

Отчет о лабораторной работе

Лабораторная работа №7

Казначеев Сергей Ильич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Контрольные вопросы	15
4 Выводы	17

Список иллюстраций

2.1 1	6
2.2 2	6
2.3 3	6
2.4 4	7
2.5 5	7
2.6 6	7
2.7 7	7
2.8 8	8
2.9 9	8
2.10 10	8
2.11 11	9
2.12 12	9
2.13 13	9
2.14 14	9
2.15 15	9
2.16 16	10
2.17 17	10
2.18 18	10
2.19 19	11
2.20 20	11
2.21 21	11
2.22 22	12
2.23 23	12
2.24 24	12
2.25 25	13
2.26 26	13
2.27 27	13
2.28 27	14

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

Для начала откроем три вкладки терминала и в каждом из них получим полномочия администратора (рис. 2.1).

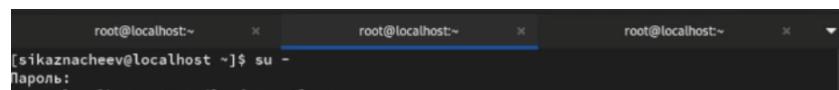
Three terminal windows are shown side-by-side. Each window has a dark header bar with the text 'root@localhost:~'. The first window shows the command '[sikaznacheev@localhost ~]\$ su -' followed by a password prompt 'Пароль:'. The other two windows are blank.

Рис. 2.1: 1

Теперь во второй вкладке пропишем команду tail -f /var/log/messages чтобы вывести события в реальном времени. После чего перейдем в 3 терминал и попробуем зайти в супер пользователя введя неправильный пароль и у нас во 2 терминале появится сообщение «FAILED SU (to root) username ...». (рис. 2.2).

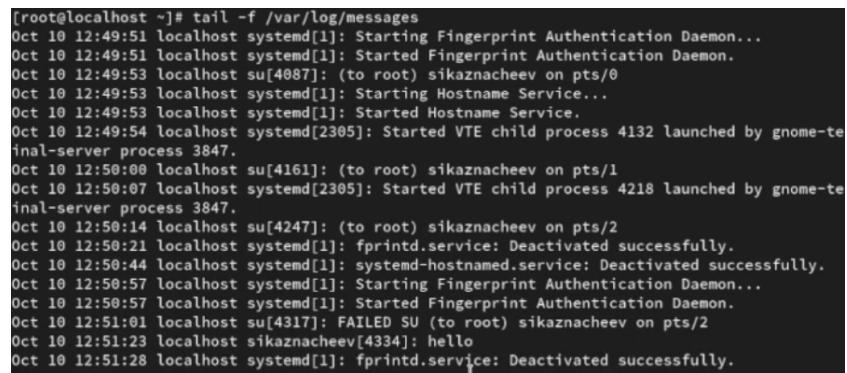
Three terminal windows are shown. The first window shows the command 'tail -f /var/log/messages'. The second window shows the output of this command, which includes several log entries from the system and user activity. The third window shows a failed 'su' command attempt, with the message 'FAILED SU (to root) sikaznacheev' appearing in the log.

Рис. 2.2: 2

После в 3 терминале введем из оболочки пользователя logger hello (рис.2.3).

Three terminal windows are shown. The first window shows the command '[sikaznacheev@localhost ~]\$ logger hello'. The second window shows the command being run. The third window is blank.

Рис. 2.3: 3

Далее открываем второй терминал и проверяя то что hello записалось (рис. 2.4).

```
Oct 10 12:51:23 localhost sikaZNACHEEV[4334]: hello
```

Рис. 2.4: 4

Затем введем команду tail -n 20 /var/log/secure чтобы увидеть сообщения, которые ранее были зафиксированы во время ошибки (рис. 2.5).

```
[root@localhost ~]# tail -n 20 /var/log/secure
```

Рис. 2.5: 5

В первой вкладке установим httpd (рис. 2.6).

```
[root@localhost ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64          15 kB/s | 13 kB     00
Extra Packages for Enterprise Linux 9 - x86_64          6.0 MB/s | 20 MB     00
Rocky Linux 9 - BaseOS      [=====] --- B/s | 0 B     --
```

Рис. 2.6: 6

После окончания процесса установки запустим веб-службу (рис. 2.7).

```
[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.
```

