

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:

Группа:

МОСКВА

2024 г.

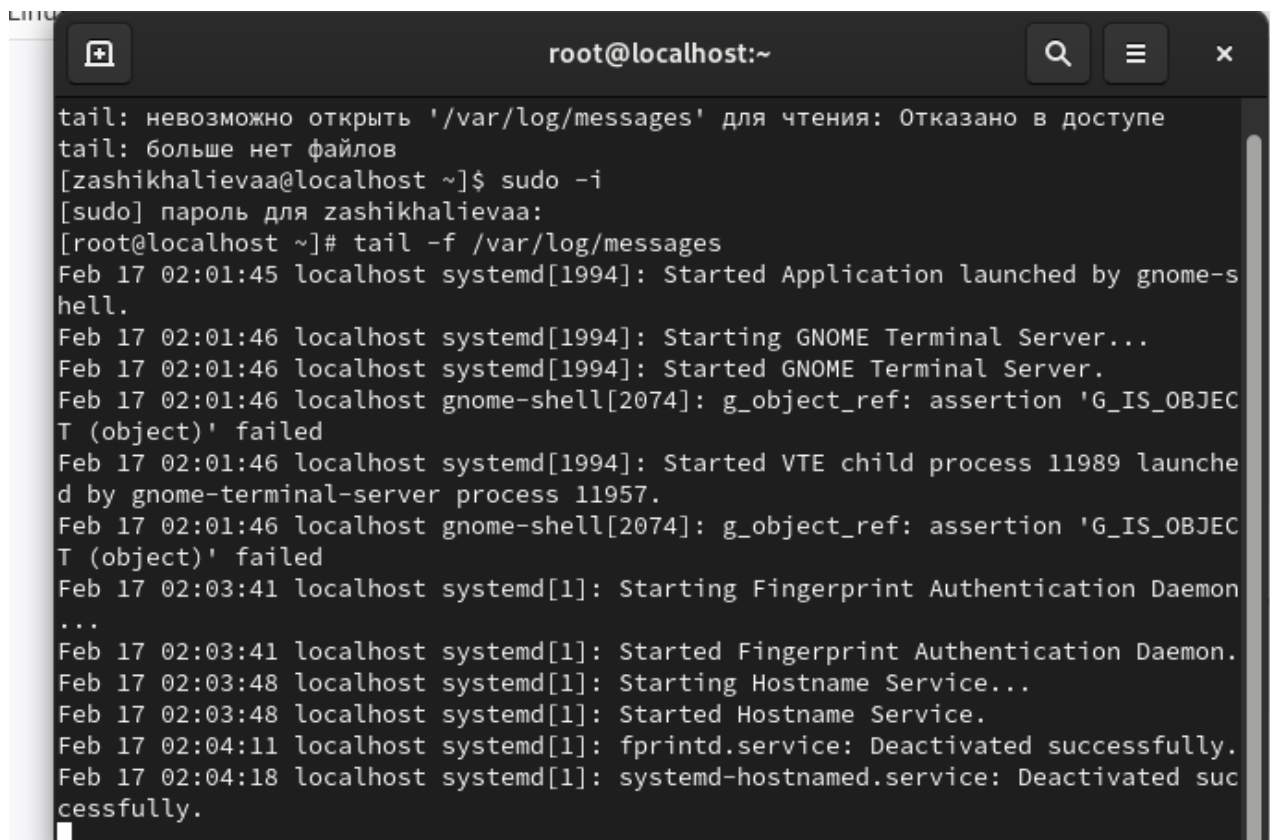
Постановка задачи

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`
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`.
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`.



The screenshot shows a terminal window titled `root@localhost:~`. The user `zashikhalievaa` has run `sudo -i` to become root. Then, they have run `tail -f /var/log/messages` in the root shell. The terminal displays a series of system logs from `/var/log/messages`, including messages about the GNOME Terminal Server starting, a g_object_ref assertion failure in gnome-shell, and the Fingerprint Authentication Daemon and Hostname Service starting and then being deactivated.

```
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
tail: больше нет файлов
[zashikhalievaa@localhost ~]$ sudo -i
[sudo] пароль для zashikhalievaa:
[root@localhost ~]# tail -f /var/log/messages
Feb 17 02:01:45 localhost systemd[1994]: Started Application launched by gnome-s
hell.
Feb 17 02:01:46 localhost systemd[1994]: Starting GNOME Terminal Server...
Feb 17 02:01:46 localhost systemd[1994]: Started GNOME Terminal Server.
Feb 17 02:01:46 localhost gnome-shell[2074]: g_object_ref: assertion 'G_IS_OBJEC
T (object)' failed
Feb 17 02:01:46 localhost systemd[1994]: Started VTE child process 11989 launche
d by gnome-terminal-server process 11957.
Feb 17 02:01:46 localhost gnome-shell[2074]: g_object_ref: assertion 'G_IS_OBJEC
T (object)' failed
Feb 17 02:03:41 localhost systemd[1]: Starting Fingerprint Authentication Daemon
...
Feb 17 02:03:41 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Feb 17 02:03:48 localhost systemd[1]: Starting Hostname Service...
Feb 17 02:03:48 localhost systemd[1]: Started Hostname Service.
Feb 17 02:04:11 localhost systemd[1]: fprintd.service: Deactivated successfully.
Feb 17 02:04:18 localhost systemd[1]: systemd-hostnamed.service: Deactivated suc
cessfully.
```

