

Презентация по лабораторной работе №7

Управление журналами событий в системе

Агджабекова Эся Рустамовна

2 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

Ход выполнения работы

Мониторинг системных событий

```
Sep 29 10:48:46 eragdzhabekova systemd-coredump[3997]: Process 3993 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:48:46 eragdzhabekova systemd[1]: Started systemd-coredump@77-3997-0.service - Process Core Dump (PID 3997/UID 0).
Sep 29 10:48:46 eragdzhabekova systemd-coredump[3998]: Process 3993 (VBoxClient) of user 1000 dumped core. #012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 3996:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x0000000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3994:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000450bf0 n/a (n/a + 0x0)#012#3 0x000000000043566a n/a (n/a + 0x0)#012#4 0x000000000045041c n/a (n/a + 0x0)#012#5 0x00000000004355d0 n/a (n/a + 0x0)#012#6 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#7 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3993:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x000000000045123 n/a (n/a + 0x0)#012#4 0x00007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:48:46 eragdzhabekova systemd[1]: systemd-coredump@77-3997-0.service: Deactivated successfully.
Sep 29 10:48:51 eragdzhabekova kernel: traps: VBoxClient[4007] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 29 10:48:51 eragdzhabekova systemd-coredump[4008]: Process 4004 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:48:51 eragdzhabekova systemd[1]: Started systemd-coredump@78-4008-0.service - Process Core Dump (PID 4008/UID 0).
Sep 29 10:48:51 eragdzhabekova systemd-coredump[4009]: Process 4004 (VBoxClient) of user 1000 dumped core. #012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4007:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x0000000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4004:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x000000000045123 n/a (n/a + 0x0)#012#4 0x00007f31747d530e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:48:51 eragdzhabekova systemd[1]: systemd-coredump@78-4008-0.service: Deactivated successfully.
```

Ошибка авторизации и команда logger

```
le libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4078:#012#0 0x0000000000041dd1b n/a (n/a + 0x0)#012#1 0x0000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4076:#012#0 0x00007f31748ea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000000434c30 n/a (n/a + 0x0)#012#2 0x0000000000450bfb n/a (n/a + 0x0)#012#3 0x000000000043566a n/a (n/a + 0x0)#012#4 0x000000000045041c n/a (n/a + 0x0)#012#5 0x00000000004355d0 n/a (n/a + 0x0)#012#6 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#7 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4077:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000416559 n/a (n/a + 0x0)#012#4 0x0000000000404860 n/a (n/a + 0x0)#012#5 0x0000000000417d6a n/a (n/a + 0x0)#012#6 0x0000000000404860 n/a (n/a + 0x0)#012#7 0x000000000045041c n/a (n/a + 0x0)#012#8 0x00000000004355d0 n/a (n/a + 0x0)#012#9 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#10 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4075:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:17 eragdzhabekova systemd[1]: systemd-coredump@83-4079-0.service: Deactivated successfully.
Sep 29 10:49:17 eragdzhabekova su[4065]: FAILED SU (to root) eragdzhabekova on pts/2
Sep 29 10:49:22 eragdzhabekova kernel: traps: VBoxClient[4090] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 29 10:49:22 eragdzhabekova systemd-coredump[4091]: Process 4087 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:22 eragdzhabekova systemd[1]: Started systemd-coredump@84-4091-0.service - Process Core Dump (PID 4091/UID 0).
Sep 29 10:49:22 eragdzhabekova systemd-coredump[4092]: Process 4087 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4090:#012#0 0x0000000000041dd1b n/a (n/a + 0x0)#012#1 0x0000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4087:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:22 eragdzhabekova systemd[1]: systemd-coredump@84-4091-0.service: Deactivated successfully.
```

Сообщение через logger

```
n/a (n/a + 0x0)#012#7 0x000000000045041c n/a (n/a + 0x0)#012#8 0x00000000004355d0 n/a (n/a + 0x0)#012#9 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#10 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4117:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:37 eragdzhabekova systemd[1]: systemd-coredump@87-4121-0.service: Deactivated successfully.
Sep 29 10:49:40 eragdzhabekova eragdzhabekova[4127]: hello
Sep 29 10:49:42 eragdzhabekova kernel: traps: VBoxClient[4132] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 29 10:49:42 eragdzhabekova systemd-coredump[4133]: Process 4129 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:42 eragdzhabekova systemd[1]: Started systemd-coredump@88-4133-0.service - Process Core Dump (PID 4133/UID 0).
Sep 29 10:49:42 eragdzhabekova systemd-coredump[4134]: Process 4129 (VBoxClient) of user 1000 dumped core.#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libXi1.so.6 from rpm libXi1-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4132:#012#0 0x000000000041dc1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045041c n/a (n/a + 0x0)#012#3 0x00000000
```