Рис. 2.7: 7

После во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-служб командой tail -f /var/log/httpd/error_log (рис. 2.8).

```
on): session opened for user gdm(uid=42) by (uid=0)
Oct 10 12:37:11 localhost polkitd[879]: Registered Authentication Agent for unix-session:c1 (system bus name :1.26 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: unable to locate daemon control file
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: stashed password to try later in open session
Oct 10 12:39:28 localhost systemd[2305]: pam_unix(systemd-user:session): session opened for user sikaznacheev(uid=1000) by sikaznacheev(uid=0)
Oct 10 12:39:28 localhost gdm-password[2283]: pam_unix(gdm-password:session): session opened for user sikaznacheev(uid=1000) by sikaznacheev(uid=0)
Oct 10 12:39:28 localhost gdm-password[2283]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 12:39:31 localhost polkitd[879]: Registered Authentication Agent for unix-session:2 (system bus name :1.73 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Oct 10 12:39:39 localhost polkitd[879]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.26, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)
Oct 10 12:39:39 localhost gdm-launch-environment[1266]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 10 12:49:53 localhost su[4087]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:00 localhost su[4161]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:14 localhost su[4247]: pam_unix(su-l:session): session opened for user root(uid=0) by sikaznacheev(uid=1000)
Oct 10 12:50:55 localhost su[4247]: pam_unix(su-l:session): session closed for user root
Oct 10 12:50:59 localhost unix_chkpwd[4324]: password check failed for user (root)
Oct 10 12:50:59 localhost su[4317]: pam_unix(su-l:auth): authentication failure; logname=sikaznacheev uid=1000 euid=0 tty=/dev/pts/2 ruser=sikaznacheev rhost= user=root
[root@localhost ~]# tail -f /var/log/httpd/error_log
[Fri Oct 10 12:53:54.282931 2025] [core:notice] [pid 14466:tid 14466] SELinux policy enabled;
httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 10 12:53:54.283326 2025] [suexec:notice] [pid 14466:tid 14466] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
[Fri Oct 10 12:53:54.302928 2025] [lbmethod_heartbeat:notice] [pid 14466:tid 14466] AH02282: No slotmem from mod_heartmonitor
[Fri Oct 10 12:53:54.319963 2025] [mpm_event:notice] [pid 14466:tid 14466] AH00489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 10 12:53:54.319983 2025] [core:notice] [pid 14466:tid 14466] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.8: 8

Далее в 3 терминале запишем в файл конфигурации /etc/httpd/conf/httpd.conf в конце добавим ErrorLog syslog:local1 (рис. 2.9).

```
IncludeOptional conf.d/*.conf

ErrorLog syslog:local1
```

Рис. 2.9: 9

После чего переходим в каталог /etc/rsyslog.d и создаем файл мониторинга событий веб-службы (рис. 2.10).

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

Рис. 2.10: 10

Далее открыв его на редактировании запишем local1.* -/var/log/httpd-error.log

(рис. 2.11).

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

Рис. 2.11: 11

После чего переходим в первую вкладку терминала и перезагружаем конфигурацию rsyslogd и веб-службу (рис. 2.12).

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

Рис. 2.12: 12

После в третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации и в том же терминале вводим echo “*.debug /var/log/messages-debug” > /etc/rsyslog.d/debug.conf

```
[root@localhost ~]# cd /etc/rsyslog.d
[root@localhost rsyslog.d]# touch debug.conf
[root@localhost rsyslog.d]# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
-bash: /etc/rsyslog.d/debug.conf: Отказано в доступе
[root@localhost rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@localhost rsyslog.d]#
```

Рис. 2.13: 13

Затем в первой вкладке терминала снова перезапускаем rsyslogd (рис. 2.14).

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

Рис. 2.14: 14

Далее переходим во вторую вкладку терминала запускаем мониторинг отладочной информации tail -f /var/log/messages-debug (рис. 2.15).

```
^C
[root@localhost ~]# tail -f /var/log/messages-debug
```

Рис. 2.15: 15

Далее в третьей вкладке терминала введем logger -p daemon.debug "Daemon Debug Message"

```
[root@localhost rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
[root@localhost rsyslog.d]#
```

Рис. 2.16: 16

Проверим это (рис. 2.17).

```
Oct 10 13:00:39 localhost root[46274]: Daemon Debug Message
```

Рис. 2.17: 17

Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы (рис. 2.18).