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`.

```
AC
[root@localhost ~]# tail -n 20 /var/log/secure
Feb 17 02:01:07 localhost gdm-password[11870]: gkr-pam: unlocked login keyring
Feb 17 02:01:37 localhost su[10842]: pam_unix(su-l:session): session closed for user alice
Feb 17 02:01:37 localhost su[10652]: pam_unix(su-l:session): session closed for user bob
Feb 17 02:01:37 localhost sudo[10258]: pam_unix(sudo-i:session): session closed for user root
Feb 17 02:01:37 localhost sudo[10840]: pam_unix(sudo:session): session closed for user root
Feb 17 02:01:37 localhost sudo[10650]: pam_unix(sudo:session): session closed for user root
Feb 17 02:03:48 localhost sudo[12052]: zashikhalievaa : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:07:22 localhost sudo[12205]: zashikhalievaa : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:07:22 localhost sudo[12205]: pam_unix(sudo-i:session): session opened for user root(uid=0) by zashikhalievaa(uid=1002)
Feb 17 02:07:28 localhost sudo[12205]: pam_unix(sudo-i:session): session closed for user root
Feb 17 02:07:54 localhost sudo[12261]: zashikhalievaa : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:07:54 localhost sudo[12261]: pam_unix(sudo-i:session): session opened for user root(uid=0) by zashikhalievaa(uid=1002)
Feb 17 02:08:07 localhost sudo[12294]: root : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:08:07 localhost sudo[12294]: pam_unix(sudo-i:session): session opened for user root(uid=0) by zashikhalievaa(uid=0)
Feb 17 02:08:30 localhost sudo[12294]: pam_unix(sudo-i:session): session closed for user root
Feb 17 02:08:31 localhost sudo[12261]: pam_unix(sudo-i:session): session closed for user root
Feb 17 02:08:38 localhost sudo[12335]: zashikhalievaa : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:08:38 localhost sudo[12335]: pam_unix(sudo-i:session): session opened for user root(uid=0) by zashikhalievaa(uid=1002)
Feb 17 02:09:31 localhost sudo[12335]: pam_unix(sudo-i:session): session closed for user root
[root@localhost ~]#
```

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`

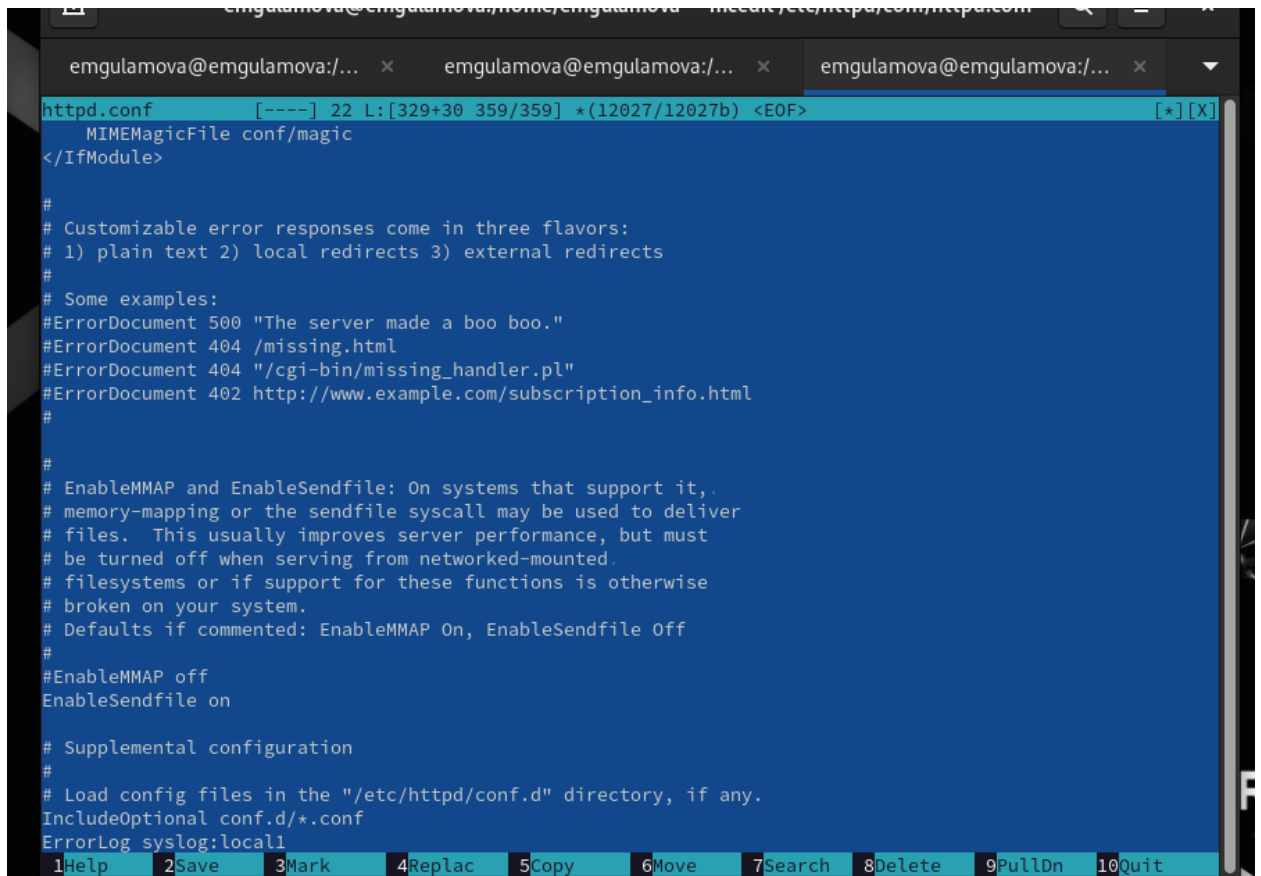
2. После окончания процесса установки запустите веб-службу:
`systemctl start httpd`
`systemctl enable httpd`

```
root@localhost:~
[zashikhalievaa@localhost ~]$ sudo -i
[sudo] пароль для zashikhalievaa:
[root@localhost ~]# dnf -y install httpd
Последняя проверка окончания срока действия метаданных: 1:59:06 назад, Пн 17 фев 2025 00:17:34.
Пакет httpd-2.4.62-1.el9.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

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`.