Рис. 3: Сообщение, записанное с помощью logger

Просмотр журнала secure

```
root@eragdzhabekova:/home/eragdzhabekova# tail -n 20 /var/log/messages
Sep 29 10:49:52 eragdzhabekova kernel: traps: VBoxClient[4156] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 29 10:49:52 eragdzhabekova systemd-coredump[4157]: Process 4153 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:52 eragdzhabekova systemd[1]: Started systemd-coredump@90-4157-0.service - Process Core Dump (PID 4157/UID 0).
Sep 29 10:49:52 eragdzhabekova systemd-coredump[4158]: Process 4153 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4156:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)#012#1 0x00000000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000000045041c n/a (n/a + 0x0)#012#3 0x0000000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4154:#012#0 0x000007f31748aea3d syscall (libc.so.6 + 0x103a3d) #012#1 0x000000000000434c30 n/a (n/a + 0x0)#012#2 0x000000000000450bfb n/a (n/a + 0x0)#012#3 0x00000000000043566a n/a (n/a + 0x0)#012#4 0x00000000000045041c n/a (n/a + 0x0)#012#5 0x0000000000004355d0 n/a (n/a + 0x0)#012#6 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#7 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4155:#012#0 0x000007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000416559 n/a (n/a + 0x0)#012#4 0x00000000000041838a n/a (n/a + 0x0)#012#5 0x000000000000417d6a n/a (n/a + 0x0)#012#6 0x000000000000404860 n/a (n/a + 0x0)#012#7 0x00000000000045041c n/a (n/a + 0x0)#012#8 0x0000000000004355d0 n/a (n/a + 0x0)#012#9 0x000007f317484011a start_thread (libc.so.6 + 0x9511a)#012#10 0x000007f31748b0c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 4153:#012#0 0x000007f31748aea3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000000450066 n/a (n/a + 0x0)#012#3 0x000000000000405123 n/a (n/a + 0x0)#012#4 0x000007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x000007f31747d53c __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Sep 29 10:49:52 eragdzhabekova systemd[1]: systemd-coredump@90-4157-0.service: Deactivated successfully.
Sep 29 10:49:57 eragdzhabekova kernel: traps: VBoxClient[4166] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Sep 29 10:49:57 eragdzhabekova systemd-coredump[4167]: Process 4163 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Sep 29 10:49:57 eragdzhabekova systemd[1]: Started systemd-coredump@91-4167-0.service - Process Core Dump (PID 4167/UID 0).
Sep 29 10:49:57 eragdzhabekova systemd-coredump[4168]: Process 4163 (VBoxClient) of user 1000 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 4162:#012#0 0x00000000000041dd1b n/a (n/a + 0x0)
```