```
OKT 10 12:36:43 localhost kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iad1-1)
OKT 10 12:36:43 localhost kernel: The list of certified hardware and cloud instances for Enter
OKT 10 12:36:43 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37
OKT 10 12:36:43 localhost kernel: BIOS-provided physical RAM map:
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usab
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reser
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000f0000-0x00000000000ffff] reser
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfefffff] usab
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reser
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000fee0ffff] reser
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reser
OKT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000100000000-0x0000000021fffffff] usab
OKT 10 12:36:43 localhost kernel: NX (Execute Disable) protection: active
OKT 10 12:36:43 localhost kernel: APIC: Static calls initialized
OKT 10 12:36:43 localhost kernel: SMBIOS 2.5 present.
OKT 10 12:36:43 localhost kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12
OKT 10 12:36:43 localhost kernel: Hypervisor detected: KVM
OKT 10 12:36:43 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
OKT 10 12:36:43 localhost kernel: kvm-clock: using sched offset of 6225533528 cycles
OKT 10 12:36:43 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles
OKT 10 12:36:43 localhost kernel: tsc: Detected 3686.398 MHz processor
OKT 10 12:36:43 localhost kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
OKT 10 12:36:43 localhost kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
OKT 10 12:36:43 localhost kernel: last_pfn = 0x220000 max_arch_pfn = 0x400000000
OKT 10 12:36:43 localhost kernel: MTRRs disabled by BIOS
OKT 10 12:36:43 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- W
OKT 10 12:36:43 localhost kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
OKT 10 12:36:43 localhost kernel: found SMP MP-table at [mem 0x0009ff0-0x0009ffff]
OKT 10 12:36:43 localhost kernel: RAMDISK: [mem 0x30c7b000-0x34635fff]
OKT 10 12:36:43 localhost kernel: ACPI: Early table checksum verification disabled
OKT 10 12:36:43 localhost kernel: ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX )
OKT 10 12:36:43 localhost kernel: ACPI: XSDT 0x00000000DFF0030 00003C (v01 VBOX VBOXXSDT 0
OKT 10 12:36:43 localhost kernel: ACPI: FACP 0x00000000DFF00F0 0000F4 (v04 VBOX VBOXFACP 0
OKT 10 12:36:43 localhost kernel: ACPI: DSDT 0x00000000DFF0640 002353 (v02 VBOX VBOXBIOS 0
OKT 10 12:36:43 localhost kernel: ACPI: FACS 0x00000000DFF0200 000040
OKT 10 12:36:43 localhost kernel: ACPI: FACS 0x00000000DFF0200 000040
OKT 10 12:36:43 localhost kernel: ACPI: APIC 0x00000000DFF0240 00008C (v02 VBOX VBOXAPIC 0
OKT 10 12:36:43 localhost kernel: ACPI: SSDT 0x00000000DFF02D0 00036C (v01 VBOX VBOXCPUT 0
OKT 10 12:36:43 localhost kernel: ACPI: Reserving FACP table memory at [mem 0xdffff00f0-0xdffff
OKT 10 12:36:43 localhost kernel: ACPI: Reserving DSDT table memory at [mem 0xdffff0640-0xdffff
OKT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdffff0200-0xdffff
OKT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdffff0200-0xdffff
OKT 10 12:36:43 localhost kernel: ACPI: Reserving APIC table memory at [mem 0xdffff0240-0xdffff
```

Рис. 2.18: 18

Затем просмотрим содержимое журнала без использования пейджера командой journalctl -no-pager и просмотрим журнал в реальном времени journalctl -f

(рис. 2.19).

