

Лабораторная работа №7

Управление журналами событий в системе

Комягин А. Н.

09 октября 2024

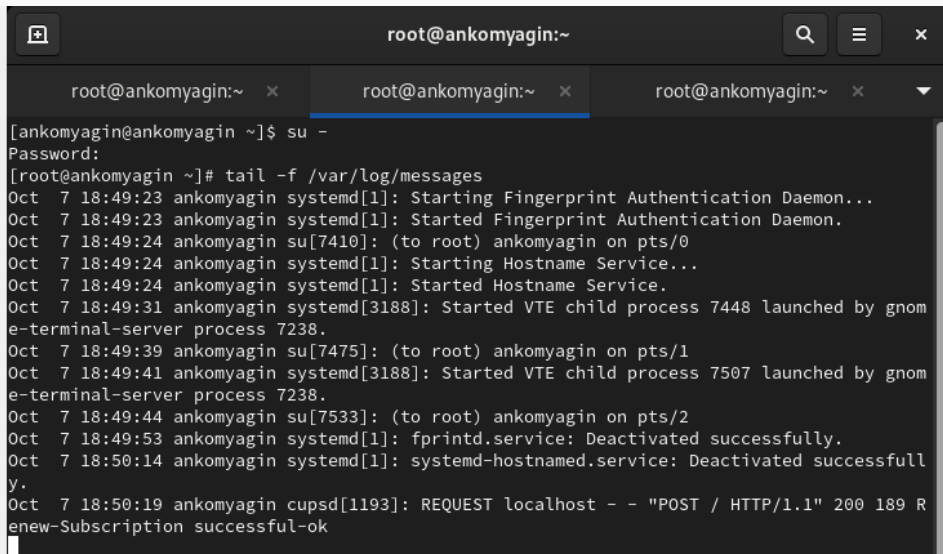
Российский университет дружбы народов, Москва, Россия

Получить навыки работы с журналами мониторинга различных событий в системе.

Выполнение лабораторной работы

Мониторинг журнала системных событий в реальном времени

Запустим мониторинг событий

A terminal window titled 'root@ankomyagin:~' with three tabs. The active tab shows the command 'tail -f /var/log/messages' being executed. The output displays various system events, including the start of the Fingerprint Authentication Daemon, Hostname Service, and VTE child processes, as well as the deactivation of fprintd.service and systemd-hostnamed.service.

```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# tail -f /var/log/messages  
Oct  7 18:49:23 ankomyagin systemd[1]: Starting Fingerprint Authentication Daemon...  
Oct  7 18:49:23 ankomyagin systemd[1]: Started Fingerprint Authentication Daemon.  
Oct  7 18:49:24 ankomyagin su[7410]: (to root) ankomyagin on pts/0  
Oct  7 18:49:24 ankomyagin systemd[1]: Starting Hostname Service...  
Oct  7 18:49:24 ankomyagin systemd[1]: Started Hostname Service.  
Oct  7 18:49:31 ankomyagin systemd[3188]: Started VTE child process 7448 launched by gnom  
e-terminal-server process 7238.  
Oct  7 18:49:39 ankomyagin su[7475]: (to root) ankomyagin on pts/1  
Oct  7 18:49:41 ankomyagin systemd[3188]: Started VTE child process 7507 launched by gnom  
e-terminal-server process 7238.  
Oct  7 18:49:44 ankomyagin su[7533]: (to root) ankomyagin on pts/2  
Oct  7 18:49:53 ankomyagin systemd[1]: fprintd.service: Deactivated successfully.  
Oct  7 18:50:14 ankomyagin systemd[1]: systemd-hostnamed.service: Deactivated successfull  
y.  
Oct  7 18:50:19 ankomyagin cupsd[1193]: REQUEST localhost - - "POST / HTTP/1.1" 200 189 R  
enew-Subscription successful-ok
```

отображение ошибки в мониторинге

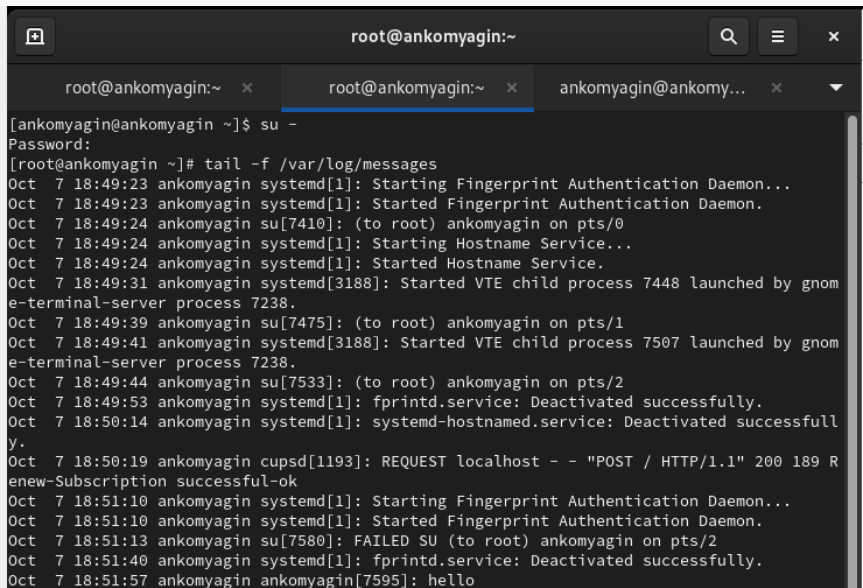
```
renew-subscription success:rc=0k
```

```
Oct  7 18:51:10 ankomyagin systemd[1]: Starting Fingerprint Authentication Daemon...
```

```
Oct  7 18:51:10 ankomyagin systemd[1]: Started Fingerprint Authentication Daemon.
```

```
Oct  7 18:51:13 ankomyagin su[7580]: FAILED SU (to root) ankomyagin on pts/2
```

