

Лабораторная работа №7

Управление журналами событий в системе

Эзиз Хатамов

4 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе Linux и изучить инструменты **rsyslog** и **systemd-journald**.

Ход выполнения работы

Мониторинг системных событий

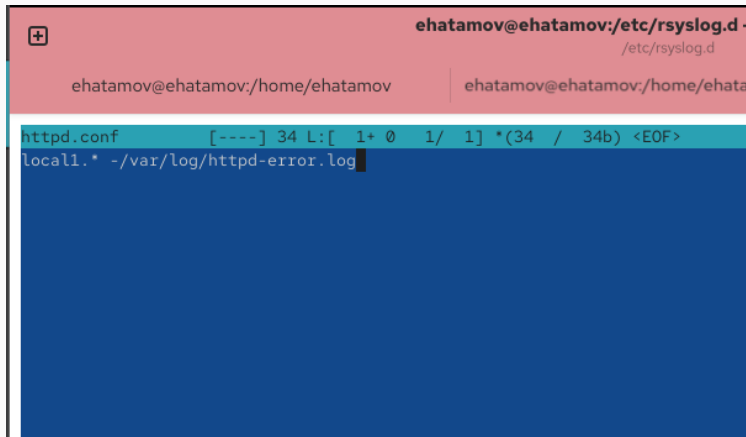
- Запущен мониторинг событий в реальном времени с помощью:
- Проверена фиксация событий при ошибках авторизации и при вводе `logger hello`
- Анализ журнала `/var/log/secure` подтвердил регистрацию всех действий

```
root@ehatamov:/home/ehatamov# tail -f /var/log/messages
Oct  2 17:03:43 ehatamov systemd[1992]: Starting gvfs-metadata.service - Virtual filesystem metadata service...
Oct  2 17:03:43 ehatamov systemd[1992]: Started gvfs-metadata.service - Virtual filesystem metadata service.
Oct  2 17:03:44 ehatamov PackageKit[1407]: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Oct  2 17:03:44 ehatamov PackageKit[1407]: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Oct  2 17:03:44 ehatamov systemd[1]: fprintd.service: Deactivated successfully.
Oct  2 17:03:45 ehatamov kernel: traps: VBoxClient[3408] trap int3 ip:41ddb sp:7fdadef4fcd0 error:0 in VBoxClient[1ddb,400000+bb000]
Oct  2 17:03:45 ehatamov systemd-coredump[3409]: Process 3405 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Oct  2 17:03:45 ehatamov systemd[1]: Started systemd-coredump@12-3409-0.service - Process Core Dump (PID 3409/UID 0).
Oct  2 17:03:45 ehatamov systemd-coredump[3410]: Process 3405 (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 3408:#012#0 0x00000000041ddb n/a (n/a + 0x0)#012#1 0x00000000041dc94 n/a (n/a + 0x0)#012#2 0x00000000045041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x00007fdaed5f211a start_thread (libc.so.6 + 0x9511a)#012#5 0x00007fdaed662c3c __clone3 (libc.so.6 + 0x105c3c)#012#012Stack trace of thread 3405:#012#0 0x00007fdaed660a3d syscall (libc.so.6 + 0x103a3d)#012#1 0x0000000004344e2 n/a (n/a + 0x0)#012#2 0x000000000450066 n/a (n/a + 0x0)#012#3 0x000000000405123 n/a (n/a + 0x0)#012#4 0x00007fdaed58730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007fdaed5873c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x0000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Oct  2 17:03:45 ehatamov systemd[1]: systemd-coredump@12-3409-0.service: Deactivated successfully.
Oct  2 17:03:50 ehatamov kernel: traps: VBoxClient[3430] trap int3 ip:41ddb sp:7fdadef4fcd0 error:0 in VBoxClient[1ddb,400000+bb000]
```

Рис. 1: Мониторинг системных событий

Настройка правил rsyslog.conf

- Установлен и запущен веб-сервер Apache
- Добавлена строка **ErrorLog** **syslog:local1** в конфигурацию httpd
- Проверена регистрация сообщений



```
ehatamov@ehatamov:/etc/rsyslog.d - /etc/rsyslog.d
ehatamov@ehatamov:/home/ehatamov | ehatamov@ehatamov:/home/ehata

httpd.conf [----] 34 L:[ 1+ 0 1/ 1] *(34 / 34b) <EOF>
local1.* -/var/log/httpd-error.log
```