```
[Fri Oct 04 19:22:07.904493 2024] [core:notice] [pid 3783:tid 3783] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 04 19:22:07.925649 2024] [suexec:notice] [pid 3783:tid 3783] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 04 19:22:08.046095 2024] [lbmethod_heartbeat:notice] [pid 3783:tid 3783] AH02282: No slotmem from mod_heartbeat
[Fri Oct 04 19:22:08.057568 2024] [mpm_event:notice] [pid 3783:tid 3783] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 04 19:22:08.057609 2024] [core:notice] [pid 3783:tid 3783] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
```

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.



```
emgulamova@emgulamova:/... x emgulamova@emgulamova:/... x emgulamova@emgulamova:/... x
httpd.conf [----] 22 L:[329+30 359/359] *(12027/12027b) <EOF> [*] [X]
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 10Quit
```

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

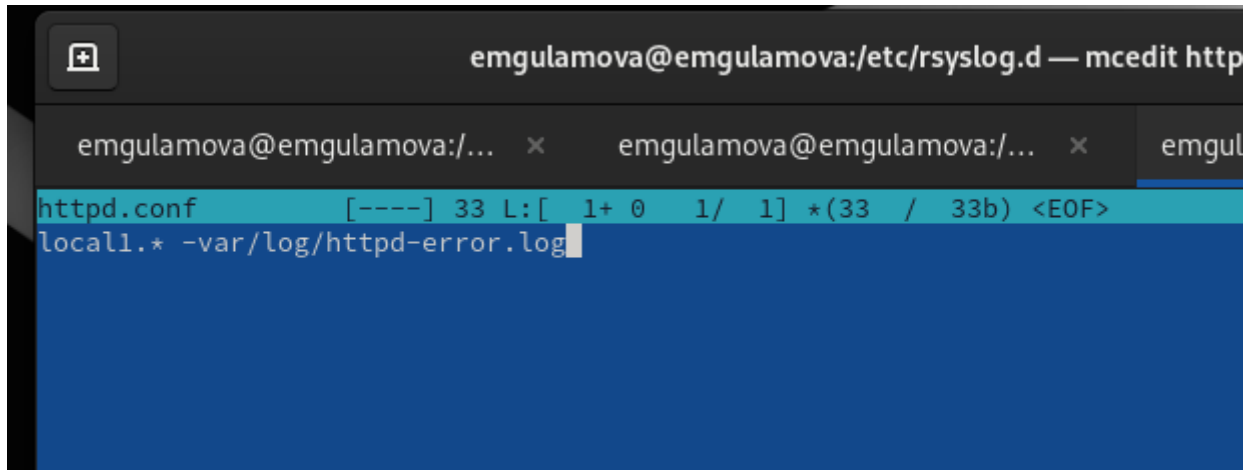
```
cd /etc/rsyslog.d
```

```
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@localhost ~]# mcedit /etc/httpd/conf/httpd.conf
[root@localhost ~]# cd /etc/rsyslog.d/
[root@localhost rsyslog.d]# touch httpd.conf
[root@localhost rsyslog.d]# mcedit httpd.conf