logger hello



A terminal window titled "root@ankomyagin:~" with a search icon, a menu icon, and a close icon in the top right. The window has three tabs: "root@ankomyagin:~", "root@ankomyagin:~", and "ankomyagin@ankomy...". The active tab is the second "root@ankomyagin:~". The terminal shows a sequence of commands and system log messages. The user switches to root using "su -", then runs "tail -f /var/log/messages". The log output shows various system events, including the starting and deactivating of services like Fingerprint Authentication Daemon, Hostname Service, and cupsd, as well as user login attempts and a successful login.

```
[ankomyagin@ankomyagin ~]$ su -
Password:
[root@ankomyagin ~]# tail -f /var/log/messages
Oct  7 18:49:23 ankomyagin systemd[1]: Starting Fingerprint Authentication Daemon...
Oct  7 18:49:23 ankomyagin systemd[1]: Started Fingerprint Authentication Daemon.
Oct  7 18:49:24 ankomyagin su[7410]: (to root) ankomyagin on pts/0
Oct  7 18:49:24 ankomyagin systemd[1]: Starting Hostname Service...
Oct  7 18:49:24 ankomyagin systemd[1]: Started Hostname Service.
Oct  7 18:49:31 ankomyagin systemd[3188]: Started VTE child process 7448 launched by gnom
e-terminal-server process 7238.
Oct  7 18:49:39 ankomyagin su[7475]: (to root) ankomyagin on pts/1
Oct  7 18:49:41 ankomyagin systemd[3188]: Started VTE child process 7507 launched by gnom
e-terminal-server process 7238.
Oct  7 18:49:44 ankomyagin su[7533]: (to root) ankomyagin on pts/2
Oct  7 18:49:53 ankomyagin systemd[1]: fprintd.service: Deactivated successfully.
Oct  7 18:50:14 ankomyagin systemd[1]: systemd-hostnamed.service: Deactivated successfull
y.
Oct  7 18:50:19 ankomyagin cupsd[1193]: REQUEST localhost - - "POST / HTTP/1.1" 200 189 R
enew-Subscription successful-ok
Oct  7 18:51:10 ankomyagin systemd[1]: Starting Fingerprint Authentication Daemon...
Oct  7 18:51:10 ankomyagin systemd[1]: Started Fingerprint Authentication Daemon.
Oct  7 18:51:13 ankomyagin su[7580]: FAILED SU (to root) ankomyagin on pts/2
Oct  7 18:51:40 ankomyagin systemd[1]: fprintd.service: Deactivated successfully.
Oct  7 18:51:57 ankomyagin ankomyagin[7595]: hello
```

мониторинг сообщений безопасности

```
[root@ankomyagin ~]# tail -n 20 /var/log/secure
Oct  7 17:51:57 ankomyagin gdm-password[3168]: gkr-pam: unable to locate daemon control file
Oct  7 17:51:57 ankomyagin gdm-password[3168]: gkr-pam: stashed password to try later in open session
Oct  7 17:51:57 ankomyagin systemd[3188]: pam_unix(systemd-user:session): session opened for user ankomyagin(uid=1000) by ankomyagin(uid=0)
Oct  7 17:51:57 ankomyagin gdm-password[3168]: pam_unix(gdm-password:session): session opened for user ankomyagin(uid=1000) by ankomyagin(uid=0)
Oct  7 17:51:57 ankomyagin gdm-password[3168]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct  7 17:51:58 ankomyagin polkitd[787]: Registered Authentication Agent for unix-session:2 (system bus name :1.70 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct  7 17:51:59 ankomyagin gdm-launch-environment[2712]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct  7 17:51:59 ankomyagin polkitd[787]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.25, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct  7 18:00:57 ankomyagin su[5218]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:11:47 ankomyagin su[5218]: pam_unix(su-l:session): session closed for user root
Oct  7 18:15:00 ankomyagin su[5565]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:35:49 ankomyagin su[5565]: pam_unix(su-l:session): session closed for user root
Oct  7 18:35:53 ankomyagin su[7071]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:43:45 ankomyagin su[7071]: pam_unix(su-l:session): session closed for user root
Oct  7 18:49:24 ankomyagin su[7410]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:49:39 ankomyagin su[7475]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:49:44 ankomyagin su[7533]: pam_unix(su-l:session): session opened for user root(uid=0) by ankomyagin(uid=1000)
Oct  7 18:51:07 ankomyagin su[7533]: pam_unix(su-l:session): session closed for user root
Oct  7 18:51:11 ankomyagin unix_chkpwd[7587]: password check failed for user (root)
Oct  7 18:51:11 ankomyagin su[7580]: pam_unix(su-l:auth): authentication failure; logname=ankomyagin uid=1000 euid=0 tty=/dev/pts/2 ruser=ankomyagin rhost= user=root
[root@ankomyagin ~]#
```