Рис. 4: Просмотр сообщений безопасности

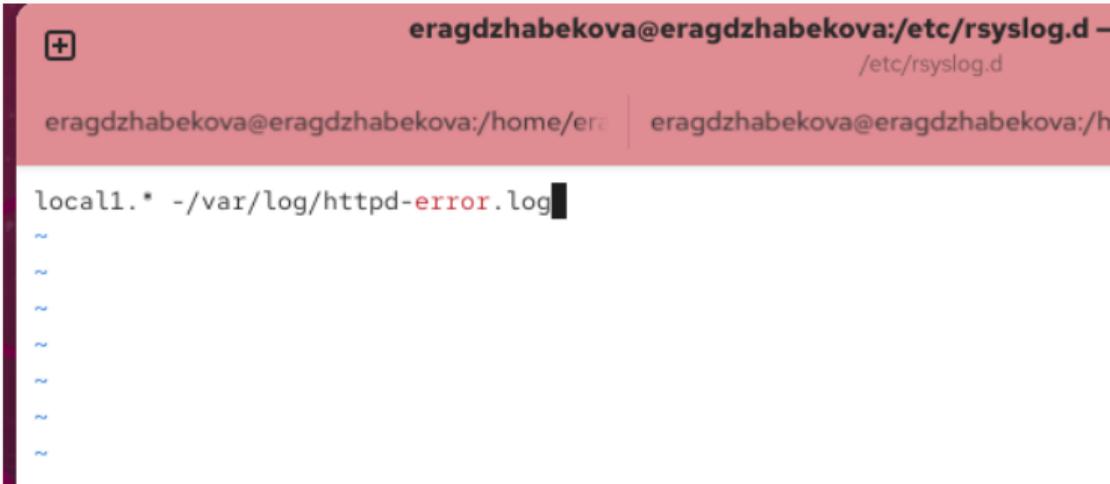
Установка и запуск Apache

```
Running scriptlet: httpd-2.4.63-1.el10_0.2.x86_64                                         11/11
Installed:
  apr-1.7.5-2.el10.x86_64                  apr-util-1.6.3-21.el10.x86_64                  apr-util-lmdb-1.6.3-21.el10.x86_64
  apr-util-openssl-1.6.3-21.el10.x86_64    httpd-2.4.63-1.el10_0.2.x86_64                httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch httpd-tools-2.4.63-1.el10_0.2.x86_64   mod_http2-2.0.29-2.el10_0.1.x86_64
  mod_lua-2.4.63-1.el10_0.2.x86_64          rocky-logos-httpd-100.4-7.el10.noarch

Complete!
root@eragdzhabekova:/home/eragdzhabekova# systemctl start httpd
root@eragdzhabekova:/home/eragdzhabekova# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
root@eragdzhabekova:/home/eragdzhabekova#
```

Рис. 5: Установка и запуск Apache

Перенаправление ошибок Apache в syslog



The screenshot shows a terminal window with a red header bar. The header bar contains the text "eragdzhabekova@eragdzhabekova:/etc/rsyslog.d – /etc/rsyslog.d". Below the header, there are two tabs: "eragdzhabekova@eragdzhabekova:/home/eragdzhabekova" and "eragdzhabekova@eragdzhabekova:/etc/rsyslog.d". The main pane of the terminal displays the following configuration line:

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

The line is preceded by several blue tilde (~) characters, indicating it is part of a multi-line configuration block.

Рис. 6: Добавление правила ErrorLog в httpd.conf

Настройка rsyslog для ошибок Apache

```
#  
# 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  
-- INSERT --
```

Отладочные сообщения через rsyslog

```
0004355d0 n/a (n/a + 0x0)#012#4 0x00007f317484011a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007f31748b0c3c  
ne3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 6254:#012#0 0x00007f31748aea3d syscall (libc.so.6 + 0x10  
#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/  
a + 0x0)#012#4 0x00007f31747d530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f31747d53c9 __libc_  
_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary architectu  
MD x86-64  
Sep 29 10:58:45 eragdzhabekova systemd[1]: systemd-coredump@195-6258-0.service: Deactivated successfully.  
Sep 29 10:58:49 eragdzhabekova root[6264]: Daemon Debug MEssage  
Sep 29 10:58:50 eragdzhabekova kernel: traps: VBoxClient[6269] trap int3 ip:41dd1b sp:7f3166188cd0 error:0 in VBo  
nt[1dd1b,400000+bb000]  
Sep 29 10:58:50 eragdzhabekova systemd-coredump[6270]: Process 6266 (VBoxClient) of user 1000 terminated abnormal  
ly signal 5/TRAP, processing...  
Sep 29 10:58:50 eragdzhabekova systemd[1]: Started systemd-coredump@196-6270-0.service - Process Core Dump (PID 6  
ID 0).  
Sep 29 10:58:50 eragdzhabekova systemd-coredump[6271]: Process 6266 (VBoxClient) of user 1000 dumped core.#012#01
```