```
[OKT 10 12:58:08 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 12:58:08 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 12:58:08 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46035" x-info="https://www.rsyslog.com"] start
OKT 10 12:58:08 localhost.localdomain rsyslogd[46035]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
OKT 10 12:58:15 localhost.localdomain systemd[1]: Stopping The Apache HTTP Server...
OKT 10 12:58:16 localhost.localdomain systemd[1]: httpd.service: Deactivated successfully.
OKT 10 12:58:16 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
OKT 10 12:58:16 localhost.localdomain systemd[1]: httpd.service: Consumed 1.264s CPU time.
OKT 10 12:58:17 localhost.localdomain httpd[46046]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
OKT 10 12:58:17 localhost.localdomain httpd[46046]: Server configured, listening on: port 80
OKT 10 12:58:17 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
OKT 10 12:59:31 localhost.localdomain PackageKit[4923]: daemon quit
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Deactivated successfully .
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Consumed 19.543s CPU time.
OKT 10 13:00:01 localhost.localdomain gnome-shell[2391]: libinput error: client bug: timer event5 debounce short: scheduled expiry is in the past (-12ms), your system is too slow
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopping System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46035" x-info="https://www.rsyslog.com"] exiting on signal 15.
OKT 10 13:00:04 localhost.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopped System Logging Service.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="46265" x-info="https://www.rsyslog.com"] start
OKT 10 13:00:04 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
OKT 10 13:00:39 localhost.localdomain root[46274]: Daemon Debug Message
OKT 10 13:01:01 localhost.localdomain CROND[46284]: (root) CMD (run-parts /etc/cron.hourly)
OKT 10 13:01:01 localhost.localdomain run-parts[46287]: (/etc/cron.hourly) starting @anacron
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Anacron started on 2025-10-10
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.daily' in 19 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.weekly' in 39 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.monthly' in 59 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Jobs will be executed sequentially
OKT 10 13:01:01 localhost.localdomain run-parts[46299]: (/etc/cron.hourly) finished @anacron
OKT 10 13:01:01 localhost.localdomain CROND[46283]: (root) CMDEND (run-parts /etc/cron.hourly)
[root@localhost ~]#
```

Рис. 2.19: 19

После чего используем фильтрацию просмотра конкретных параметров журнала введя команду journalctl и дважды нажав на tab

```
[root@localhost ~]# journalctl
Display all 107 possibilities? (y or n)
```

Рис. 2.20: 20

Пробуем просмотреть события для uid0

```
[root@localhost ~]# journalctl _UID=0
```

Рис. 2.21: 21

После чего запустим journalctl -n 20 для просмотра только сообщений об ошибке используем комаду journalctl -p err

```
[root@localhost ~]# journalctl -n 20
OKT 10 12:59:31 localhost.localdomain systemd[1]: packagekit.service: Consumed 19.543s CPU time.
OKT 10 13:00:01 localhost.localdomain gnome-shell[2391]: libinput error: client bug: timer ev...
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopping System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46035]: [origin software="rsyslogd" swVersion="9...
OKT 10 13:00:04 localhost.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
OKT 10 13:00:04 localhost.localdomain systemd[1]: Stopped System Logging Service...
OKT 10 13:00:04 localhost.localdomain systemd[1]: Starting System Logging Service...
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: [origin software="rsyslogd" swVersion="9...
OKT 10 13:00:04 localhost.localdomain systemd[1]: Started System Logging Service.
OKT 10 13:00:04 localhost.localdomain rsyslogd[46265]: imjournal: journal files changed, relo...
OKT 10 13:00:39 localhost.localdomain root[46274]: Daemon Debug Message
OKT 10 13:01:01 localhost.localdomain CROND[46284]: (root) CMD (run-parts /etc/cron.hourly)
OKT 10 13:01:01 localhost.localdomain run-parts[46287]: (/etc/cron.hourly) starting @anacron
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Anacron started on 2025-10-10
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.daily' in 19 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.weekly' in 39 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Will run job 'cron.monthly' in 59 min.
OKT 10 13:01:01 localhost.localdomain anacron[46297]: Jobs will be executed sequentially
OKT 10 13:01:01 localhost.localdomain run-parts[46299]: (/etc/cron.hourly) finished @anacron
OKT 10 13:01:01 localhost.localdomain CROND[46283]: (root) CMDEND (run-parts /etc/cron.hourly)
[root@localhost ~]# journalctl -p err
OKT 10 12:36:43 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:Genuine...
OKT 10 12:36:43 localhost systemd[1]: Invalid DMI field header.
OKT 10 12:36:44 localhost kernel: Warning: Unmaintained driver is detected: e1000
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ vmwgfx seems to be running
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ This configuration is likely to cause problems
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ Please switch to a supported configuration
OKT 10 12:36:51 localhost systemd[1]: Invalid DMI field header.
OKT 10 12:36:53 localhost systemd-udevd[732]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 >
OKT 10 12:36:53 localhost systemd-udevd[740]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 >
OKT 10 12:36:58 localhost alsactl[928]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: file ...
OKT 10 12:37:01 localhost.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
OKT 10 12:39:28 localhost.localdomain gdm-password[2283]: gkr-pam: unable to locate daemon configuration file
OKT 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by gdm-launch-environment
OKT 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by gdm-launch-environment
OKT 10 12:39:38 localhost.localdomain gdm-wayland-session[1318]: GLib: Source ID 2 was not fo...
OKT 10 12:39:39 localhost.localdomain gdm-launch-environment[1266]: GLib-GObject: g_object_unref()
lines 1-16/16 (END)
```

Рис. 2.22: 22

Теперь просмотрим сообщений вчерашнего дня введя команду journalctl --since yesterday