Установка Арасче и запуск веб-службы

```
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-bdb-1.6.1-23.el9.x86_64 2/11
  Installing     : apr-util-1.6.1-23.el9.x86_64    3/11
  Installing     : apr-util-openssl-1.6.1-23.el9.x86_64 4/11
  Installing     : httpd-tools-2.4.57-11.el9_4.1.x86_64 5/11
Running scriptlet: httpd-filesystem-2.4.57-11.el9_4.1.noarch 6/11
  Installing     : httpd-filesystem-2.4.57-11.el9_4.1.noarch 6/11
  Installing     : httpd-core-2.4.57-11.el9_4.1.x86_64 7/11
  Installing     : mod_lua-2.4.57-11.el9_4.1.x86_64 8/11
  Installing     : rocky-logos-httpd-90.15-2.el9.noarch 9/11
  Installing     : mod_http2-2.0.26-2.el9_4.x86_64 10/11
  Installing     : httpd-2.4.57-11.el9_4.1.x86_64 11/11
Running scriptlet: httpd-2.4.57-11.el9_4.1.x86_64 11/11
  Verifying      : rocky-logos-httpd-90.15-2.el9.noarch 1/11
  Verifying      : mod_lua-2.4.57-11.el9_4.1.x86_64 2/11
  Verifying      : httpd-tools-2.4.57-11.el9_4.1.x86_64 3/11
  Verifying      : httpd-2.4.57-11.el9_4.1.x86_64 4/11
  Verifying      : httpd-filesystem-2.4.57-11.el9_4.1.noarch 5/11
  Verifying      : apr-util-openssl-1.6.1-23.el9.x86_64 6/11
  Verifying      : apr-util-bdb-1.6.1-23.el9.x86_64 7/11
  Verifying      : apr-util-1.6.1-23.el9.x86_64 8/11
  Verifying      : mod_http2-2.0.26-2.el9_4.x86_64 9/11
  Verifying      : apr-1.7.0-12.el9_3.x86_64 10/11
  Verifying      : httpd-core-2.4.57-11.el9_4.1.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-2.4.57-11.el9_4.1.x86_64    httpd-core-2.4.57-11.el9_4.1.x86_64
httpd-filesystem-2.4.57-11.el9_4.1.noarch httpd-tools-2.4.57-11.el9_4.1.x86_64
mod_http2-2.0.26-2.el9_4.x86_64   mod_lua-2.4.57-11.el9_4.1.x86_64
rocky-logos-httpd-90.15-2.el9.noarch
```

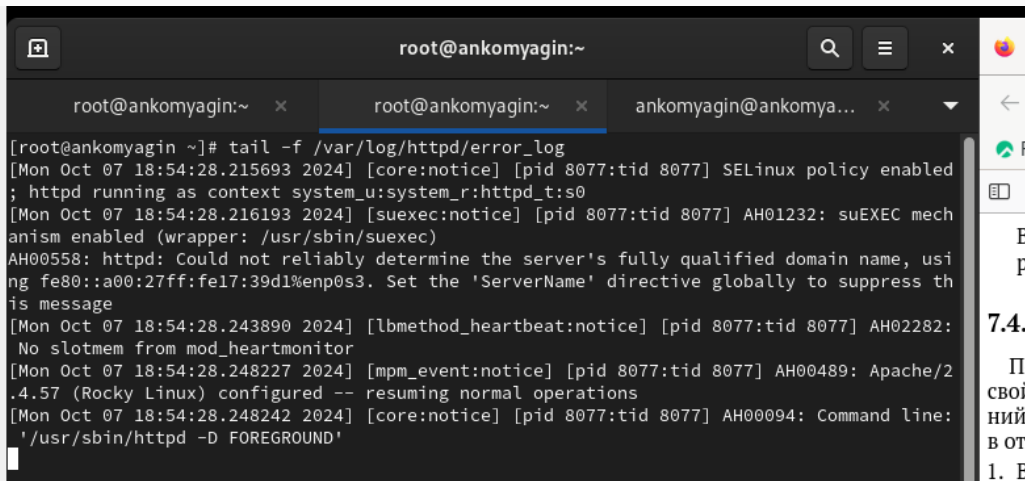
Complete!

```
[root@ankomyagin ~]# systemctl start httpd
```

```
[root@ankomyagin ~]# systemctl enable httpd
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
```

```
[root@ankomyagin ~]#
```