- `journalctl` — общий вывод
- `journalctl -f` — реальное время
- `journalctl _UID=0` — фильтрация по пользователю root
- `journalctl -p err` — вывод ошибок
- `--since yesterday` — фильтрация по дате
- `-o verbose` — детальный вывод записей

```
root@ehatamov: /home/ehatamov# journalctl _UID=0
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Collecting audit messages is disabled.
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Journal started
Oct 02 17:02:27 ehatamov.localdomain systemd-journald[282]: Runtime Journal (/run/log/journal/b47de17405e044edba8d1cda0fbff070) is
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'msr' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Inserted module 'fuse'
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_alua' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_emc' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd-modules-load[283]: Module 'scsi_dh_rdcac' is built in
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static Device Nodes in
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-sysusers.service - Create System Users...
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'nobody' with GID 65534.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'users' with GID 100.
Oct 02 17:02:27 ehatamov.localdomain systemd-sysusers[298]: Creating group 'systemd-journal' with GID 190.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-sysusers.service - Create System Users.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-vconsole-setup.service - Virtual Console Setup.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: dracut-cmdline-ask.service - dracut ask for additional cmdline parameters was sk
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting dracut-cmdline.service - dracut cmdline hook...
Oct 02 17:02:27 ehatamov.localdomain dracut-cmdline[308]: dracut-105-4.el10_0
Oct 02 17:02:27 ehatamov.localdomain dracut-cmdline[308]: Using kernel command line parameters: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished dracut-cmdline.service - dracut cmdline hook.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting dracut-pre-udev.service - dracut pre-udev hook...
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Finished dracut-pre-udev.service - dracut pre-udev hook.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device Events and Files...
Oct 02 17:02:27 ehatamov.localdomain systemd-udevd[408]: Using default interface naming scheme 'rhel-10.0'.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: Started systemd-udevd.service - Rule-based Manager for Device Events and Files.
Oct 02 17:02:27 ehatamov.localdomain systemd[1]: dracut-pre-trigger.service - dracut pre-trigger hook was skipped because no trigg
```

Рис. 3: Использование journalctl

- Создан каталог `/var/log/journal`
- Установлены права:
 - `chown root:systemd-journal /var/log/journal`
 - `chmod 2755 /var/log/journal`

Постоянный журнал journald

```
root@ehatamov:/home/ehatamov# journalctl -b
root@ehatamov:/home/ehatamov# mkdir -p /var/log/journal
root@ehatamov:/home/ehatamov# chown root:systemd-journal /var/log/journal/
root@ehatamov:/home/ehatamov# chmod 2755 /var/log/journal/
root@ehatamov:/home/ehatamov# killall -USR1 systemd-journald
root@ehatamov:/home/ehatamov# journalctl -b
Oct 02 17:02:27 ehatamov.localdomain kernel: Linux version 6.12.0-55.12.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockwell.com)
Oct 02 17:02:27 ehatamov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.12.1.el10_0.x86_64 root=/dev/mapper:
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-provided physical RAM map:
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffff] ACPI data
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fec000000-0x000000000fec00ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fee000000-0x000000000fee00ffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000000fffc00000-0x000000000fffffffff] reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000011ffffffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: NX (Execute Disable) protection: active
Oct 02 17:02:27 ehatamov.localdomain kernel: APIC: Static calls initialized
Oct 02 17:02:27 ehatamov.localdomain kernel: SMBIOS 2.5 present.
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 02 17:02:27 ehatamov.localdomain kernel: DMI: Memory slots populated: 0/0
Oct 02 17:02:27 ehatamov.localdomain kernel: Hypervisor detected: KVM
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 02 17:02:27 ehatamov.localdomain kernel: kvm-clock: using sched offset of 4082479414 cycles
Oct 02 17:02:27 ehatamov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle:
Oct 02 17:02:27 ehatamov.localdomain kernel: tsc: Detected 3187.196 MHz processor
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
Oct 02 17:02:27 ehatamov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Oct 02 17:02:27 ehatamov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Oct 02 17:02:27 ehatamov.localdomain kernel: total RAM covered: 4096M
Oct 02 17:02:27 ehatamov.localdomain kernel: Found optimal setting for mtrr clean up
Oct 02 17:02:27 ehatamov.localdomain kernel: gran_size: 64K chunk_size: 16 num_reg: 3 lose cover RAM: 00
```

Рис. 4: Постоянный журнал journald

Итоги работы

В ходе выполнения работы были изучены механизмы системного логирования Linux, принципы настройки **rsyslog** и **journald**, а также использование утилиты **journalctl** для анализа событий.

Полученные навыки позволяют администрировать систему, отслеживать события и выявлять ошибки в работе служб.