[root@localhost rsyslog.d]# ls
httpd.conf
[root@localhost rsyslog.d]# touch debug.conf
[root@localhost rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@localhost rsyslog.d]#
```

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

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"`

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

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@localhost ~]# journalctl
Feb 16 21:27:33 localhost kernel: Linux version 5.14.0-503.23.2.el9_5.x86_64 (mockbuild@iadi-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719)
Feb 16 21:27:33 localhost kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://redhat.com/ecosystem
Feb 16 21:27:33 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-503.23.2.el9_5.x86_64 root=/dev/mapper/rh-root ro crashkernel=16-46:192M
Feb 16 21:27:33 localhost kernel: BIOS-provided physical RAM map:
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000000000fffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000fffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x0000000007fff0000-0x0000000007fffff] ACPI data
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000ffffffff] reserved
Feb 16 21:27:33 localhost kernel: NX (Execute Disable) protection: active
Feb 16 21:27:33 localhost kernel: APIC: Static calls initialized
Feb 16 21:27:33 localhost kernel: SMBIOS 2.5 present.
Feb 16 21:27:33 localhost kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 16 21:27:33 localhost kernel: Hypervisor detected: KVM
Feb 16 21:27:33 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 16 21:27:33 localhost kernel: kvm-clock: using sched offset of 4864383621 cycles
Feb 16 21:27:33 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Feb 16 21:27:33 localhost kernel: tsc: Detected 2496.004 MHz processor
Feb 16 21:27:33 localhost kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Feb 16 21:27:33 localhost kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Feb 16 21:27:33 localhost kernel: last_pfn = 0x7ffff max_arch_pfn = 0x400000000
Feb 16 21:27:33 localhost kernel: MTRRs disabled by BIOS
Feb 16 21:27:33 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Feb 16 21:27:33 localhost kernel: found SMP MP-table at [mem 0x0009ffff-0x0009ffff]
Feb 16 21:27:33 localhost kernel: Incomplete global flushes, disabling PCID
Feb 16 21:27:33 localhost kernel: RAMDISK: [mem 0x30f0f000-0x3477ffff]
Feb 16 21:27:33 localhost kernel: ACPI: Early table checksum verification disabled
Feb 16 21:27:33 localhost kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
Feb 16 21:27:33 localhost kernel: ACPI: XSDT 0x0000000007FFF0030 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
Feb 16 21:27:33 localhost kernel: ACPI: FACP 0x0000000007FFF00F0 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
Feb 16 21:27:33 localhost kernel: ACPI: DSDT 0x0000000007FFF0610 002353 (v02 VBOX VBOXBIOS 00000002 INTL 20100528)
Feb 16 21:27:33 localhost kernel: ACPI: FACS 0x0000000007FFF0200 000040
Feb 16 21:27:33 localhost kernel: ACPI: FACS 0x0000000007FFF0200 000040
Feb 16 21:27:33 localhost kernel: ACPI: APIC 0x0000000007FFF0240 000054 (v02 VBOX VBOXAPIC 00000001 ASL 00000061)
Feb 16 21:27:33 localhost kernel: ACPI: SSDT 0x0000000007FFF02A0 00036C (v01 VBOX VBOXCPUPT 00000002 INTL 20100528)
Feb 16 21:27:33 localhost kernel: ACPI: Reserving FACP table memory at [mem 0x7ffff00f0-0x7ffff01e3]
Feb 16 21:27:33 localhost kernel: ACPI: Reserving DSDT table memory at [mem 0x7ffff0610-0x7ffff2962]
Feb 16 21:27:33 localhost kernel: ACPI: Reserving FACS table memory at [mem 0x7ffff0200-0x7ffff023f]
Feb 16 21:27:33 localhost kernel: ACPI: Reserving FACS table memory at [mem 0x7ffff0200-0x7ffff023f]
```