A terminal window titled 'root@ankomyagin:~' with three tabs. The active tab shows the command 'tail -f /var/log/httpd/error_log' and its output. The output contains several log entries, including SELinux policy enabled, suEXEC mechanism enabled, a warning about domain name determination, and Apache/2.4.57 (Rocky Linux) resuming normal operations. The terminal window has a dark theme and standard window controls.

```
root@ankomyagin:~  
[root@ankomyagin ~]# tail -f /var/log/httpd/error_log  
[Mon Oct 07 18:54:28.215693 2024] [core:notice] [pid 8077:tid 8077] SELinux policy enabled  
; httpd running as context system_u:system_r:httpd_t:s0  
[Mon Oct 07 18:54:28.216193 2024] [suexec:notice] [pid 8077:tid 8077] AH01232: suEXEC mech  
anism enabled (wrapper: /usr/sbin/suexec)  
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, usi  
ng fe80::a00:27ff:fe17:39d1%enp0s3. Set the 'ServerName' directive globally to suppress th  
is message  
[Mon Oct 07 18:54:28.243890 2024] [lbmethod_heartbeat:notice] [pid 8077:tid 8077] AH02282:  
No slotmem from mod_heartbeat  
[Mon Oct 07 18:54:28.248227 2024] [mpm_event:notice] [pid 8077:tid 8077] AH00489: Apache/2  
.4.57 (Rocky Linux) configured -- resuming normal operations  
[Mon Oct 07 18:54:28.248242 2024] [core:notice] [pid 8077:tid 8077] AH00094: Command line:  
'/usr/sbin/httpd -D FOREGROUND'
```

```
/etc/httpd/conf/httpd.conf
```

```

root@ankomyagin:~
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf

#
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>

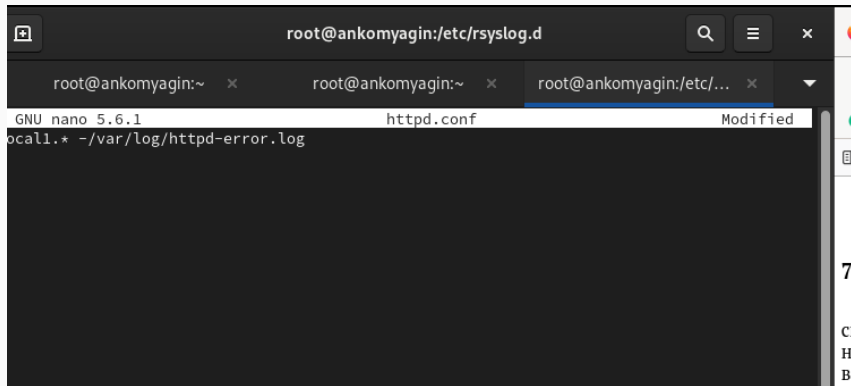
#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html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

#
# 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 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:local

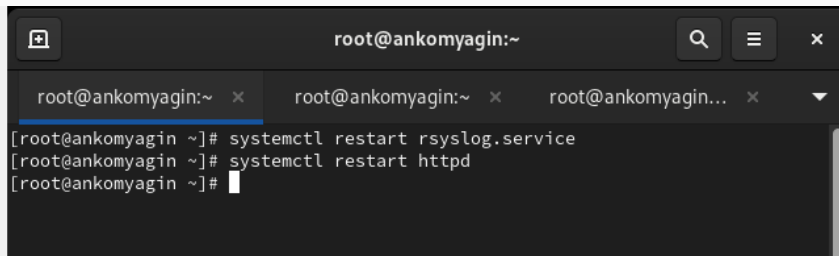

```



The screenshot shows a terminal window with a dark background. At the top, the title bar reads "root@ankomyagin:/etc/rsyslog.d". Below the title bar, there are three tabs: "root@ankomyagin:~", "root@ankomyagin:~", and "root@ankomyagin:/etc/...". The active tab is "root@ankomyagin:/etc/...". The terminal content shows the GNU nano 5.6.1 editor editing the file "httpd.conf". The first line of the file is "local.* -/var/log/httpd-error.log". The status bar at the bottom of the editor shows "Modified".

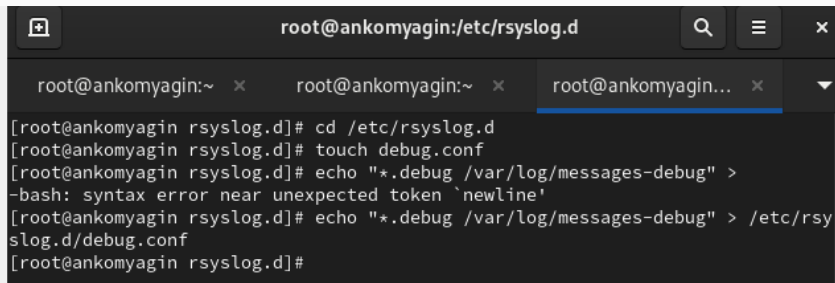
```
root@ankomyagin:/etc/rsyslog.d
root@ankomyagin:~ x root@ankomyagin:~ x root@ankomyagin:/etc/... x
GNU nano 5.6.1 httpd.conf Modified
local.* -/var/log/httpd-error.log
```

