qualified dom
Sep 08 17:37:25 ndbaranov httpd[4041]: Server configured, listening on: port 80
Sep 08 17:37:25 ndbaranov systemd[1]: Started The Apache HTTP Server.
Sep 08 17:38:13 ndbaranov PackageKit[1799]: daemon quit
Sep 08 17:38:13 ndbaranov systemd[1]: packagekit.service: Deactivated successfully.
Sep 08 17:38:13 ndbaranov systemd[1]: packagekit.service: Consumed 5.659s CPU time.
Sep 08 17:38:45 ndbaranov systemd[1]: Stopping System Logging Service...
Sep 08 17:38:46 ndbaranov rsyslogd[4032]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4032" x-info
Sep 08 17:38:46 ndbaranov systemd[1]: rsyslog.service: Deactivated successfully.
Sep 08 17:38:46 ndbaranov systemd[1]: Stopped System Logging Service.
Sep 08 17:38:46 ndbaranov systemd[1]: Starting System Logging Service...
Sep 08 17:38:51 ndbaranov systemd[1]: Started System Logging Service.
Sep 08 17:38:51 ndbaranov rsyslogd[4243]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4243" x-info
Sep 08 17:38:51 ndbaranov rsyslogd[4243]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https
Sep 08 17:39:24 ndbaranov root[4251]: Daemon Debug Message
Sep 08 17:42:25 ndbaranov systemd[1]: Starting Cleanup of Temporary Directories...
Sep 08 17:42:26 ndbaranov systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Sep 08 17:42:26 ndbaranov systemd[1]: Finished Cleanup of Temporary Directories.
Sep 08 17:42:26 ndbaranov systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated succes
lines 1-20/20 (END)
```

journalctl: просмотр ошибок

```
Activities Terminal Sep 8 17:43 en
root@ndbaranov:~

[root@ndbaranov ~]# journalctl -p err
Sep 08 17:27:21 ndbaranov kernel: Warning: Unmaintained driver is detected: e1000
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported h
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to
Sep 08 17:27:29 ndbaranov alsactl[822]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hwid us
Sep 08 17:27:31 ndbaranov kernel: Warning: Unmaintained driver is detected: ip_set
Sep 08 17:27:50 ndbaranov gdm-password[12096]: gkr-pam: unable to locate daemon control file
Sep 08 17:27:57 ndbaranov gdm-wayland-session[1228]: GLib: Source ID 2 was not found when attempting to remove it
Sep 08 17:27:57 ndbaranov gdm-launch-environment[1169]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object
[root@ndbaranov ~]# journalctl --since today
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.r
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be v
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/d
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009bfff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000000fffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000ff000-0x000000000000fffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000100000-0x000000000000fffff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000ffff000-0x000000000000fffff] ACPI data
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000100000000-0x00000001fffffffff] usable
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
Sep 08 17:27:19 ndbaranov kernel: SMBIOS 2.5 present.
Sep 08 17:27:19 ndbaranov kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 08 17:27:19 ndbaranov kernel: Hypervisor detected: KVM
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: using sched offset of 8803561385 cycles
Sep 08 17:27:19 ndbaranov kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_id
Sep 08 17:27:19 ndbaranov kernel: tsc: Detected 3593.376 MHz processor
Sep 08 17:27:19 ndbaranov kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> reserved
Sep 08 17:27:19 ndbaranov kernel: e820: remove [mem 0x00000000-0x000000fff] usable
Sep 08 17:27:19 ndbaranov kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Sep 08 17:27:19 ndbaranov kernel: MTRR map: 3 entries (3 fixed + 0 variable; max 19), built from 8 variable MTRRs
Sep 08 17:27:19 ndbaranov kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Sep 08 17:27:19 ndbaranov kernel: CPU MTRRs all blank - virtualized system.
Sep 08 17:27:19 ndbaranov kernel: last_pfn = 0x0000 max_arch_pfn = 0x400000000
Sep 08 17:27:19 ndbaranov kernel: found SMP MP-table at [mem 0x0000fbf0-0x00009bfff]
Sep 08 17:27:19 ndbaranov kernel: RAMDISK: [mem 0x30cda000-0x34664ffff]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Early table checksum verification disabled
Sep 08 17:27:19 ndbaranov kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
Sep 08 17:27:19 ndbaranov kernel: ACPI: XSDT 0x0000000000000000 00002c (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
Sep 08 17:27:19 ndbaranov kernel: ACPI: FACP 0x0000000000000000 000007 (v01 VBOX VBOXFACP 00000001 ASL 00000001)
```

journalctl: фильтрация по времени

