

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №7**

*дисциплина: Основы администрирования операционных систем*

Студент: Хамди Мохаммад, 1032235868

**МОСКВА**

**2024 г.**

## Постановка задачи

Получить навыки работы с журналами мониторинга различных событий в системе.

## Выполнение работы

### Мониторинг журнала системных событий в реальном времени

1. Запустите три вкладки терминала и в каждом из них получите полномочия администратора: su -
2. На второй вкладке терминала запустите мониторинг системных событий в реальном времени: tail -f /var/log/messages

```
[root@hamdimohammad hmohammad]# tail -f /var/log/messages
Oct 10 10:27:48 hamdimohammad PackageKit[1398]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Oct 10 10:27:48 hamdimohammad PackageKit[1398]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct 10 10:28:07 hamdimohammad systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 10 10:28:07 hamdimohammad systemd[1]: Started Fingerprint Authentication Daemon.
Oct 10 10:28:09 hamdimohammad su[2765]: (to root) hmohammad on pts/0
Oct 10 10:28:11 hamdimohammad systemd[1754]: Started VTE child process 2801 launched by gnome-terminal-serve
r process 2632.
Oct 10 10:28:14 hamdimohammad su[2827]: (to root) hmohammad on pts/1
Oct 10 10:28:16 hamdimohammad systemd[1754]: Started VTE child process 2858 launched by gnome-terminal-serve
r process 2632.
Oct 10 10:28:19 hamdimohammad su[2883]: (to root) hmohammad on pts/2
Oct 10 10:28:38 hamdimohammad systemd[1]: fprintd.service: Deactivated successfully.
```

3. В третьей вкладке терминала вернитесь к учётной записи своего пользователя достаточно нажать Ctrl + d ) и попробуйте получить полномочия администратора, но введите неправильный пароль. Обратите внимание, что во второй вкладке терминала с мониторингом событий или ничего не отобразится, или появится сообщение «FAILED SU (to root) username ...». Отображаемые на экране сообщения также фиксируются в файле /var/log/messages.

```
[hmohammad@hamdimohammad ~]$ su
Password:
[root@hamdimohammad hmohammad]#
exit
[hmohammad@hamdimohammad ~]$ su
Password:
su: Authentication failure
[hmohammad@hamdimohammad ~]$ logger hello
[hmohammad@hamdimohammad ~]$
```

4. В третьей вкладке терминала из оболочки пользователя введите `logger hello`  
Во второй вкладке терминала с мониторингом событий вы увидите сообщение, которое также будет зафиксировано в файле `/var/log/messages`.

```
[root@hamdimohammad hmohammad]# tail -f /var/log/messages
Oct 10 10:27:48 hamdimohammad PackageKit[1398]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Oct 10 10:27:48 hamdimohammad PackageKit[1398]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct 10 10:28:07 hamdimohammad systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 10 10:28:07 hamdimohammad systemd[1]: Started Fingerprint Authentication Daemon.
Oct 10 10:28:09 hamdimohammad su[2765]: (to root) hmohammad on pts/0
Oct 10 10:28:11 hamdimohammad systemd[1754]: Started VTE child process 2801 launched by gnome-terminal-server process 2632.
Oct 10 10:28:14 hamdimohammad su[2827]: (to root) hmohammad on pts/1
Oct 10 10:28:16 hamdimohammad systemd[1754]: Started VTE child process 2858 launched by gnome-terminal-server process 2632.
Oct 10 10:28:19 hamdimohammad su[2883]: (to root) hmohammad on pts/2
Oct 10 10:28:38 hamdimohammad systemd[1]: fprintd.service: Deactivated successfully.
Oct 10 10:29:13 hamdimohammad systemd[1754]: Starting Mark boot as successful...
Oct 10 10:29:13 hamdimohammad systemd[1754]: Finished Mark boot as successful.
Oct 10 10:30:21 hamdimohammad systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 10 10:30:21 hamdimohammad systemd[1]: Started Fingerprint Authentication Daemon.
Oct 10 10:30:25 hamdimohammad su[2936]: FAILED SU (to root) hmohammad on pts/2
Oct 10 10:30:31 hamdimohammad hmohammad[2948]: hello
```

5. Во второй вкладке терминала с мониторингом остановите трассировку файла сообщений мониторинга реального времени, используя `Ctrl + c`. Затем запустите мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов):

```
tail -n 20 /var/log/secure
```