перезагрузка конфигураций



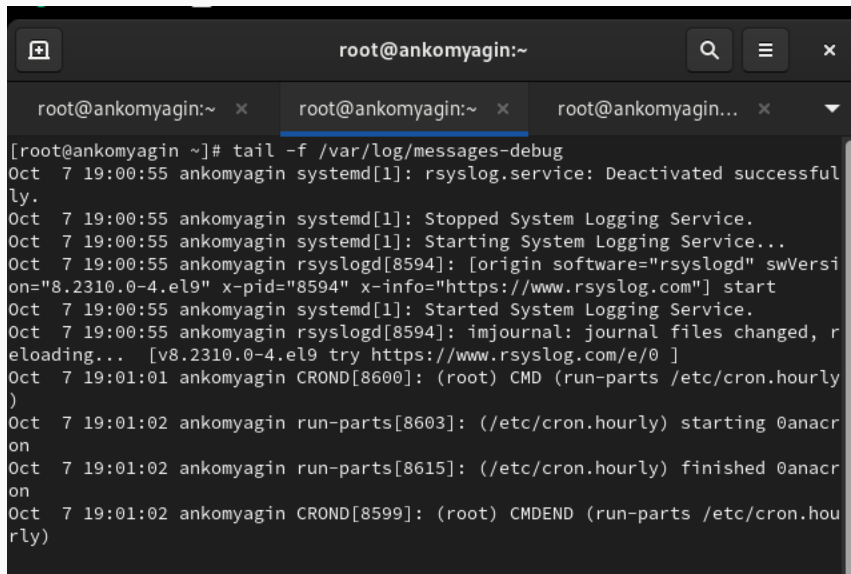
A terminal window titled 'root@ankomyagin:~' with search, menu, and close buttons. It contains three tabs, all labeled 'root@ankomyagin:~'. The active tab shows the following commands and prompts:

```
[root@ankomyagin ~]# systemctl restart rsyslog.service
[root@ankomyagin ~]# systemctl restart httpd
[root@ankomyagin ~]#
```



```
root@ankomyagin:/etc/rsyslog.d

root@ankomyagin:~ x root@ankomyagin:~ x root@ankomyagin... x ▼
[root@ankomyagin rsyslog.d]# cd /etc/rsyslog.d
[root@ankomyagin rsyslog.d]# touch debug.conf
[root@ankomyagin rsyslog.d]# echo "*.debug /var/log/messages-debug" >
-bash: syntax error near unexpected token `newline'
[root@ankomyagin rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@ankomyagin rsyslog.d]#
```

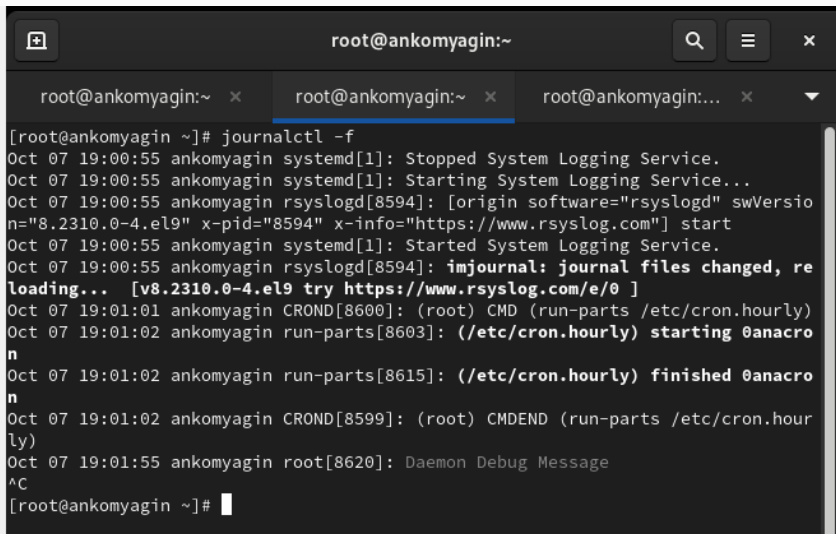
A terminal window titled 'root@ankomyagin:~' with a search icon, a menu icon, and a close icon in the top right. Below the title bar are three tabs, all labeled 'root@ankomyagin:~', with the middle one selected. The terminal content shows the execution of 'tail -f /var/log/messages-debug' and subsequent log messages from 'systemd' and 'rsyslogd' regarding the deactivation and restart of the System Logging Service, followed by cron jobs running 'anacron'.