Рис. 8: Вывод отладочного сообщения через logger

Использование journalctl

```
root@eragdzhabekova:/home/eragdzhabekova# journalctl
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000100000-0x0000000007fffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000007ff0000-0x0000000007fffff] ACPI data
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: APIC: Static calls initialized
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: SMBIOS 2.5 present.
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: Memory slots populated: 0/0
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Hypervisor detected: KVM
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: kvm-clock: using sched offset of 4050277964 cycles
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: clocksource: kvm-clock: mask: 0xfffffffffffffff max_cycles: 0x1cd
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: tsc: Detected 3187.202 MHz processor
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: last_pfn = 0x80000 max_arch_pfn = 0x40000000
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 35), built from 16
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC UC WB WP UC- WT
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: found SMP MP-table at [mem 0x0009fbff-0x0009fbff]
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Incomplete global flushes, disabling PCID
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: RAMDISK: [mem 0x34338000-0x36193fff]
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: Early table checksum verification disabled
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: RSDP 0x0000000000E0000 000024 (v02 VBOX )
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: XSDT 0x000000007FF0030 00003C (v01 VBOX   VBOXXSDT 00000001)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: FACP 0x000000007FFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001)
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: ACPI: DSDT 0x000000007EE5E610 0022E2 (v02 VBOX   VBOXNDTCS 00000001)
```

Рис. 9: Просмотр журнала с момента запуска

Фильтрация в journalctl

```
root@eragdzhabekova:/home/eragdzhabekova# journalctl -p err
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* vmmwgfx seems to be running on a
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely br
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: vmmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported gr
Sep 29 10:41:58 eragdzhabekova.localdomain kernel: Warning: Unmaintained driver is detected: el000
Sep 29 10:41:59 eragdzhabekova.localdomain alsactl[875]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to
Sep 29 10:41:59 eragdzhabekova.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Sep 29 10:42:09 eragdzhabekova.localdomain gdm-password[1896]: gkr-pam: unable to locate daemon control file
Sep 29 10:42:12 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-xdg\x2duser\x2ddirs-2034.scope -
Sep 29 10:42:13 eragdzhabekova.localdomain systemd[1908]: Failed to start app-gnome-vmware\x2duser-2235.scope - Appli
Sep 29 10:42:14 eragdzhabekova.localdomain systemd-coredump[2699]: [..] Process 2693 (VBoxClient) of user 1000 dumped
Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64
Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64
Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64
Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64
Module libwayland-client.so.0 from rpm wayland-1.22.0-1.el10.x86_64
Stack trace of thread 2697:
#0 0x000000000041dd1b n/a (n/a + 0x0)
#1 0x000000000041dc94 n/a (n/a + 0x0)
#2 0x000000000045041c n/a (n/a + 0x0)
#3 0x00000000004355d0 n/a (n/a + 0x0)
#4 0x00007f317484011a start_thread (libc.so.6 + 0x105)
#5 0x00007f31748b0c3c __clone3 (libc.so.6 + 0x105)

Stack trace of thread 2695:
#0 0x00007f31748aea3d syscall (libc.so.6 + 0x103a)
#1 0x0000000000434c30 n/a (n/a + 0x0)
#2 0x0000000000450fb0 n/a (n/a + 0x0)
#3 0x000000000043566a n/a (n/a + 0x0)
#4 0x000000000045041c n/a (n/a + 0x0)
```

Рис. 10: Фильтрация ТОЛЬКО ОШИБОК

Постоянный журнал journald

```
root@eragdzhabekova:/home/eragdzhabekova# mkdir -p /var/log/journal
root@eragdzhabekova:/home/eragdzhabekova# chown root:systemd-journal /var/log/journal/
root@eragdzhabekova:/home/eragdzhabekova# chmod 2755 /var/log/journal/
root@eragdzhabekova:/home/eragdzhabekova# killall -USR1 systemd-journald
root@eragdzhabekova:/home/eragdzhabekova# journalctl -b
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-bu...
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0...
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-provided physical RAM map:
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000000000100000-0x00000000007fffffff] usable
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x000000007ffff000-0x000000007fffffff] ACPI data
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: BIOS-e820: [mem 0x00000000ffffc0000-0x00000000ffffcfffff] reserved
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: NX (Execute Disable) protection: active
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: APIC: Static calls initialized
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: SMBIOS 2.5 present.
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 10:41:55 eragdzhabekova.localdomain kernel: DMI: Memory slots populated: 0/0
```

Рис. 11: Включение постоянного журнала journald

Итоги работы

Вывод

В ходе лабораторной работы были изучены принципы работы с системными журналами в Linux.

Рассмотрена настройка rsyslog, перенаправление сообщений Apache и отладочных логов.

Освоено использование `journalctl` с фильтрацией и настройка постоянного журнала `journald`.

Получены практические навыки администрирования системных журналов.