Вы увидите сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды `su`.

```
[root@hamdimohammad hmohammad]# tail -n 20 /var/log/secure
Oct 10 10:23:51 hamdimohammad polkitd[823]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Oct 10 10:23:57 hamdimohammad sshd[1182]: Server listening on 0.0.0.0 port 22.
Oct 10 10:23:57 hamdimohammad sshd[1182]: Server listening on :: port 22.
Oct 10 10:23:58 hamdimohammad systemd[1219]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 10 10:24:00 hamdimohammad gdm-launch-environment[1214]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 10 10:24:16 hamdimohammad polkitd[823]: 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)
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: gkr-pam: unable to locate daemon control file
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: gkr-pam: stashed password to try later in open session
Oct 10 10:26:37 hamdimohammad systemd[1754]: pam_unix(systemd-user:session): session opened for user hmohammad(uid=1000) by hmohammad(uid=0)
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: pam_unix(gdm-password:session): session opened for user hmohammad(uid=1000) by hmohammad(uid=0)
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 10:26:41 hamdimohammad polkitd[823]: 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 10 10:26:46 hamdimohammad gdm-launch-environment[1214]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 10 10:26:46 hamdimohammad polkitd[823]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct 10 10:28:09 hamdimohammad su[2765]: pam_unix(su:session): session opened for user root(uid=0) by hmohammad(uid=1000)
Oct 10 10:28:15 hamdimohammad su[2827]: pam_unix(su:session): session opened for user root(uid=0) by hmohammad(uid=1000)
Oct 10 10:28:19 hamdimohammad su[2883]: pam_unix(su:session): session opened for user root(uid=0) by hmohammad(uid=1000)
Oct 10 10:30:19 hamdimohammad su[2883]: pam_unix(su:session): session closed for user root
Oct 10 10:30:23 hamdimohammad unix_chkpwd[2943]: password check failed for user (root)
Oct 10 10:30:23 hamdimohammad su[2936]: pam_unix(su:auth): authentication failure; logname=hmohammad uid=1000 euid=0 tty=/dev/pts/2 ruser=hmohammad rhost= user=root
[root@hamdimohammad hmohammad]#
```

## Изменение правил rsyslog.conf

По умолчанию веб-служба не регистрирует свои сообщения через rsyslog, а пишет свой собственный журнал (в каталоге /var/log/httpd). Настройте регистрацию сообщений веб-службы через syslog, создав правило, регистрирующее отладочные сообщения в отдельном лог-файле. Для этого выполните следующие действия.

1. В первой вкладке терминала установите Apache, если он не был ранее установлен:  
`dnf -y install httpd`

2. После окончания процесса установки запустите веб-службу:  
`systemctl start httpd`  
`systemctl enable httpd`

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

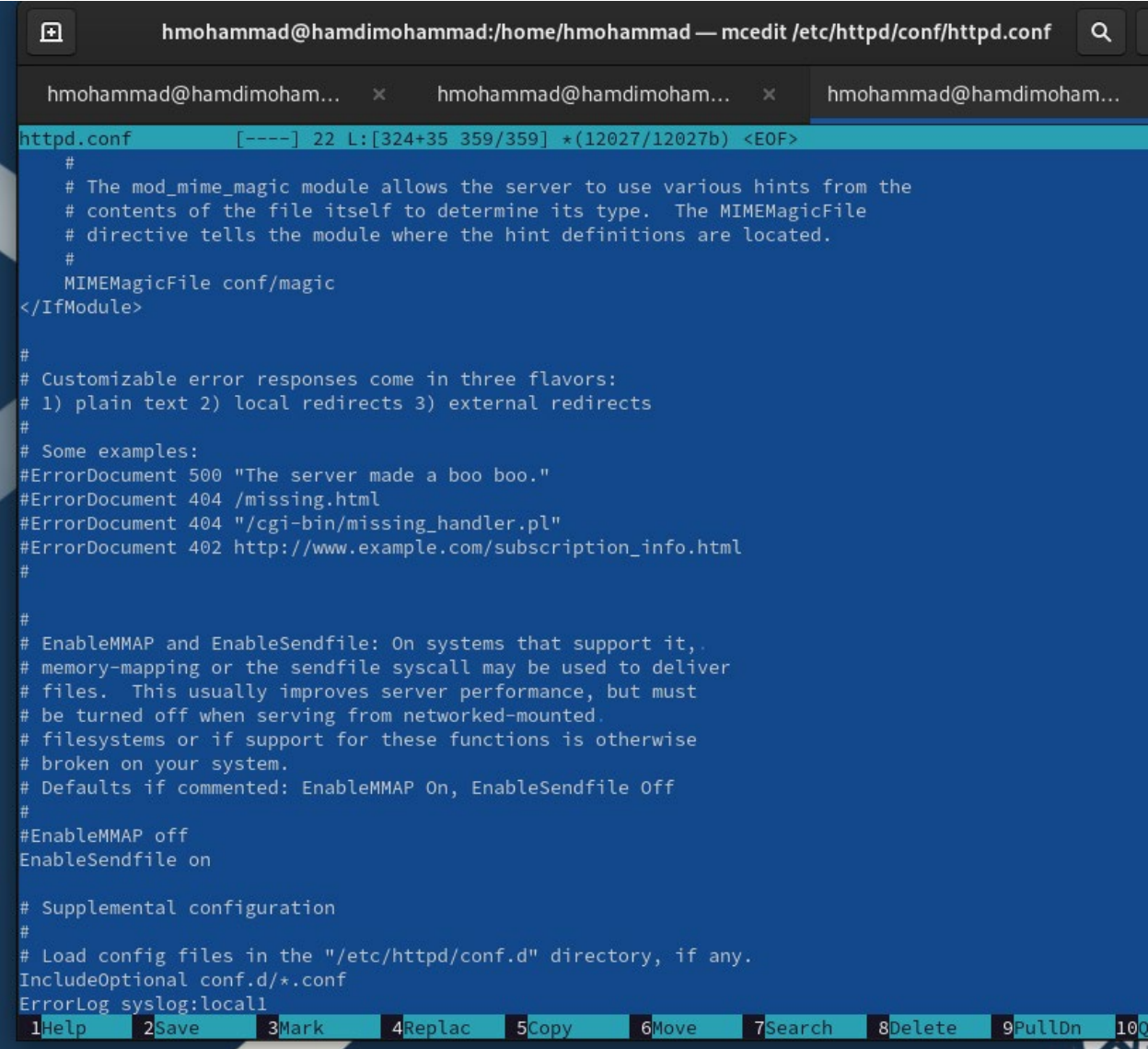
3. Во второй вкладке терминала посмотрите журнал сообщений об ошибках веб-службы:  
`tail -f /var/log/httpd/error_log`  
Чтобы закрыть трассировку файла журнала, используйте `Ctrl + c`.

```
[root@hamdimohammad hmohammad]#
[root@hamdimohammad hmohammad]# tail -f /var/log/httpd/error_log
[Thu Oct 10 10:36:00.406327 2024] [core:notice] [pid 9295:tid 9295] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 10 10:36:00.416200 2024] [suexec:notice] [pid 9295:tid 9295] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:feba:a06d%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Thu Oct 10 10:36:00.511210 2024] [lbmethod_heartbeat:notice] [pid 9295:tid 9295] AH02282: No slotmem from mod_heartbeat
[Thu Oct 10 10:36:00.518251 2024] [mpm_event:notice] [pid 9295:tid 9295] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Thu Oct 10 10:36:00.518315 2024] [core:notice] [pid 9295:tid 9295] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

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

`ErrorLog syslog:local1`

Здесь `local0` — `local7` — это «настраиваемые» средства (объекты), которые `syslog` предоставляет пользователю для регистрации событий приложения в системном журнале.