Использование journalctl

содержимое журнала событий

```
Oct 07 17:10:41 ankomyagin kernel: Linux version 5.14.0-427.35.1.el9_4.x86_64 (mockbuild@iadi-prod-build001.bld.equ.rocks)
Oct 07 17:10:41 ankomyagin kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at https://access.redhat.com/articles/6842461
Oct 07 17:10:41 ankomyagin kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.35.1.el9_4.x86_64 root=/dev/vda1
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' fpu save/restore mode
Oct 07 17:10:41 ankomyagin kernel: signal: max sigframe size: 1776
Oct 07 17:10:41 ankomyagin kernel: BIOS-provided physical RAM map:
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000000100000-0x00000000000dfffff] usable
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x000000000dfff0000-0x000000000dffffff] ACPI data
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffff] usable
Oct 07 17:10:41 ankomyagin kernel: NX (Execute Disable) protection: active
Oct 07 17:10:41 ankomyagin kernel: SMBIOS 2.5 present.
Oct 07 17:10:41 ankomyagin kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 07 17:10:41 ankomyagin kernel: Hypervisor detected: KVM
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: Using mrs 4b564d01 and 4b564d00
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: using sched offset of 8561155907 cycles
Oct 07 17:10:41 ankomyagin kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_cycles: 0x1cd42e4dffb
Oct 07 17:10:41 ankomyagin kernel: tsc: Detected 2687.996 MHz processor
Oct 07 17:10:41 ankomyagin kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 07 17:10:41 ankomyagin kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Oct 07 17:10:41 ankomyagin kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 07 17:10:41 ankomyagin kernel: MTRRs disabled by BIOS
Oct 07 17:10:41 ankomyagin kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Oct 07 17:10:41 ankomyagin kernel: last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
Oct 07 17:10:41 ankomyagin kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
Oct 07 17:10:41 ankomyagin kernel: Incomplete global flushes, disabling PCID
Oct 07 17:10:41 ankomyagin kernel: RAMDISK: [mem 0x3143d000-0x34a16fff]
Oct 07 17:10:41 ankomyagin kernel: ACPI: Early table checksum verification disabled
Oct 07 17:10:41 ankomyagin kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
Oct 07 17:10:41 ankomyagin kernel: ACPI: XSDT 0x0000000000000000 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
Oct 07 17:10:41 ankomyagin kernel: ACPI: FACP 0x00000000000000F0 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
Oct 07 17:10:41 ankomyagin kernel: ACPI: DSDT 0x0000000000000020 002353 (v02 VBOX VBOXBIOS 00000002 INTL 20100528)
Oct 07 17:10:41 ankomyagin kernel: ACPI: FACS 0x0000000000000000 000040
Oct 07 17:10:41 ankomyagin kernel: ACPI: FACS 0x0000000000000000 000040
Oct 07 17:10:41 ankomyagin kernel: ACPI: APIC 0x0000000000000020 00006C (v02 VBOX VBOXAPIC 00000001 ASL 00000061)
```

lines 1-44



```
root@ankomyagin:~  
[root@ankomyagin ~]# journalctl -f  
Oct 07 19:00:55 ankomyagin systemd[1]: Stopped System Logging Service.  
Oct 07 19:00:55 ankomyagin systemd[1]: Starting System Logging Service...  
Oct 07 19:00:55 ankomyagin rsyslogd[8594]: [origin software="rsyslogd" swVersio  
n="8.2310.0-4.el9" x-pid="8594" x-info="https://www.rsyslog.com"] start  
Oct 07 19:00:55 ankomyagin systemd[1]: Started System Logging Service.  
Oct 07 19:00:55 ankomyagin rsyslogd[8594]: imjournal: journal files changed, re  
loading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]  
Oct 07 19:01:01 ankomyagin CROND[8600]: (root) CMD (run-parts /etc/cron.hourly)  
Oct 07 19:01:02 ankomyagin run-parts[8603]: (/etc/cron.hourly) starting 0anacro  
n  
Oct 07 19:01:02 ankomyagin run-parts[8615]: (/etc/cron.hourly) finished 0anacro  
n  
Oct 07 19:01:02 ankomyagin CROND[8599]: (root) CMDEND (run-parts /etc/cron.hour  
ly)  
Oct 07 19:01:55 ankomyagin root[8620]: Daemon Debug Message  
^C  
[root@ankomyagin ~]#
```

последние строки журнала

```
root@ankomyagin:~  
[root@ankomyagin ~]# journalctl -n 20  
Oct 07 18:59:03 ankomyagin systemd[1]: Stopped The Apache HTTP Server.  
Oct 07 18:59:03 ankomyagin systemd[1]: Starting The Apache HTTP Server...  
Oct 07 18:59:03 ankomyagin httpd[8386]: AH00558: httpd: Could not reliably det>  
Oct 07 18:59:03 ankomyagin httpd[8386]: Server configured, listening on: port >  
Oct 07 18:59:03 ankomyagin systemd[1]: Started The Apache HTTP Server.  
Oct 07 18:59:30 ankomyagin PackageKit[8069]: daemon quit  
Oct 07 18:59:30 ankomyagin systemd[1]: packagekit.service: Deactivated success>  
Oct 07 19:00:54 ankomyagin systemd[1]: Stopping System Logging Service...  
Oct 07 19:00:55 ankomyagin rsyslogd[8375]: [origin software="rsyslogd" swVersi>  
Oct 07 19:00:55 ankomyagin systemd[1]: rsyslog.service: Deactivated successfu>  
Oct 07 19:00:55 ankomyagin systemd[1]: Stopped System Logging Service.  
Oct 07 19:00:55 ankomyagin systemd[1]: Starting System Logging Service...  
Oct 07 19:00:55 ankomyagin rsyslogd[8594]: [origin software="rsyslogd" swVersi>  
Oct 07 19:00:55 ankomyagin systemd[1]: Started System Logging Service.  
Oct 07 19:00:55 ankomyagin rsyslogd[8594]: imjournal: journal files changed, r>  
Oct 07 19:01:01 ankomyagin CROND[8600]: (root) CMD (run-parts /etc/cron.hourly)  
Oct 07 19:01:02 ankomyagin run-parts[8603]: (/etc/cron.hourly) starting 0anacr>  
Oct 07 19:01:02 ankomyagin run-parts[8615]: (/etc/cron.hourly) finished 0anacr>  
Oct 07 19:01:02 ankomyagin CROND[8599]: (root) CMDEND (run-parts /etc/cron.hou>  
Oct 07 19:01:55 ankomyagin root[8620]: Daemon Debug Message  
lines 1-20/20 (END)
```