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

```
Feb 17 02:26:59 localhost.localdomain sudo[12951]: pam_unix(sudo:session): session closed for user root
Feb 17 02:28:50 localhost.localdomain systemd[1]: Starting Fingerprint Authentication Daemon...
Feb 17 02:28:50 localhost.localdomain systemd[1]: Started Fingerprint Authentication Daemon.
Feb 17 02:29:21 localhost.localdomain systemd[1]: fprintd.service: Deactivated successfully.
Feb 17 02:29:42 localhost.localdomain unix_chkpwd[13007]: password check failed for user (zashikhalievaa)
Feb 17 02:29:42 localhost.localdomain sudo[12981]: pam_unix(sudo-i:auth): authentication failure; logname=zashikhalievaa uid=1002 euid=0 tty=/dev/pts/2 ru
zashikhalievaa rhost= user=zashikhalievaa
Feb 17 02:29:44 localhost.localdomain systemd[1]: Starting Fingerprint Authentication Daemon...
Feb 17 02:29:44 localhost.localdomain systemd[1]: Started Fingerprint Authentication Daemon.
Feb 17 02:29:48 localhost.localdomain sudo[12981]: zashikhalievaa : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash
Feb 17 02:29:48 localhost.localdomain sudo[12981]: pam_unix(sudo-i:session): session opened for user root(uid=0) by zashikhalievaa(uid=1002)
Feb 17 02:29:48 localhost.localdomain systemd[1]: Starting Hostname Service...
Feb 17 02:29:48 localhost.localdomain systemd[1]: Started Hostname Service.
Feb 17 02:30:14 localhost.localdomain systemd[1]: fprintd.service: Deactivated successfully.
Feb 17 02:30:18 localhost.localdomain systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Feb 17 02:30:30 localhost.localdomain systemd[1]: Starting PackageKit Daemon...
Feb 17 02:30:30 localhost.localdomain PackageKit[13062]: daemon start
Feb 17 02:30:30 localhost.localdomain systemd[1]: Started PackageKit Daemon.
Feb 17 02:30:30 localhost.localdomain PackageKit[13062]: search-file transaction /536_cbdcbce from uid 0 finished with success after 412ms
Feb 17 02:31:00 localhost.localdomain PackageKit[13062]: search-file transaction /537_dadbbeeb from uid 0 finished with success after 50ms
Feb 17 02:31:11 localhost.localdomain PackageKit[13062]: new install-packages transaction /538_dcbdbedb scheduled from uid 0
Feb 17 02:31:12 localhost.localdomain PackageKit[13062]: in /538_dcbdbedb for install-packages package mc;1:4.8.26-5.el9;x86_64;appstream was installing f
id 0
Feb 17 02:31:12 localhost.localdomain PackageKit[13062]: install-packages transaction /538_dcbdbedb from uid 0 finished with success after 376ms
Feb 17 02:31:18 localhost.localdomain PackageKit[13062]: uid 0 is trying to obtain org.freedesktop.packagekit.package-install auth (only_trusted:1)
Feb 17 02:31:18 localhost.localdomain PackageKit[13062]: new install-packages transaction /539_aacbeadb scheduled from uid 0
Feb 17 02:31:18 localhost.localdomain PackageKit[13062]: uid 0 obtained auth for org.freedesktop.packagekit.package-install
Feb 17 02:31:24 localhost.localdomain systemd[1]: Started /usr/bin/systemctl start man-db-cache-update.
Feb 17 02:31:24 localhost.localdomain systemd[1]: Starting man-db-cache-update.service...
Feb 17 02:31:24 localhost.localdomain PackageKit[13062]: in /539_aacbeadb for install-packages package mc;1:4.8.26-5.el9;x86_64;appstream was installing f
id 0
Feb 17 02:31:24 localhost.localdomain PackageKit[13062]: install-packages transaction /539_aacbeadb from uid 0 finished with success after 6179ms
Feb 17 02:31:25 localhost.localdomain systemd[1]: man-db-cache-update.service: Deactivated successfully.
Feb 17 02:31:25 localhost.localdomain systemd[1]: Finished man-db-cache-update.service.
Feb 17 02:31:25 localhost.localdomain systemd[1]: run-r1ecd21fc354d4ea7a5662c5578e55697.service: Deactivated successfully.
Feb 17 02:36:30 localhost.localdomain PackageKit[13062]: daemon quit
Feb 17 02:36:30 localhost.localdomain systemd[1]: packagekit.service: Deactivated successfully.
Feb 17 02:36:30 localhost.localdomain systemd[1]: packagekit.service: Consumed 1.793s CPU time.
[root@localhost ~]#
```


3. Режим просмотра журнала в реальном времени:

journalctl -f

Используйте Ctrl + c для прерывания просмотра.

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

```
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
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=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
[root@localhost ~]# journalctl
_AUDIT_LOGINUID=
_AUDIT_SESSION=
AVAILABLE=
AVAILABLE_PRETTY=
_BOOT_ID=
_CAP_EFFECTIVE=
_CMDLINE=
CODE_FILE=
CODE_FUNC=
CODE_LINE=
_COMM=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
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=
DISK_AVAILABLE=
DISK_AVAILABLE_PRETTY=
DISK_KEEP_FREE=
DISK_KEEP_FREE_PRETTY=
[root@localhost ~]# journalctl

INITRD_USEC=
INVOCATION_ID=
JOB_ID=
JOB_RESULT=
JOB_TYPE=
JOURNAL_NAME=
JOURNAL_PATH=
_KERNEL_DEVICE=
_KERNEL_SUBSYSTEM=
KERNEL_USEC=
LEADER=
LIMIT=
LIMIT_PRETTY=
_MACHINE_ID=
MAX_USE=
MAX_USE_PRETTY=
MESSAGE=
MESSAGE_ID=

ERRNO=
_EXE=
_GID=
GLIB_DOMAIN=
GLIB_OLD_LOG_API=
_HOSTNAME=
INITRD_USEC=
INVOCATION_ID=
JOB_ID=
JOB_RESULT=
JOB_TYPE=
JOURNAL_NAME=
JOURNAL_PATH=
_KERNEL_DEVICE=
_KERNEL_SUBSYSTEM=
KERNEL_USEC=
LEADER=
LIMIT=
LIMIT_PRETTY=
_MACHINE_ID=
MAX_USE=
MAX_USE_PRETTY=
MESSAGE=
MESSAGE_ID=

_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=

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=

TIMESTAMP_BOOTTIME=
TIMESTAMP_MONOTONIC=
_TRANSPORT=
_UDEV_DEVLINK=
_UDEV_DEVNODE=
_UDEV_SYSNAME=
_UID=
UNIT=
UNIT_RESULT=
USER_ID=
USER_INVOCATION_ID=
USERSPACE_USEC=
USER_UNIT=
WP_OBJECT=
WP_OBJECT_TYPE=

_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=
USER_ID=
USER_INVOCATION_ID=
USERSPACE_USEC=
USER_UNIT=
WP_OBJECT=
WP_OBJECT_TYPE=
```