```
Activities Terminal Sep 8 17:43 en
root@ndbaranov:~

Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02ab]
Sep 08 17:27:19 ndbaranov kernel: ACPI: Reserving SSDT table memory at [mem 0xdfff02b0-0xdfff030e]
Sep 08 17:27:19 ndbaranov kernel: No NUMA configuration found
Sep 08 17:27:19 ndbaranov kernel: Faking a node at [mem 0x0000000000000000-0x000000001fffffffff]
(root@ndbaranov ~) # journalctl --since yesterday -p err
Sep 08 17:27:21 ndbaranov kernel: Warning: Unmaintained driver is detected: e1000
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hy
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Sep 08 17:27:21 ndbaranov kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to
Sep 08 17:27:29 ndbaranov alsactl[822]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hwid us
Sep 08 17:27:31 ndbaranov kernel: Warning: Unmaintained driver is detected: ip_set
Sep 08 17:27:50 ndbaranov gdm-password[12096]: gkr-pam: unable to locate daemon control file
Sep 08 17:27:57 ndbaranov gdm-wayland-session[1228]: GLib: Source ID 2 was not found when attempting to remove it
Sep 08 17:27:57 ndbaranov gdm-launch-environment[1169]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (objec
(root@ndbaranov ~) # journalctl -o verbose
Mon 2025-09-08 17:27:19.909689 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=1;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (6
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
Mon 2025-09-08 17:27:19.909708 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=2;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat 5
Mon 2025-09-08 17:27:19.909750 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=3;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
PRIORITY=6
MESSAGE=Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev/mapper/rl-root ro r
Mon 2025-09-08 17:27:19.909758 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=4;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
```

journalctl: вывод по службе

```
Activities Terminal Sep 8 17:44 en
root@ndbaranov:~

PRIORITy=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (6
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
Mon 2025-09-08 17:27:19.909708 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=2;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITy=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat E
Mon 2025-09-08 17:27:19.909750 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=3;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
PRIORITy=6
MESSAGE=Command line: BOOT_IMAGE=(hdd,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev/mapper/rl-root ro r
Mon 2025-09-08 17:27:19.909758 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=4;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
_BOOT_ID=c912c9ff4569401aa9c31541b7d6a544
_MACHINE_ID=ce5436fdb891482c88cb03327500575e
_HOSTNAME=ndbaranov
_RUNTIME_SCOPE=initrd
PRIORITy=4
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Mon 2025-09-08 17:27:19.909764 MSK [s=ab8feab543c64577a043e852a2ae9dcc;i=5;b=c912c9ff4569401aa9c31541b7d6a544;m=3a99
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
[root@ndbaranov ~]# journalctl _SYSTEMD_UNIT=sshd.service
Sep 08 17:27:32 ndbaranov sshd[1139]: Server listening on 0.0.0.0 port 22.
Sep 08 17:27:32 ndbaranov sshd[1139]: Server listening on :: port 22.
[root@ndbaranov ~]#
```


Постоянное хранение журналов

```
Activities Terminal Sep 8 17:45 en [Search] [Menu] [Close]
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# mkdir -p /var/log/journal
[root@ndbaranov ~]# chown root:systemd-journal /var/log/journal
[root@ndbaranov ~]# chmod 775 /var/log/journal
[root@ndbaranov ~]# killall -USR1 systemd-journald
[root@ndbaranov ~]# journalctl -b
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud inst
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 fre
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000f0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000100000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000dffff0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000100000000-0x00000001
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
Sep 08 17:27:19 ndbaranov kernel: SMBIOS 2.5 present.
Sep 08 17:27:19 ndbaranov kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS
Sep 08 17:27:19 ndbaranov kernel: Hypervisor detected: KVM
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: using sched offset of 8803561305
Sep 08 17:27:19 ndbaranov kernel: clocksource: kvm-clock: mask: 0xffffffffffff
Sep 08 17:27:19 ndbaranov kernel: tsc: Detected 3593.376 Mhz processor
lines 1-23 ...skipping...
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro
skylin
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be vi
ewed at
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/de
v/mapp
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000100000-0x000000000dffff0000] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dffff0000] ACPI data
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000ffff0000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000100000000-0x0000000100000000] usable
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
```

Проверка работы хранения

```
Activities Terminal Sep 8 17:45 en root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# mkdir -p /var/log/journal
[root@ndbaranov ~]# chown root:systemd-journal /var/log/journal
[root@ndbaranov ~]# chmod 775 /var/log/journal
[root@ndbaranov ~]# killall -USR1 systemd-journald
[root@ndbaranov ~]# journalctl -b
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud inst
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 fre
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000f0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000100000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000dffff0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000100000000-0x00000001
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
Sep 08 17:27:19 ndbaranov kernel: SMBIOS 2.5 present.
Sep 08 17:27:19 ndbaranov kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS
Sep 08 17:27:19 ndbaranov kernel: Hypervisor detected: KVM
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Sep 08 17:27:19 ndbaranov kernel: kvm-clock: using sched offset of 8803561305
Sep 08 17:27:19 ndbaranov kernel: clocksource: kvm-clock: mask: 0xffffffffffff
Sep 08 17:27:19 ndbaranov kernel: tsc: Detected 3593.376 Mhz processor
lines 1-23 ...skipping...
Sep 08 17:27:19 ndbaranov kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro
skylin
Sep 08 17:27:19 ndbaranov kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be vi
ewed ab
Sep 08 17:27:19 ndbaranov kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/de
v/mapp
Sep 08 17:27:19 ndbaranov kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Sep 08 17:27:19 ndbaranov kernel: BIOS-provided physical RAM map:
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x000000000000100000-0x000000000dffff0000] usable
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dffff0000] ACPI data
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000ffff0000] reserved
Sep 08 17:27:19 ndbaranov kernel: BIOS-e820: [mem 0x0000000100000000-0x0000000100000000] usable
Sep 08 17:27:19 ndbaranov kernel: NX (Execute Disable) protection: active
Sep 08 17:27:19 ndbaranov kernel: APIC: Static calls initialized
```

Получены навыки работы с системными журналами ОС Linux.
Настроена регистрация сообщений Apache через syslog, добавлены правила для отладки, изучена работа journalctl и journald.
Реализовано постоянное хранение журналов в /var/log/journal.