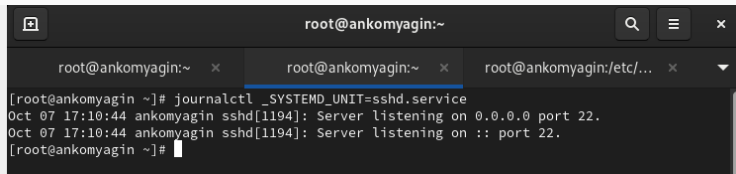
сообщения об ошибках

```
root@ankomyagin:~  
[root@ankomyagin ~]# journalctl -p err  
Oct 07 17:10:41 ankomyagin systemd[1]: Invalid DMI field header.  
Oct 07 17:10:41 ankomyagin kernel: Warning: Unmaintained driver is detected: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx 0000:00:02.0: [drm] *ERROR* This component is unmaintained. Please report bugs to https://bugzilla.kernel.org/show_bug.cgi?id=198882.  
Oct 07 17:10:43 ankomyagin systemd[1]: Invalid DMI field header.  
Oct 07 17:10:44 ankomyagin alsactl[822]: alsa-lib main.c:1554:(snd_use_case_map) warning: Unmaintained driver is detected: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx 0000:00:02.0: [drm] *ERROR* This component is unmaintained. Please report bugs to https://bugzilla.kernel.org/show_bug.cgi?id=198882.  
Oct 07 17:10:56 ankomyagin systemd[1]: Failed to start vboxadd.service.  
Oct 07 17:10:56 ankomyagin systemd[1]: Failed to start vboxadd-service.service.  
Oct 07 17:51:57 ankomyagin gdm-password[3168]: gkr-pam: unable to locate daemon helper  
Oct 07 17:51:59 ankomyagin gdm-wayland-session[2732]: GLib: Source ID 2 was not found when attempting to remove a message  
Oct 07 17:51:59 ankomyagin gdm-launch-environment[2712]: GLib-GObject: G_OBJECT() is deprecated. Use g_object_ref() instead.  
[root@ankomyagin ~]# journalctl --since yesterday  
Oct 07 17:10:41 ankomyagin kernel: Linux version 5.14.0-427.35.1.el9_4.x86_64 (root@tk1) (gcc version 9.3.0 (Red Hat 9.3.0-2)) #1 SMP Tue Aug 14 22:03:11 UTC 2024  
Oct 07 17:10:41 ankomyagin kernel: The list of certified hardware and cloud images can be found at https://www.redhat.com/en/tech-tips-by-topic/certified-hardware  
Oct 07 17:10:41 ankomyagin kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x001: 'XSAVE' (disabled)  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x002: 'XCR0' (disabled)  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x004: 'XCR2' (disabled)  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: xstate_offset[2]: 576, xstate_size[2]: 128, xstate_offset[3]: 0, xstate_size[3]: 0  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Enabled xstate features 0x7, context offset is 0, maximum enabled xstate feature value is 7  
Oct 07 17:10:41 ankomyagin kernel: signal: max sigframe size: 1776  
Oct 07 17:10:41 ankomyagin kernel: BIOS-provided physical RAM map:  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] type 2  
Oct 07 17:10:41 ankomyagin kernel: NX (Execute Disable) protection: active  
Oct 07 17:10:41 ankomyagin kernel: SMBIOS 2.5 present.  
Oct 07 17:10:41 ankomyagin kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS 1.0  
Oct 07 17:10:41 ankomyagin kernel: Hypervisor detected: KVM  
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: using sched offset of 8561155907ns  
Oct 07 17:10:41 ankomyagin kernel: clocksource: kvm-clock: mask: 0xffffffffffff  
Oct 07 17:10:41 ankomyagin kernel: tsc: Detected 2687.996 MHz processor  
Oct 07 17:10:41 ankomyagin kernel: e820: update [mem 0x00000000-0x00000fff] usable  
Oct 07 17:10:41 ankomyagin kernel: e820: remove [mem 0x00000000-0x00000fff] usable
```

сообщения со вчерашнего дня

```
root@ankomyagin:~  
root@ankomyagin:~ x root@ankomyagin:/etc/... x  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
PRIORITY=5  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
MESSAGE=Linux version 5.14.0-427.35.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.e  
_BOOT_ID=477d6db0574947c6bc8f460474ec2368  
_MACHINE_ID=4ba93f35e9cf455cadf6df9e21001a8d  
_HOSTNAME=ankomyagin  
_RUNTIME_SCOPE=initrd  
Mon 2024-10-07 17:10:41.117620 MSK [s=e6a59bd21ceb4ca4bfeedb695bda3277;i=2;b=477d6db057494  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
PRIORITY=5  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=477d6db0574947c6bc8f460474ec2368  
_MACHINE_ID=4ba93f35e9cf455cadf6df9e21001a8d  
_HOSTNAME=ankomyagin  
_RUNTIME_SCOPE=initrd  
MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can  
Mon 2024-10-07 17:10:41.117626 MSK [s=e6a59bd21ceb4ca4bfeedb695bda3277;i=3;b=477d6db057494  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=477d6db0574947c6bc8f460474ec2368  
_MACHINE_ID=4ba93f35e9cf455cadf6df9e21001a8d  
_HOSTNAME=ankomyagin  
_RUNTIME_SCOPE=initrd  
PRIORITY=6  
MESSAGE=Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.35.1.el9_4.x86_64 roo  
Mon 2024-10-07 17:10:41.117629 MSK [s=e6a59bd21ceb4ca4bfeedb695bda3277;i=4;b=477d6db057494  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=477d6db0574947c6bc8f460474ec2368  
_MACHINE_ID=4ba93f35e9cf455cadf6df9e21001a8d  
_HOSTNAME=ankomyagin  
_RUNTIME_SCOPE=initrd  
PRIORITY=6
```