5. Просмотрите события для UID0: journalctl _UID=0

```
[root@localhost ~]# journalctl -UID=0
Failed to parse timestamp: ID=0
[root@localhost ~]# journalctl _UID=0
фев 16 21:27:33 localhost systemd-journald[218]: Journal started
фев 16 21:27:33 localhost systemd-journald[218]: Runtime Journal (/run/log/journal/fd1db2d5c0c74bffa13d35e97b298403) is 4.4M, max 35.4M, 31.0M free.
фев 16 21:27:33 localhost systemd-modules-load[219]: Inserted module 'fuse'
фев 16 21:27:33 localhost systemd-modules-load[219]: Module 'msr' is built in
фев 16 21:27:33 localhost systemd-sysusers[220]: Creating group 'nobody' with GID 65534.
фев 16 21:27:33 localhost systemd-sysusers[220]: Creating group 'users' with GID 100.
фев 16 21:27:33 localhost systemd-sysusers[220]: Creating group 'dbus' with GID 81.
фев 16 21:27:33 localhost systemd-sysusers[220]: Creating user 'dbus' (System Message Bus) with UID 81 and GID 81.
фев 16 21:27:33 localhost systemd[1]: Starting Create Volatile Files and Directories...
фев 16 21:27:33 localhost systemd[1]: Finished Create Volatile Files and Directories.
фев 16 21:27:33 localhost systemd[1]: Finished Setup Virtual Console.
фев 16 21:27:33 localhost systemd[1]: dracut ask for additional cmdline parameters was skipped because no trigger condition checks were met.
фев 16 21:27:33 localhost systemd[1]: Starting dracut cmdline hook...
фев 16 21:27:33 localhost dracut-cmdline[233]: dracut-9.5 (Blue Onyx) dracut-057-70.git20240819.el9
фев 16 21:27:33 localhost dracut-cmdline[233]: Using kernel command line parameters: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-503.23.2.el9_5.x86_64 root=/dev
фев 16 21:27:33 localhost systemd[1]: Finished dracut cmdline hook.
фев 16 21:27:33 localhost systemd[1]: Starting dracut pre-udev hook...
фев 16 21:27:33 localhost systemd[1]: Finished dracut pre-udev hook.
фев 16 21:27:33 localhost systemd[1]: Starting Rule-based Manager for Device Events and Files...
фев 16 21:27:33 localhost systemd-udevd[345]: Using default interface naming scheme 'rhel-9.0'.
фев 16 21:27:33 localhost systemd[1]: Started Rule-based Manager for Device Events and Files.
фев 16 21:27:33 localhost systemd[1]: dracut pre-trigger hook was skipped because no trigger condition checks were met.
фев 16 21:27:33 localhost systemd[1]: Starting Coldplug All udev Devices...
фев 16 21:27:33 localhost systemd[1]: sys-module-fuse.device: Failed to enqueue SYSTEND_WANTS= job, ignoring: Unit sys-fs-fuse-connections.mount not found.
фев 16 21:27:33 localhost systemd[1]: Finished Coldplug All udev Devices.
фев 16 21:27:33 localhost systemd[1]: nm-initrd.service was skipped because of an unmet condition check (ConditionPathExists=/run/NetworkManager/initrd/needn
фев 16 21:27:33 localhost systemd[1]: Reached target Network.
фев 16 21:27:33 localhost systemd[1]: nm-wait-online-initrd.service was skipped because of an unmet condition check (ConditionPathExists=/run/NetworkManager/
фев 16 21:27:33 localhost systemd[1]: Starting dracut initqueue hook...
фев 16 21:27:33 localhost systemd[1]: Starting Show Plymouth Boot Screen...
фев 16 21:27:33 localhost systemd[1]: Received SIGRTMIN+20 from PID 371 (plymouthd).
фев 16 21:27:33 localhost systemd[1]: Started Show Plymouth Boot Screen.
фев 16 21:27:33 localhost systemd[1]: Dispatch Password Requests to Console Directory Watch was skipped because of an unmet condition check (ConditionPathExi
фев 16 21:27:33 localhost systemd[1]: Started Forward Password Requests to Plymouth Directory Watch
```