```
httpd.conf [----] 22 L:[324+35 359/359] *(12027/12027b) <EOF>
#
# 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:local1
```

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 100

5. В каталоге /etc/rsyslog.d создайте файл мониторинга событий веб-службы:

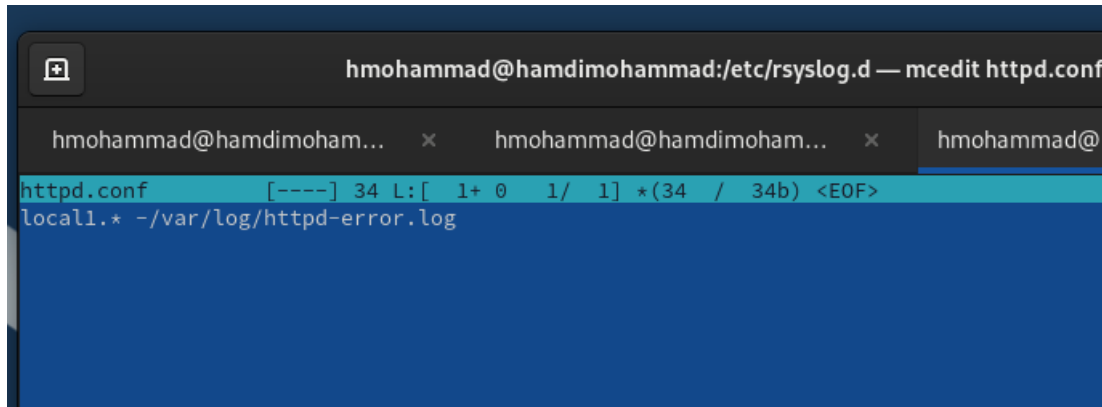
```
cd /etc/rsyslog.d
```

```
touch httpd.conf
```

Открыв его на редактирование, пропишите в нём

```
local1.* -/var/log/httpd-error.log
```

Эта строка позволит отправлять все сообщения, получаемые для объекта local1 (который теперь используется службой httpd), в файл /var/log/httpd-error.log.

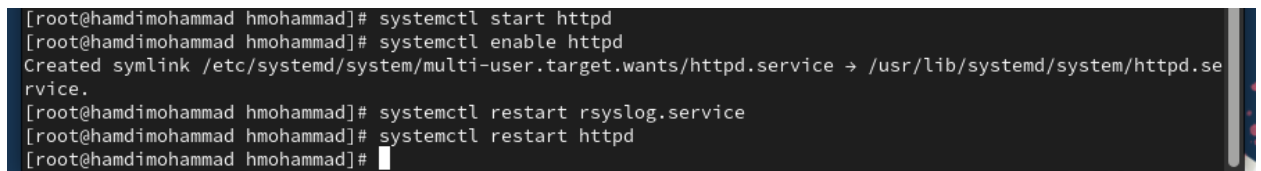


6. Перейдите в первую вкладку терминала и перезагрузите конфигурацию rsyslogd и веб-службу:

```
systemctl restart rsyslog.service
```

```
systemctl restart httpd
```

Все сообщения об ошибках веб-службы теперь будут записаны в файл /var/log/httpd-error.log, что можно наблюдать или в режиме реального времени, используя команду tail с соответствующими параметрами, или непосредственно просматривая указанный файл.





7. В третьей вкладке терминала создайте отдельный файл конфигурации для мониторинга отладочной информации:

```
cd /etc/rsyslog.d
```

```
touch debug.conf
```

В этом же терминале введите

```
echo "*.debug /var/log/messages-debug" >
```

```
/etc/rsyslog.d/debug.conf
```

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

8. В первой вкладке терминала снова перезапустите rsyslogd:

```
systemctl restart rsyslog.service
```

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

9. Во второй вкладке терминала запустите мониторинг отладочной информации:

```
tail -f /var/log/messages-debug
```

10. В третьей вкладке терминала введите:

```
logger -p daemon.debug "Daemon Debug Message"
```

```
[root@hamdimohammad rsyslog.d]# touch debug.conf  
[root@hamdimohammad rsyslog.d]# echo "*.debug /var/log/messages-debug" > debug.conf  
[root@hamdimohammad rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"  
[root@hamdimohammad rsyslog.d]#
```

11. В терминале с мониторингом посмотрите сообщение отладки. Чтобы закрыть трассировку файла журнала, используйте Ctrl + c .

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# tail -f /var/log/messages-debug  
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopping System Logging Service...  
Oct 10 10:42:08 hamdimohammad rsyslogd[42580]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42580" x-info="https://www.rsyslog.com"] exiting on signal 15.  
Oct 10 10:42:08 hamdimohammad systemd[1]: rsyslog.service: Deactivated successfully.  
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopped System Logging Service.  
Oct 10 10:42:08 hamdimohammad systemd[1]: Starting System Logging Service...  
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42803" x-info="https://www.rsyslog.com"] start  
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]  
Oct 10 10:42:08 hamdimohammad systemd[1]: Started System Logging Service.  
Oct 10 10:42:46 hamdimohammad root[42821]: Daemon Debug Message  
[root@hamdimohammad hmohammad]#
```



## Использование journalctl

1. Во второй вкладке терминала посмотрите содержимое журнала с событиями с момента последнего запуска системы:

journalctl

Для пролистывания журнала используйте или Enter (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра используйте q .

```
[root@hamdimohammad hamdimohammad]# journalctl
Oct 10 10:23:30 hamdimohammad kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build>
Oct 10 10:23:30 hamdimohammad kernel: The list of certified hardware and cloud instances for Enterprise Lin>
Oct 10 10:23:30 hamdimohammad kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x>
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point register>
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, usin>
Oct 10 10:23:30 hamdimohammad kernel: signal: max sigframe size: 1776
Oct 10 10:23:30 hamdimohammad kernel: BIOS-provided physical RAM map:
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000fffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000dfff0000-0x00000000dffffffffff] ACPI data
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00ffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00ffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ffffffffff] usable
Oct 10 10:23:30 hamdimohammad kernel: NX (Execute Disable) protection: active
Oct 10 10:23:30 hamdimohammad kernel: SMBIOS 2.5 present.
Oct 10 10:23:30 hamdimohammad kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 10 10:23:30 hamdimohammad kernel: Hypervisor detected: KVM
Oct 10 10:23:30 hamdimohammad kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 10 10:23:30 hamdimohammad kernel: kvm-clock: using sched offset of 7396320779 cycles
Oct 10 10:23:30 hamdimohammad kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e>
Oct 10 10:23:30 hamdimohammad kernel: tsc: Detected 2599.998 MHz processor
Oct 10 10:23:30 hamdimohammad kernel: e820: update [mem 0x00000000-0x00000ffff] usable ==> reserved
Oct 10 10:23:30 hamdimohammad kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 10 10:23:30 hamdimohammad kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 10:23:30 hamdimohammad kernel: MTRRs disabled by BIOS
Oct 10 10:23:30 hamdimohammad kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Oct 10 10:23:30 hamdimohammad kernel: last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
Oct 10 10:23:30 hamdimohammad kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
```