доп информация о sshd



A terminal window titled 'root@ankomyagin:~' with search, menu, and close icons. It shows three tabs: 'root@ankomyagin:~', 'root@ankomyagin:~' (selected), and 'root@ankomyagin:/etc/...'. The terminal output shows the command 'journalctl _SYSTEMD_UNIT=sshd.service' and its results: 'Oct 07 17:10:44 ankomyagin sshd[1194]: Server listening on 0.0.0.0 port 22.' and 'Oct 07 17:10:44 ankomyagin sshd[1194]: Server listening on :: port 22.'

```
[root@ankomyagin ~]# journalctl _SYSTEMD_UNIT=sshd.service
Oct 07 17:10:44 ankomyagin sshd[1194]: Server listening on 0.0.0.0 port 22.
Oct 07 17:10:44 ankomyagin sshd[1194]: Server listening on :: port 22.
[root@ankomyagin ~]#
```

Постоянный журнал journald

доп информация о sshd

```
root@ankomyagin:~  
root@ankomyagin:~ x root@ankomyagin:~ x root@ankomyagin:/etc/... x  
[root@ankomyagin ~]# mkdir -p /var/log/journal  
[root@ankomyagin ~]# chown root:systemd-journal /var/log/journal  
[root@ankomyagin ~]# chmod 2755 /var/log/journal  
[root@ankomyagin ~]# killall -USR1 systemd-journald  
[root@ankomyagin ~]# journalctl -b  
Oct 07 17:10:41 ankomyagin kernel: Linux version 5.14.0-427.35.1.el9_4.x86_64 (mockbuild@i>  
Oct 07 17:10:41 ankomyagin kernel: The list of certified hardware and cloud instances for >  
Oct 07 17:10:41 ankomyagin kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-42>  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating >  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'>  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'>  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256 >  
Oct 07 17:10:41 ankomyagin kernel: x86/fpu: Enabled xstate features 0x7, context size is 8>  
Oct 07 17:10:41 ankomyagin kernel: signal: max sigframe size: 1776  
Oct 07 17:10:41 ankomyagin kernel: BIOS-provided physical RAM map:  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000dffff000-0x0000000000dffffff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec00fff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fee00fff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x0000000000ffffff] >  
Oct 07 17:10:41 ankomyagin kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011ffffff] >  
Oct 07 17:10:41 ankomyagin kernel: NX (Execute Disable) protection: active  
Oct 07 17:10:41 ankomyagin kernel: SMBIOS 2.5 present.  
Oct 07 17:10:41 ankomyagin kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBo>  
Oct 07 17:10:41 ankomyagin kernel: Hypervisor detected: KVM  
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00  
Oct 07 17:10:41 ankomyagin kernel: kvm-clock: using sched offset of 8561155907 cycles  
Oct 07 17:10:41 ankomyagin kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cy>  
Oct 07 17:10:41 ankomyagin kernel: tsc: Detected 2687.996 MHz processor  
Oct 07 17:10:41 ankomyagin kernel: e820: update [mem 0x000000000-0x000000fff] usable ==> res>
```


Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

- Основной файл конфигурации для rsyslogd — это `/etc/rsyslog.conf`.

2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?

- Сообщения, связанные с аутентификацией, обычно записываются в файл `/var/log/auth.log` (или `/var/log/secure` в некоторых дистрибутивах).

3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?

- По умолчанию ротация файлов журналов происходит раз в неделю (это может варьироваться в зависимости от конфигурации системы и используемого инструмента ротации, например, `logrotate`).

4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом `info` в файл `/var/log/messages.info`?

- Добавим строку: `*.info /var/log/messages.info`.

5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?

- Команда `tail -f /var/log/syslog` (или другой соответствующий файл журнала).

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?

- Используем команду: `journalctl _PID=1 -since "YYYY-MM-DD 09:00" -until "YYYY-MM-DD 15:00"` (замените YYYY-MM-DD на нужную дату).

7. Какая команда позволяет вам видеть сообщения `journald` после последней перезагрузки системы?

- Команда: `journalctl -b`.

8. Какая процедура позволяет сделать журнал `journald` постоянным?

- Чтобы сделать журнал `journald` постоянным, нужно отредактировать файл конфигурации `/etc/systemd/journald.conf` и установить параметр `Storage=persistent`. Затем перезапустите службу `journald` с помощью команды `systemctl restart systemd-journald`.

Вывод

В ходе выполнения лабораторной работы я получил навыки работы с журналами мониторинга различных событий в системе.