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

```
[root@localhost ~]# journalctl -n 20
фев 17 02:31:24 localhost.localdomain PackageKit[13062]: in /539_aacbeadb for install-packages package mc;1:4.8.26-5.el9;x86_64;appstream was installing for
фев 17 02:31:24 localhost.localdomain PackageKit[13062]: install-packages transaction /539_aacbeadb from uid 0 finished with success after 6179ms
фев 17 02:31:25 localhost.localdomain systemd[1]: man-db-cache-update.service: Deactivated successfully.
фев 17 02:31:25 localhost.localdomain systemd[1]: Finished man-db-cache-update.service.
фев 17 02:31:25 localhost.localdomain systemd[1]: run-r1ecd21fc354d4ea7a5662c5578e55697.service: Deactivated successfully.
фев 17 02:36:30 localhost.localdomain PackageKit[13062]: daemon quit
фев 17 02:36:30 localhost.localdomain systemd[1]: packagekit.service: Deactivated successfully.
фев 17 02:36:30 localhost.localdomain systemd[1]: packagekit.service: Consumed 1.793s CPU time.
фев 17 02:45:25 localhost.localdomain systemd[1]: Starting PackageKit Daemon...
фев 17 02:45:25 localhost.localdomain PackageKit[13627]: daemon start
фев 17 02:45:26 localhost.localdomain systemd[1]: Started PackageKit Daemon.
фев 17 02:45:26 localhost.localdomain PackageKit[13627]: search-file transaction /540_bcbacedb from uid 0 finished with success after 547ms
фев 17 02:46:05 localhost.localdomain PackageKit[13627]: search-file transaction /541_bdaaabba from uid 0 finished with success after 35ms
фев 17 02:49:08 localhost.localdomain systemd[1]: Starting Fingerprint Authentication Daemon...
фев 17 02:49:08 localhost.localdomain systemd[1]: Started Fingerprint Authentication Daemon.
фев 17 02:49:14 localhost.localdomain gdm-password[13728]: gkr-pam: unlocked login keyring
фев 17 02:49:14 localhost.localdomain NetworkManager[818]: <info> [1739749754.5694] agent-manager: agent[62bc482545c87b8b,1.68/org.gnome.Shell.NetworkAgent
фев 17 02:49:38 localhost.localdomain systemd[1]: fprintd.service: Deactivated successfully.
фев 17 02:51:11 localhost.localdomain PackageKit[13627]: daemon quit
фев 17 02:51:11 localhost.localdomain systemd[1]: packagekit.service: Deactivated successfully.
lines 1-20/20 (END)
```

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

```
[root@localhost ~]# journalctl -p err
Feb 16 21:27:33 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:GenuineIntel:12th Gen Intel(R) Core(TM) i5-12450H will not be maintained
Feb 16 21:27:33 localhost systemd[1]: Invalid DMI field header.
Feb 16 21:27:33 localhost kernel: Warning: Unmaintained driver is detected: e1000
Feb 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
Feb 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Feb 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to avoid problems.
Feb 16 21:27:35 localhost systemd[1]: Invalid DMI field header.
Feb 16 21:27:37 localhost alsactl[734]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use case configuration -2
Feb 16 21:27:37 localhost kernel: Warning: Unmaintained driver is detected: ip_set
Feb 16 21:28:03 localhost.localdomain gdm-password[1978]: gkr-pam: unable to locate daemon control file
Feb 16 21:28:08 localhost.localdomain gdm-wayland-session[1032]: GLib: Source ID 2 was not found when attempting to remove it
Feb 16 21:28:08 localhost.localdomain gdm-launch-environment[876]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object)' failed
Feb 17 01:07:06 localhost.localdomain sudo[10761]: bob : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/bob ; USER=root ; COMMAND=/bin/su alice
Feb 17 01:07:26 localhost.localdomain sudo[10779]: bob : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/bob ; USER=root ; COMMAND=su-alice
Feb 17 01:40:33 localhost.localdomain sudo[11371]: pam_unix(sudo:auth): conversation failed
Feb 17 01:40:33 localhost.localdomain sudo[11371]: pam_unix(sudo:auth): auth could not identify password for [alice]
Feb 17 01:40:35 localhost.localdomain sudo[11371]: alice : 1 incorrect password attempt ; TTY=pts/2 ; PWD=/data/main ; USER=root ; COMMAND=/bin/su -carol
Feb 17 02:00:39 localhost.localdomain gdm-password[11857]: gkr-pam: the password for the login keyring was invalid.
```

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@localhost ~]# journalctl --since yesterday
Feb 16 21:27:33 localhost kernel: Linux version 5.14.0-503.23.2.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719)
Feb 16 21:27:33 localhost kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, h
Feb 16 21:27:33 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-503.23.2.el9_5.x86_64 root=/dev/mapper/rhl-root ro crashkernel=1G-4G:19
Feb 16 21:27:33 localhost kernel: BIOS-provided physical RAM map:
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x00000000007ffff000-0x00000000007fffff] ACPI data
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Feb 16 21:27:33 localhost kernel: BIOS-e820: [mem 0x000000000fff00000-0x000000000fffff] reserved
Feb 16 21:27:33 localhost kernel: NX (Execute Disable) protection: active
Feb 16 21:27:33 localhost kernel: APIC: Static calls initialized
Feb 16 21:27:33 localhost kernel: SMBIOS 2.5 present.
Feb 16 21:27:33 localhost kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 16 21:27:33 localhost kernel: Hypervisor detected: KVM
Feb 16 21:27:33 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 16 21:27:33 localhost kernel: kvm-clock: using sched offset of 4864383621 cycles
Feb 16 21:27:33 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Feb 16 21:27:33 localhost kernel: tsc: Detected 2496.004 MHz processor
Feb 16 21:27:33 localhost kernel: e820: update [mem 0x00000000-0x000000fff] usable ==> reserved
Feb 16 21:27:33 localhost kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Feb 16 21:27:33 localhost kernel: last_pfn = 0x7ffff0 max_arch_pfn = 0x400000000
Feb 16 21:27:33 localhost kernel: MTRRs disabled by BIOS
Feb 16 21:27:33 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
Feb 16 21:27:33 localhost kernel: GnuK SMP MP table: 0x00000000-0x000000ff 0x000000ff0-0x000000fff
```

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