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

```
Oct 10 10:38:30 hamdimohammad systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated successfully.
Oct 10 10:40:45 hamdimohammad systemd[1]: Stopping System Logging Service...
Oct 10 10:40:45 hamdimohammad rsyslogd[1276]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="1276" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 10 10:40:45 hamdimohammad systemd[1]: rsyslog.service: Deactivated successfully.
Oct 10 10:40:45 hamdimohammad systemd[1]: Stopped System Logging Service.
Oct 10 10:40:46 hamdimohammad systemd[1]: Starting System Logging Service...
Oct 10 10:40:46 hamdimohammad rsyslogd[42580]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42580" x-info="https://www.rsyslog.com"] start
Oct 10 10:40:46 hamdimohammad rsyslogd[42580]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 10 10:40:46 hamdimohammad systemd[1]: Started System Logging Service.
Oct 10 10:40:54 hamdimohammad systemd[1]: Stopping The Apache HTTP Server...
Oct 10 10:40:55 hamdimohammad systemd[1]: httpd.service: Deactivated successfully.
Oct 10 10:40:55 hamdimohammad systemd[1]: Stopped The Apache HTTP Server.
Oct 10 10:40:55 hamdimohammad systemd[1]: Starting The Apache HTTP Server...
Oct 10 10:40:55 hamdimohammad httpd[42592]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:feba:a06d%enp0s3. Set the 'ServerName' directive globally to suppress this message
Oct 10 10:40:55 hamdimohammad httpd[42592]: Server configured, listening on: port 80
Oct 10 10:40:55 hamdimohammad systemd[1]: Started The Apache HTTP Server.
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopping System Logging Service...
Oct 10 10:42:08 hamdimohammad rsyslogd[42580]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42580" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 10 10:42:08 hamdimohammad systemd[1]: rsyslog.service: Deactivated successfully.
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopped System Logging Service.
Oct 10 10:42:08 hamdimohammad systemd[1]: Starting System Logging Service...
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42803" x-info="https://www.rsyslog.com"] start
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 10 10:42:08 hamdimohammad systemd[1]: Started System Logging Service.
Oct 10 10:42:46 hamdimohammad root[42821]: Daemon Debug Message
Oct 10 10:43:01 hamdimohammad PackageKit[4396]: daemon quit
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Deactivated successfully.
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Consumed 5.535s CPU time.
[root@hamdimohammad hmohammad]#
```

## 3. Режим просмотра журнала в реальном времени: `journalctl -f` Используйте `Ctrl + c` для прерывания просмотра.

```
[root@hamdimohammad hmohammad]#
[root@hamdimohammad hmohammad]# journalctl -f
Oct 10 10:42:08 hamdimohammad systemd[1]: rsyslog.service: Deactivated successfully.
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopped System Logging Service.
Oct 10 10:42:08 hamdimohammad systemd[1]: Starting System Logging Service...
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42803" x-info="https://www.rsyslog.com"] start
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Oct 10 10:42:08 hamdimohammad systemd[1]: Started System Logging Service.
Oct 10 10:42:46 hamdimohammad root[42821]: Daemon Debug Message
Oct 10 10:43:01 hamdimohammad PackageKit[4396]: daemon quit
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Deactivated successfully.
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Consumed 5.535s CPU time.
^C
[root@hamdimohammad hmohammad]#
```

4. Для использования фильтрации просмотра конкретных параметров журнала введите `journalctl` и дважды нажмите клавишу `Tab` .

```
hmoammad@hamdimoham... x hmoammad@hamdimoham... x hmoammad@hamdimoham...
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
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_STDDEV=
DBUS_BROKER_POLICY_TYPE=
DBUS_BROKER_RECEIVER_SECURITY_LABEL=
DBUS_BROKER_RECEIVER_UNIQUE_NAME=
DBUS_BROKER_RECEIVER_WELL_KNOWN_NAME_0=
DBUS_BROKER_SENDER_SECURITY_LABEL=
DBUS_BROKER_SENDER_UNIQUE_NAME=
DBUS_BROKER_TRANSMIT_ACTION=
DEVICE=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
ERRNO=
_EXE=
_GID=
--More--
_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=
```

