Лабораторная работа 7

Управление журналами событий в системе

Хохлачёва Полина Дмитриевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

2 Выполнение лабораторной работы

Открываем три терминала и во втором терминале запускаем мониторинг в реальном времени(рис. 2.1).

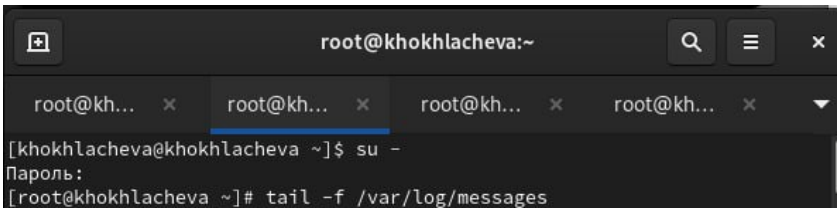


Рис. 2.1: Запуск мониторинга

Устанавливаем Apache(рис. 2.2).

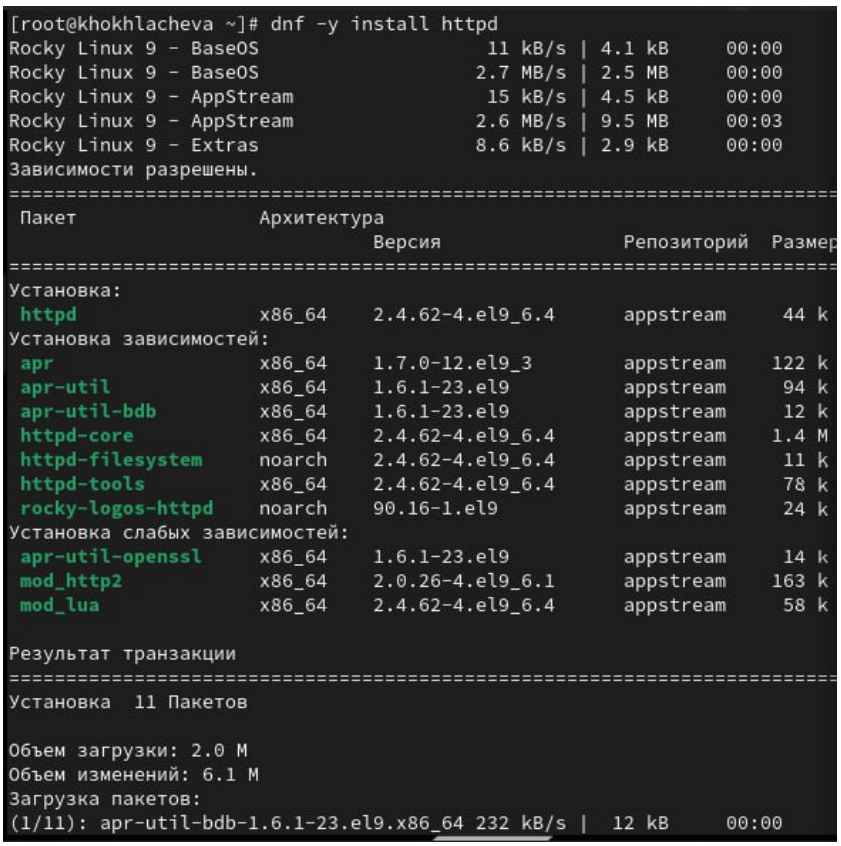


Рис. 2.2: Установка

В файл конфигурации добавляем строку(рис. 2.3).