```
[root@localhost ~]# journalctl --since yesterday
```

Рис. 2.23: 23

Затем выведем все сообщения с ошибкой приоритета которые были зафиксированы со вчерашнего дня

```
[root@localhost ~]# journalctl --since yesterday -p err
OKT 10 12:36:43 localhost kernel: Warning: Deprecated Hardware is detected: x86_64-v2:Genuine...
OKT 10 12:36:43 localhost systemd[1]: Invalid DMI field header.
OKT 10 12:36:44 localhost kernel: Warning: Unmaintained driver is detected: e1000
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ vmwgfx seems to be running
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ This configuration is likely to cause problems
OKT 10 12:36:46 localhost kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ Please switch to a supported configuration
OKT 10 12:36:51 localhost systemd[1]: Invalid DMI field header.
OKT 10 12:36:53 localhost systemd-udevd[732]: vboxuser: /etc/udev/rules.d/60-vboxadd.rules:2 >
OKT 10 12:36:53 localhost systemd-udevd[740]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 >
OKT 10 12:36:58 localhost alsactl[928]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: file ...
OKT 10 12:37:01 localhost.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
OKT 10 12:39:28 localhost.localdomain gdm-password[2283]: gkr-pam: unable to locate daemon configuration file
OKT 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by gdm-launch-environment
OKT 10 12:39:29 localhost.localdomain systemd[2305]: Failed to start Application launched by gdm-launch-environment
OKT 10 12:39:38 localhost.localdomain gdm-wayland-session[1318]: GLib: Source ID 2 was not fo...
OKT 10 12:39:39 localhost.localdomain gdm-launch-environment[1266]: GLib-GObject: g_object_unref()
lines 1-16/16 (END)
```

Рис. 2.24: 24

Затем выведем детальную информацию с помощью команды journalctl -o verbose

```
OKT 10 12:39:39 localhost.localdomain gdm-ta
[root@localhost ~]# journalctl -o verbose
```

Рис. 2.25: 25

Далее просмотрим дополнительную информацию о модуле sshd введя команду journalctl _SYSTEMD_UNIT=sshd.service

```
[root@localhost ~]# journalctl _SYSTEMD_UNIT=sshd.service
OKT 10 12:37:02 localhost.localdomain sshd[1226]: Server listening on 0.0.0.0 port 22.
OKT 10 12:37:02 localhost.localdomain sshd[1226]: Server listening on :: port 22.
[root@localhost ~]#
```

Рис. 2.26: 26

После чего откроем новый терминал и создадим новый каталог и скорректируем его права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию и для принятия изменений необходимо перезагрузить систему или использовать команду killall SR1 systemd-journald

```
[root@localhost ~]# mkdir -p /var/log/journal
[root@localhost ~]# chown root:systemd-journal /var/log/journal
[root@localhost ~]# chmod 2755 /var/log/journal
[root@localhost ~]# killall -USR1 systemd-journald
[root@localhost ~]#
```

Рис. 2.27: 27

Теперь журнал systemd теперь постоянный и можем проверить это командой journalctl -b