5. Просмотрите события для UID0:  
journalctl \_UID=0

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# journalctl _UID=0  
Oct 10 10:23:30 hamdimohammad systemd-journald[271]: Journal started  
Oct 10 10:23:30 hamdimohammad systemd-journald[271]: Runtime Journal (/run/log/journal/e9732fe1220a4deab3e1  
Oct 10 10:23:30 hamdimohammad systemd-sysusers[274]: Creating group 'nobody' with GID 65534.  
Oct 10 10:23:30 hamdimohammad systemd-sysusers[274]: Creating group 'users' with GID 100.  
Oct 10 10:23:30 hamdimohammad systemd-sysusers[274]: Creating group 'dbus' with GID 81.  
Oct 10 10:23:30 hamdimohammad systemd-sysusers[274]: Creating user 'dbus' (System Message Bus) with UID 81  
Oct 10 10:23:30 hamdimohammad systemd-modules-load[273]: Inserted module 'fuse'  
Oct 10 10:23:30 hamdimohammad systemd-modules-load[273]: Module 'msr' is built in  
Oct 10 10:23:30 hamdimohammad systemd[1]: Starting Create Volatile Files and Directories...  
Oct 10 10:23:30 hamdimohammad systemd[1]: Finished Create Volatile Files and Directories.  
Oct 10 10:23:30 hamdimohammad systemd[1]: Finished Setup Virtual Console.  
Oct 10 10:23:30 hamdimohammad systemd[1]: dracut ask for additional cmdline parameters was skipped because  
Oct 10 10:23:30 hamdimohammad systemd[1]: Starting dracut cmdline hook...  
Oct 10 10:23:30 hamdimohammad dracut-cmdline[291]: dracut-9.4 (Blue Onyx) dracut-057-53.git20240104.el9  
Oct 10 10:23:30 hamdimohammad dracut-cmdline[291]: Using kernel command line parameters: BOOT_IMAGE=(hdb  
Oct 10 10:23:31 hamdimohammad systemd[1]: Finished dracut cmdline hook.  
Oct 10 10:23:31 hamdimohammad systemd[1]: Starting dracut pre-udev hook...  
Oct 10 10:23:31 hamdimohammad systemd[1]: Finished dracut pre-udev hook.  
Oct 10 10:23:31 hamdimohammad systemd[1]: Starting Rule-based Manager for Device Events and Files...  
Oct 10 10:23:31 hamdimohammad systemd-udevd[405]: Using default interface naming scheme 'rhel-9.0'.  
Oct 10 10:23:31 hamdimohammad systemd[1]: Started Rule-based Manager for Device Events and Files.  
Oct 10 10:23:31 hamdimohammad systemd[1]: dracut pre-trigger hook was skipped because no trigger condition  
Oct 10 10:23:31 hamdimohammad systemd[1]: Starting Coldplug All udev Devices...  
Oct 10 10:23:31 hamdimohammad systemd[1]: sys-module-fuse.device: Failed to enqueue SYSTEMD_WANTS= job, ign  
Oct 10 10:23:31 hamdimohammad systemd[1]: Finished Coldplug All udev Devices.  
Oct 10 10:23:31 hamdimohammad systemd[1]: nm-initrd.service was skipped because of an unmet condition check  
Oct 10 10:23:31 hamdimohammad systemd[1]: Reached target Network.  
Oct 10 10:23:31 hamdimohammad systemd[1]: nm-wait-online-initrd.service was skipped because of an unmet con  
Oct 10 10:23:31 hamdimohammad systemd[1]: Starting dracut initqueue hook...  
Oct 10 10:23:31 hamdimohammad systemd[1]: Starting Show Plymouth Boot Screen...  
Oct 10 10:23:31 hamdimohammad systemd[1]: Received SIGRTMIN+20 from PID 424 (plymouthd).  
Oct 10 10:23:31 hamdimohammad systemd[1]: Started Show Plymouth Boot Screen.  
Oct 10 10:23:31 hamdimohammad systemd[1]: Dispatch Password Requests to Console Directory Watch was skipped  
Oct 10 10:23:31 hamdimohammad systemd[1]: Started Forward Password Requests to Plymouth Directory Watch.
```

6. Для отображения последних 20 строк журнала введите  
journalctl -n 20

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# journalctl -n 20  
Oct 10 10:40:46 hamdimohammad systemd[1]: Started System Logging Service.  
Oct 10 10:40:54 hamdimohammad systemd[1]: Stopping The Apache HTTP Server...  
Oct 10 10:40:55 hamdimohammad systemd[1]: httpd.service: Deactivated successfully.  
Oct 10 10:40:55 hamdimohammad systemd[1]: Stopped The Apache HTTP Server.  
Oct 10 10:40:55 hamdimohammad systemd[1]: Starting The Apache HTTP Server...  
Oct 10 10:40:55 hamdimohammad httpd[42592]: AH00558: httpd: Could not reliably determine the server's fully  
Oct 10 10:40:55 hamdimohammad httpd[42592]: Server configured, listening on: port 80  
Oct 10 10:40:55 hamdimohammad systemd[1]: Started The Apache HTTP Server.  
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopping System Logging Service...  
Oct 10 10:42:08 hamdimohammad rsyslogd[42580]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid  
Oct 10 10:42:08 hamdimohammad systemd[1]: rsyslog.service: Deactivated successfully.  
Oct 10 10:42:08 hamdimohammad systemd[1]: Stopped System Logging Service.  
Oct 10 10:42:08 hamdimohammad systemd[1]: Starting System Logging Service...  
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid  
Oct 10 10:42:08 hamdimohammad rsyslogd[42803]: imjournal: journal files changed, reloading... [v8.2310.0-4  
Oct 10 10:42:08 hamdimohammad systemd[1]: Started System Logging Service.  
Oct 10 10:42:46 hamdimohammad root[42821]: Daemon Debug Message  
Oct 10 10:43:01 hamdimohammad PackageKit[4396]: daemon quit  
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Deactivated successfully.  
Oct 10 10:43:01 hamdimohammad systemd[1]: packagekit.service: Consumed 5.535s CPU time.  
lines 1-20/20 (END)
```