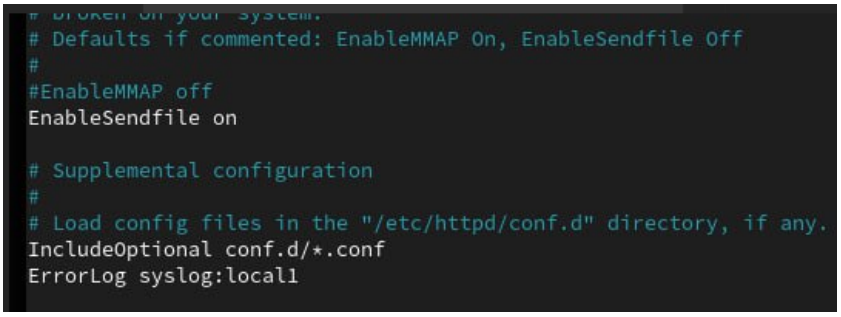


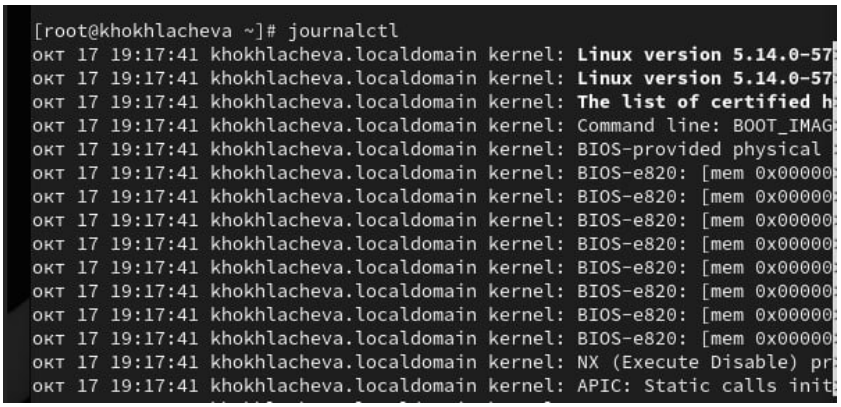
Рис. 2.3: Добавление

Создаём отдельный файл и вводим строку(рис. 2.4).

```
[root@khokhlacheva ~]# cd /etc/rsyslog.d
[root@khokhlacheva rsyslog.d]# touch httpd.conf
[root@khokhlacheva rsyslog.d]# nano httpd.conf
[root@khokhlacheva rsyslog.d]# cd /etc/rsyslog.d
[root@khokhlacheva rsyslog.d]# touch debug.conf
[root@khokhlacheva rsyslog.d]# echo "*.debug /var/log/messages-debug" >/e
tc/rsyslog.d/debug.conf
```

Рис. 2.4: Создание и вывод

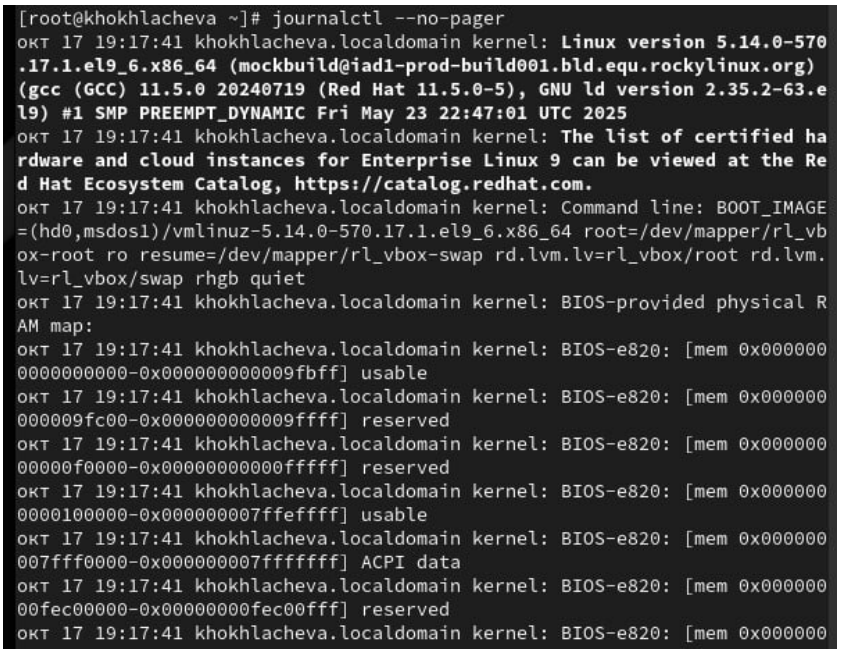
Смотрим содержания журнала(рис. 2.5).



```
[root@khokhlacheva ~]# journalctl
окт 17 19:17:41 khokhlacheva.localdomain kernel: Linux version 5.14.0-57
окт 17 19:17:41 khokhlacheva.localdomain kernel: Linux version 5.14.0-57
окт 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified h
окт 17 19:17:41 khokhlacheva.localdomain kernel: Command line: BOOT_IMAG
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-provided physical
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000
окт 17 19:17:41 khokhlacheva.localdomain kernel: NX (Execute Disable) pr
окт 17 19:17:41 khokhlacheva.localdomain kernel: APIC: Static calls init
```