```

[KT 10 12:36:43 localhost kernel: Linux version 5.14.0-570.37.1.el9_6.x86_64 (mockbuild@iadi-prod-build001.bld.equinor.no)
[KT 10 12:36:43 localhost kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be vi...
[KT 10 12:36:43 localhost kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.37.1.el9_6.x86_64 root=/dev...
[KT 10 12:36:43 localhost kernel: BIOS-provided physical RAM map:
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usable
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x00000000000fffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000000fffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffffff] usable
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000dfft0000-0x0000000000fe00fff] ACPI data
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x00000000fffff] reserved
[KT 10 12:36:43 localhost kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x00000000fffff] reserved
[KT 10 12:36:43 localhost kernel: NX (Execute Disable) protection: active
[KT 10 12:36:43 localhost kernel: APIC: static calls initialized
[KT 10 12:36:43 localhost kernel: SMBIOS 2.5 present.
[KT 10 12:36:43 localhost kernel: DMI: innotele GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[KT 10 12:36:43 localhost kernel: Hypervisor detected: KVM
[KT 10 12:36:43 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
[KT 10 12:36:43 localhost kernel: kvm-clock: using sched offset of 6225335328 cycles
[KT 10 12:36:43 localhost kernel: clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd42e4dff, max_idl...
[KT 10 12:36:43 localhost kernel: tsc: Detected 3080.399 MHz processor
[KT 10 12:36:43 localhost kernel: e820: update [mem 0x00000000-0x000000ff] usable ==> reserved
[KT 10 12:36:43 localhost kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
[KT 10 12:36:43 localhost kernel: last_pfn = 0x220000 max_arch_pfn = 0x4000000000
[KT 10 12:36:43 localhost kernel: MTRRs disabled by BIOS
[KT 10 12:36:43 localhost kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- NT
[KT 10 12:36:43 localhost kernel: last_pfn = 0xe0000 max_arch_pfn = 0x4000000000
[KT 10 12:36:43 localhost kernel: found SMP MP-table at [mem 0x0009ff00-0x0009ffff]
[KT 10 12:36:43 localhost kernel: RANDISK: [mem 0x30c7b000-0x34635fff]
[KT 10 12:36:43 localhost kernel: ACPI: Early table checksum verification disabled
[KT 10 12:36:43 localhost kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
[KT 10 12:36:43 localhost kernel: ACPI: XSDT 0x0000000000000030 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
[KT 10 12:36:43 localhost kernel: ACPI: FACP 0x0000000000FF00F0 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
[KT 10 12:36:43 localhost kernel: ACPI: DSDT 0x0000000000FF0040 002353 (v02 VBOX VBOXBIOS 00000002 INTL 20100528)
[KT 10 12:36:43 localhost kernel: ACPI: FACS 0x0000000000FF0200 000040
[KT 10 12:36:43 localhost kernel: ACPI: FACS 0x0000000000FF0200 000040
[KT 10 12:36:43 localhost kernel: ACPI: APIC 0x0000000000FF0240 000008 (v02 VBOX VBOXAPIC 00000001 ASL 00000061)
[KT 10 12:36:43 localhost kernel: ACPI: SSDT 0x0000000000FF02D0 00036C (v01 VBOX VBOXCPUT 00000002 INTL 20100528)
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACP table memory at [mem 0xdfff00f0-0xdfff01e3]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving DSDT table memory at [mem 0xdfff0640-0xdfff2992]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving FACS table memory at [mem 0xdfff0200-0xdfff023f]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving APIC table memory at [mem 0xdfff0240-0xdfff02cb]
[KT 10 12:36:43 localhost kernel: ACPI: Reserving SSDT table memory at [mem 0xdfff02d0-0xdfff063b]
[KT 10 12:36:43 localhost kernel: No NUMA configuration found
[KT 10 12:36:43 localhost kernel: Faking a node at [mem 0x0000000000000000-0x0000000021fffff]
[KT 10 12:36:43 localhost kernel: NODE_DATA(0) allocated [mem 0x21ffd1000-0x21ffbffff]
[KT 10 12:36:43 localhost kernel: crashkernel reserved: 0x00000000c0f00000 - 0x000000000df000000 (256 MB)
[KT 10 12:36:43 localhost kernel: Zone ranges:
[KT 10 12:36:43 localhost kernel: DMA [mem 0x0000000000000000-0x00000000000fffff]
[KT 10 12:36:43 localhost kernel: DMA32 [mem 0x0000000000100000-0x0000000000fffff]
[KT 10 12:36:43 localhost kernel: Normal [mem 0x0000000010000000-0x0000000021fffff]
[KT 10 12:36:43 localhost kernel: Device empty
[KT 10 12:36:43 localhost kernel: Movable zone start for each node

```

Рис. 2.28: 27

3 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd?

Ответ - файл /etc/rsyslog.conf

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

Ответ - файл журнала айнтефекации /var/log/auth.log

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

Ответ - период ротации журналов по умолчанию раз в неделю

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

Ответ - строку /var/log/message.info

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

Ответ - команда tail -f /var/log/syslog

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

Ответ - команда journalctl _PID=1 –since “9:00” –until “15:00”

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

Ответ - команда journalctl -b

8. Какая процедура позволяет сделать журнал journald постоянным?

Ответ - команда создать каталог и перезапустить службу mkdir -p /var/log/journal
systemctl restart systemd-journald

4 Выводы

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