7. Для просмотра только сообщений об ошибках введите `journalctl -p err`

```
[root@hamdimohammad hmohammad]# journalctl -p err
Oct 10 10:23:30 hamdimohammad systemd[1]: Invalid DMI field header.
Oct 10 10:23:32 hamdimohammad kernel: Warning: Unmaintained driver is detected: el000
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an u>
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broke>
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graph>
Oct 10 10:23:41 hamdimohammad systemd[1]: Invalid DMI field header.
Oct 10 10:23:43 hamdimohammad systemd-udevd[689]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only netw>
Oct 10 10:23:43 hamdimohammad systemd-udevd[708]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only netwo>
Oct 10 10:23:48 hamdimohammad alsactl[854]: alsalib main.c:1554:(snd_use_case_mgr_open) error: failed to i>
Oct 10 10:23:56 hamdimohammad kernel: Warning: Unmaintained driver is detected: ip_set
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: gkr-pam: unable to locate daemon control file
Oct 10 10:26:46 hamdimohammad gdm-wayland-session[1267]: GLib: Source ID 2 was not found when attempting to>
Oct 10 10:26:46 hamdimohammad gdm-launch-environment[1214]: GLib-GObject: g_object_unref: assertion 'G_IS->
lines 1-13/13 (END)
```

8. Если вы хотите просмотреть сообщения журнала, записанные за определённый период времени, вы можете использовать параметры `--since` и `--until`. Обе опции принимают параметр времени в формате `YYYY-MM-DD hh:mm:ss`. Кроме того, вы можете использовать `yesterday`, `today` и `tomorrow` в качестве параметров. Например, для просмотра всех сообщений со вчерашнего дня введите `journalctl --since yesterday`

```
[root@hamdimohammad hmohammad]# journalctl --since yesterday
Oct 10 10:23:30 hamdimohammad kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build>
Oct 10 10:23:30 hamdimohammad kernel: The list of certified hardware and cloud instances for Enterprise Lin>
Oct 10 10:23:30 hamdimohammad kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x>
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point register>
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, usin>
Oct 10 10:23:30 hamdimohammad kernel: signal: max sigframe size: 1776
Oct 10 10:23:30 hamdimohammad kernel: BIOS-provided physical RAM map:
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbf] usable
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000009fc0-0x00000000000009ffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000010000-0x000000000000dfffff] usable
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000000dffff000-0x00000000000dffffff] ACPI data
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Oct 10 10:23:30 hamdimohammad kernel: NX (Execute Disable) protection: active
Oct 10 10:23:30 hamdimohammad kernel: SMBIOS 2.5 present.
Oct 10 10:23:30 hamdimohammad kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 10 10:23:30 hamdimohammad kernel: Hypervisor detected: KVM
Oct 10 10:23:30 hamdimohammad kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 10 10:23:30 hamdimohammad kernel: kvm-clock: using sched offset of 7396320779 cycles
Oct 10 10:23:30 hamdimohammad kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e>
Oct 10 10:23:30 hamdimohammad kernel: tsc: Detected 2599.998 MHz processor
Oct 10 10:23:30 hamdimohammad kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 10 10:23:30 hamdimohammad kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 10 10:23:30 hamdimohammad kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 10 10:23:30 hamdimohammad kernel: MTRRs disabled by BIOS
Oct 10 10:23:30 hamdimohammad kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Oct 10 10:23:30 hamdimohammad kernel: last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
Oct 10 10:23:30 hamdimohammad kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
```

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

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# journalctl --since yesterday -p err  
Oct 10 10:23:30 hamdimohammad systemd[1]: Invalid DMI field header.  
Oct 10 10:23:32 hamdimohammad kernel: Warning: Unmaintained driver is detected: e1000  
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an u>  
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broke>  
Oct 10 10:23:32 hamdimohammad kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graph>  
Oct 10 10:23:41 hamdimohammad systemd[1]: Invalid DMI field header.  
Oct 10 10:23:43 hamdimohammad systemd-udevd[689]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 Only netw>  
Oct 10 10:23:43 hamdimohammad systemd-udevd[708]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 Only netwo>  
Oct 10 10:23:48 hamdimohammad alsactl[854]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to i>  
Oct 10 10:23:56 hamdimohammad kernel: Warning: Unmaintained driver is detected: ip_set  
Oct 10 10:26:37 hamdimohammad gdm-password[1733]: gkr-pam: unable to locate daemon control file  
Oct 10 10:26:46 hamdimohammad gdm-wayland-session[1267]: GLib: Source ID 2 was not found when attempting to>  
Oct 10 10:26:46 hamdimohammad gdm-launch-environment[1214]: GLib-GObject: g_object_unref: assertion 'G_IS_>  
lines 1-13/13 (END)
```

10. Если вам нужна детальная информация, то используйте `journalctl -o verbose`