Рис. 2.5: Содержание

Просмотр содержания журнала без использования пейджера(рис. 2.6).



```
[root@khokhlacheva ~]# journalctl --no-pager
окт 17 19:17:41 khokhlacheva.localdomain kernel: Linux version 5.14.0-570
.17.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org)
(gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-5), GNU ld version 2.35.2-63.e
l9) #1 SMP PREEMPT_DYNAMIC Fri May 23 22:47:01 UTC 2025
окт 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified ha
rdware and cloud instances for Enterprise Linux 9 can be viewed at the Re
d Hat Ecosystem Catalog, https://catalog.redhat.com.
окт 17 19:17:41 khokhlacheva.localdomain kernel: Command line: BOOT_IMAGE
=(hd0,msdos1)/vmlinuz-5.14.0-570.17.1.el9_6.x86_64 root=/dev/mapper/rl_vb
ox-root ro resume=/dev/mapper/rl_vbox-swap rd.lvm.lv=rl_vbox/root rd.lvm.
lv=rl_vbox/swap rhgb quiet
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-provided physical R
AM map:
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
0000000000-0x000000000009fbff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
000009fc00-0x000000000009ffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
00000f0000-0x00000000000fffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
0000100000-0x000000007ffeffff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
007fff0000-0x000000007fffffff] ACPI data
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
00fec00000-0x00000000fec00fff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000
```

Рис. 2.6: Просмотр

Также можем просмотреть детальную информацию(рис. 2.7).

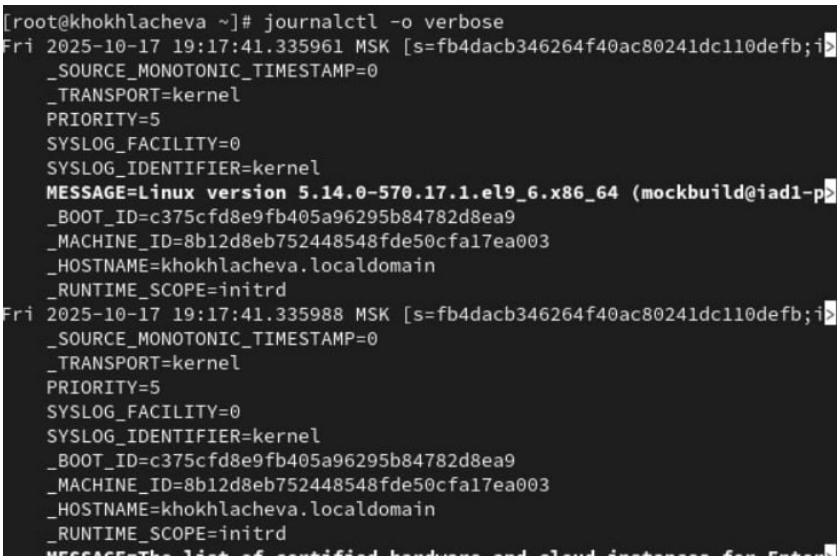


Рис. 2.7: Детальная информация

Получаем полномочия администратора,создаем каталог для хранения журнала, корректируем права доступа(рис. 2.8).