```
[root@localhost ~]# journalctl --since yesterday -p err
фев 16 21:27:33 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:GenuineIntel:12th Gen Intel(R) Core(TM) i5-12450H will not be maintained
фев 16 21:27:33 localhost systemd[1]: Invalid DMI field header.
фев 16 21:27:33 localhost kernel: Warning: Unmaintained driver is detected: e1000
фев 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
фев 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
фев 16 21:27:34 localhost kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to avoid problems.
фев 16 21:27:35 localhost systemd[1]: Invalid DMI field header.
фев 16 21:27:37 localhost alsactl[734]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use case configuration -2
фев 16 21:27:37 localhost kernel: Warning: Unmaintained driver is detected: ip_set
фев 16 21:28:03 localhost.localdomain gdm-password[1978]: gkr-pam: unable to locate daemon control file
фев 16 21:28:08 localhost.localdomain gdm-wayland-session[1032]: GLib: Source ID 2 was not found when attempting to remove it
фев 16 21:28:08 localhost.localdomain gdm-launch-environment[876]: GLib-GObject: g_object_unref: assertion 'G_IS_OBJECT (object)' failed
фев 17 01:07:06 localhost.localdomain sudo[10761]: bob : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/bob ; USER=root ; COMMAND=/bin/su alice
фев 17 01:07:26 localhost.localdomain sudo[10779]: bob : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/bob ; USER=root ; COMMAND=su-alice
фев 17 01:40:33 localhost.localdomain sudo[11371]: pam_unix(sudo:auth): conversation failed
фев 17 01:40:33 localhost.localdomain sudo[11371]: pam_unix(sudo:auth): auth could not identify password for [alice]
фев 17 01:40:35 localhost.localdomain sudo[11371]: alice : 1 incorrect password attempt ; TTY=pts/2 ; PWD=/data/main ; USER=root ; COMMAND=/bin/su -carol
фев 17 02:00:39 localhost.localdomain gdm-password[11857]: gkr-pam: the password for the login keyring was invalid.
lines 1-18/18 (END)
```

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

```
[root@localhost ~]# journalctl -o verbose
journalctl: неверный ключ - «0»
[root@localhost ~]# journalctl -o verbose
sun 2025-02-16 21:27:33.486020 MSK [s=e927e32ade4946159e37f149c27c7ec8;i=1;b=653f8f93607143c29007a2c02cefef2b;m=1713cf;t=62e468faf59c4;x=e16495216e1c94b4]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 5.14.0-503.23.2.el9_5.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-5), G
  _BOOT_ID=653f8f93607143c29007a2c02cefef2b
  _MACHINE_ID=fd1db2d5c0c74bffa13d35e97b298403
  _HOSTNAME=localhost
  _RUNTIME_SCOPE=initrd
sun 2025-02-16 21:27:33.486039 MSK [s=e927e32ade4946159e37f149c27c7ec8;i=2;b=653f8f93607143c29007a2c02cefef2b;m=1713e1;t=62e468faf59d7;x=b3d25b235018e839]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=653f8f93607143c29007a2c02cefef2b
  _MACHINE_ID=fd1db2d5c0c74bffa13d35e97b298403
  _HOSTNAME=localhost
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.
sun 2025-02-16 21:27:33.486044 MSK [s=e927e32ade4946159e37f149c27c7ec8;i=3;b=653f8f93607143c29007a2c02cefef2b;m=1713e7;t=62e468faf59dc;x=5d385241fcecff6c]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=653f8f93607143c29007a2c02cefef2b
  _MACHINE_ID=fd1db2d5c0c74bffa13d35e97b298403
  _HOSTNAME=localhost
  _RUNTIME_SCOPE=initrd
```

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

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`

Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Основной файл конфигурации для настройки 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 зависимости от дистрибутива.

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

По умолчанию файлы журналов ротацируются раз в неделю (7 дней) с помощью `logrotate`, если в конфигурации не указано иное.

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

Чтобы записывать все сообщения с приоритетом `info`, добавьте следующую строку в конфигурацию `rsyslog`

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

Команда для просмотра сообщений журнала в режиме реального времени:

`tail -f /var/log/syslog`

или

`journalctl -f`

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

Для просмотра сообщений для PID 1 в указанное время можно использовать:

```
journalctl _PID=1 --since "09:00" --until "15:00"
```

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

Чтобы увидеть сообщения journald после последней перезагрузки, используйте:

```
journalctl -b
```

8. Какая процедура позволяет сделать журнал journald постоянным?

Чтобы сделать журнал journald постоянным, необходимо создать каталог /var/log/journal, если он не существует, и установить необходимые разрешения. Это можно сделать с помощью следующих команд:

```
mkdir -p /var/log/journal
```

```
systemd-tmpfiles --create --prefix /var/log/journal
```

Заключение

Получены навыки работы с журналом событий.