```
Thu 2024-10-10 10:23:30.346043 MSK [s=819e8a9f8c2f4f3e8df7e8dfdf3b2dc7;i=1;b=bb9043b8e29a4942a89a7edaf229c0>  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
PRIORITY=5  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
MESSAGE=Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org)>  
_BOOT_ID=bb9043b8e29a4942a89a7edaf229c0c6  
_MACHINE_ID=e9732fe1220a4deab3e1dfd7eba0f263  
_HOSTNAME=hamdimohammad  
_RUNTIME_SCOPE=initrd  
Thu 2024-10-10 10:23:30.346107 MSK [s=819e8a9f8c2f4f3e8df7e8dfdf3b2dc7;i=2;b=bb9043b8e29a4942a89a7edaf229c0>  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
PRIORITY=5  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=bb9043b8e29a4942a89a7edaf229c0c6  
_MACHINE_ID=e9732fe1220a4deab3e1dfd7eba0f263  
_HOSTNAME=hamdimohammad  
_RUNTIME_SCOPE=initrd  
MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the >  
Thu 2024-10-10 10:23:30.346141 MSK [s=819e8a9f8c2f4f3e8df7e8dfdf3b2dc7;i=3;b=bb9043b8e29a4942a89a7edaf229c0>  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
SYSLOG_IDENTIFIER=kernel  
_BOOT_ID=bb9043b8e29a4942a89a7edaf229c0c6  
_MACHINE_ID=e9732fe1220a4deab3e1dfd7eba0f263  
_HOSTNAME=hamdimohammad  
_RUNTIME_SCOPE=initrd  
PRIORITY=6  
MESSAGE=Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x86_64 root=/dev/mapper/r1->  
Thu 2024-10-10 10:23:30.346171 MSK [s=819e8a9f8c2f4f3e8df7e8dfdf3b2dc7;i=4;b=bb9043b8e29a4942a89a7edaf229c0>  
_SOURCE_MONOTONIC_TIMESTAMP=0  
_TRANSPORT=kernel  
SYSLOG_FACILITY=0  
lines 1-37
```

11. Для просмотра дополнительной информации о модуле sshd введите `journalctl _SYSTEMD_UNIT=sshd.service`

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# journalctl _SYSTEMD_UNIT=sshd.service  
Oct 10 10:23:57 hamdimohammad sshd[1182]: Server listening on 0.0.0.0 port 22.  
Oct 10 10:23:57 hamdimohammad sshd[1182]: Server listening on :: port 22.  
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]#
```

## Постоянный журнал journald

По умолчанию журнал journald хранит сообщения в оперативной памяти системы и записи доступны в каталоге `/run/log/journal` только до перезагрузки системы. Для того чтобы сделать журнал journald постоянным, выполните следующие действия.

1. Запустите терминал и получите полномочия администратора.
2. Создайте каталог для хранения записей журнала: `mkdir -p /var/log/journal`
3. Скорректируйте права доступа для каталога `/var/log/journal`, чтобы journald смог записывать в него информацию: `chown root:systemd-journal /var/log/journal chmod 2755 /var/log/journal`
4. Для принятия изменений необходимо или перезагрузить систему (перезапустить службу `systemd-journald` недостаточно), или использовать команду: `killall -USR1 systemd-journald`
5. Журнал systemd теперь постоянный. Если вы хотите видеть сообщения журнала с момента последней перезагрузки, используйте: `journalctl -b`

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# mkdir -p /var/log/journal  
[root@hamdimohammad hmohammad]# chown root:systemd-journal /var/log/journal/  
[root@hamdimohammad hmohammad]# chmod 2755 /var/log/journal/  
[root@hamdimohammad hmohammad]# killall -USR1 systemd-journald  
[root@hamdimohammad hmohammad]# journalctl -b  
Oct 10 10:23:30 hamdimohammad kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build>  
Oct 10 10:23:30 hamdimohammad kernel: The list of certified hardware and cloud instances for Enterprise Lin  
Oct 10 10:23:30 hamdimohammad kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x>  
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'  
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'  
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'  
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256  
Oct 10 10:23:30 hamdimohammad kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using  
Oct 10 10:23:30 hamdimohammad kernel: signal: max sigframe size: 1776  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-provided physical RAM map:  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000000100000-0x000000000000dfffff] usable  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000000dfff0000-0x000000000000dfffff] ACPI data  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved  
Oct 10 10:23:30 hamdimohammad kernel: BIOS-e820: [mem 0x000000000ffc000000-0x000000000fffffffff] reserved
```



## Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Файл конфигурации для rsyslogd — это `/etc/rsyslog.conf`. Дополнительные конфигурации могут находиться в директории `/etc/rsyslog.d/`.

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

Сообщения, связанные с аутентификацией, обычно записываются в файл `/var/log/auth.log` на большинстве систем Linux.

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

По умолчанию ротация журналов происходит еженедельно. Это определяется настройками в файле `/etc/logrotate.conf` или в файлах конфигурации в `/etc/logrotate.d/`.

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

В файл `/etc/rsyslog.conf` добавьте следующую 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 `journalctl -f` позволяет вам наблюдать за сообщениями журнала в режиме реального времени.

6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны

Команда `journalctl` выводит все сообщения журнала `journald`, а для сообщений `rsyslog` можно использовать команду `cat /var/log/syslog` (или другой файл журнала в зависимости от системы).

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

Команда `journalctl -b` выводит сообщения journald, записанные после последней перезагрузки.

8. Какая процедура позволяет сделать журнал journald постоянным?

Создайте каталог для хранения записей журнала: `mkdir -p /var/log/journal`

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

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

## **Заключение**

Получены навыки работы с журналом событий.