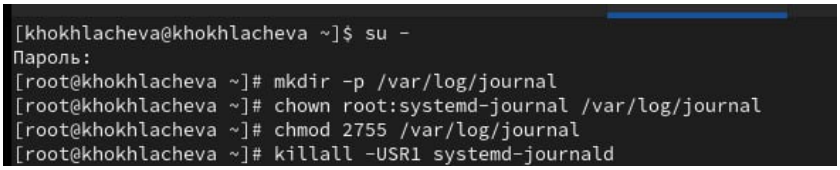
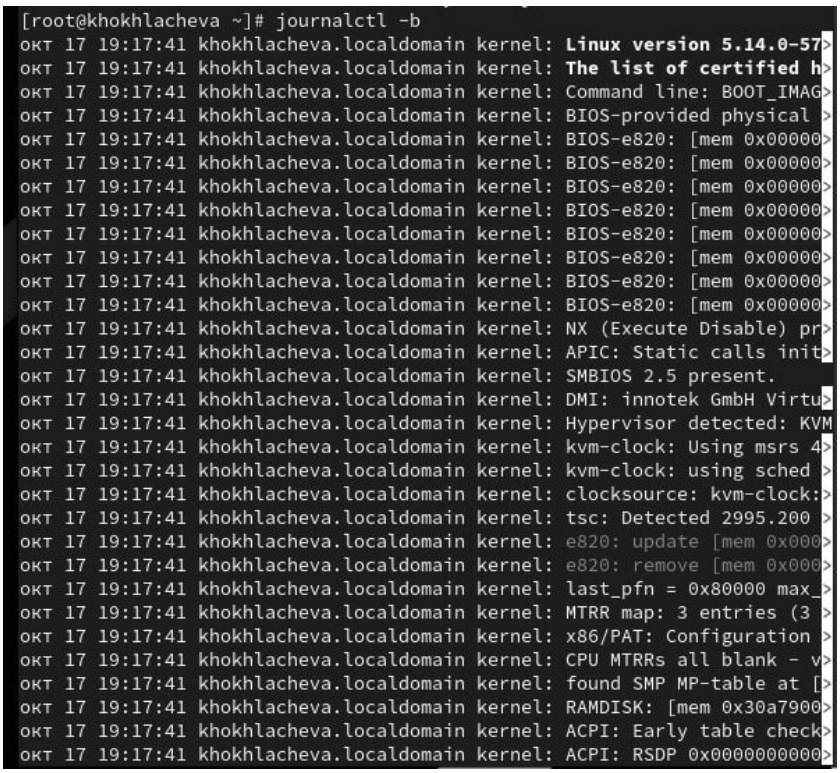


Рис. 2.8: Права доступа

Просмотр сообщений журнала(рис. 2.9).



```
[root@khokhlacheva ~]# journalctl -b
окт 17 19:17:41 khokhlacheva.localdomain kernel: Linux version 5.14.0-57>
окт 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified h>
окт 17 19:17:41 khokhlacheva.localdomain kernel: Command line: BOOT_IMAG>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-provided physical >
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: NX (Execute Disable) pr>
окт 17 19:17:41 khokhlacheva.localdomain kernel: APIC: Static calls init>
окт 17 19:17:41 khokhlacheva.localdomain kernel: SMBIOS 2.5 present.
окт 17 19:17:41 khokhlacheva.localdomain kernel: DMI: innotek GmbH Virtu>
окт 17 19:17:41 khokhlacheva.localdomain kernel: Hypervisor detected: KVM
окт 17 19:17:41 khokhlacheva.localdomain kernel: kvm-clock: Using msrs 4>
окт 17 19:17:41 khokhlacheva.localdomain kernel: kvm-clock: using sched >
окт 17 19:17:41 khokhlacheva.localdomain kernel: clocksource: kvm-clock:>
окт 17 19:17:41 khokhlacheva.localdomain kernel: tsc: Detected 2995.200 >
окт 17 19:17:41 khokhlacheva.localdomain kernel: e820: update [mem 0x000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: e820: remove [mem 0x000>
окт 17 19:17:41 khokhlacheva.localdomain kernel: last_pfn = 0x80000 max_>
окт 17 19:17:41 khokhlacheva.localdomain kernel: MTRR map: 3 entries (3 >
окт 17 19:17:41 khokhlacheva.localdomain kernel: x86/PAT: Configuration >
окт 17 19:17:41 khokhlacheva.localdomain kernel: CPU MTRRs all blank - v>
окт 17 19:17:41 khokhlacheva.localdomain kernel: found SMP MP-table at [>
окт 17 19:17:41 khokhlacheva.localdomain kernel: RAMDISK: [mem 0x30a7900>
окт 17 19:17:41 khokhlacheva.localdomain kernel: ACPI: Early table check>
окт 17 19:17:41 khokhlacheva.localdomain kernel: ACPI: RSDP 0x0000000000>
```

Рис. 2.9: Просмотр

3 Выводы

Мы получили навыки работы с журналами мониторинга различных событий в системе.