

# **Лабораторная работа 7**

**Управление журналами событий в системе**

Хохлачёва Полина Дмитриевна

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
<b>3 Выводы</b>	<b>11</b>

# **Список иллюстраций**

2.1	Запуск мониторинга . . . . .	6
2.2	Установка . . . . .	7
2.3	Добавление . . . . .	7
2.4	Создание и вывод . . . . .	8
2.5	Содержание . . . . .	8
2.6	Просмотр . . . . .	8
2.7	Детальная информация . . . . .	9
2.8	Права доступа . . . . .	9
2.9	Просмотр . . . . .	10

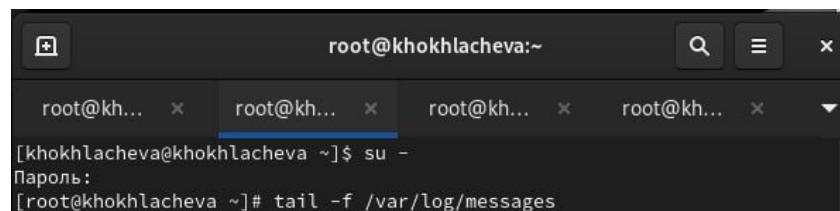
# **Список таблиц**

# **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).



The screenshot shows a terminal window with four tabs. The active tab at the bottom has the command `[root@khokhlacheva ~]# tail -f /var/log/messages` entered. The prompt `[root@khokhlacheva ~]#` is visible, along with the password entry line `Пароль:`.

Рис. 2.1: Запуск мониторинга

Устанавливаем Apache(рис. 2.2).

```
[root@khokhlacheva ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS           11 kB/s | 4.1 kB    00:00
Rocky Linux 9 - BaseOS           2.7 MB/s | 2.5 MB    00:00
Rocky Linux 9 - AppStream        15 kB/s | 4.5 kB    00:00
Rocky Linux 9 - AppStream        2.6 MB/s | 9.5 MB    00:03
Rocky Linux 9 - Extras          8.6 kB/s | 2.9 kB    00:00
Зависимости разрешены.
=====
Пакет          Архитектура      Версия      Репозиторий  Размер
=====
Установка:
httpd          x86_64        2.4.62-4.el9_6.4  appstream   44 k
Установка зависимостей:
apr            x86_64        1.7.0-12.el9_3   appstream   122 k
apr-util       x86_64        1.6.1-23.el9     appstream   94 k
apr-util-bdb   x86_64        1.6.1-23.el9     appstream   12 k
httpd-core     x86_64        2.4.62-4.el9_6.4  appstream   1.4 M
httpd-filesystem noarch       2.4.62-4.el9_6.4  appstream   11 k
httpd-tools    x86_64        2.4.62-4.el9_6.4  appstream   78 k
rocky-logos-httpd noarch       90.16-1.el9     appstream   24 k
Установка слабых зависимостей:
apr-util-openssl x86_64        1.6.1-23.el9     appstream   14 k
mod_http2      x86_64        2.0.26-4.el9_6.1  appstream   163 k
mod_lua         x86_64        2.4.62-4.el9_6.4  appstream   58 k
Результат транзакции
=====
Установка 11 Пакетов

Объем загрузки: 2.0 M
Объем изменений: 6.1 M
Загрузка пакетов:
(1/11): apr-util-bdb-1.6.1-23.el9.x86_64 232 kB/s | 12 kB    00:00
```

Рис. 2.2: Установка

В файл конфигурации добавляем строку(рис. 2.3).

```
# Disables 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
```

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" >/etc/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 5.14.0-570.17.1.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.el9) #1 SMP PREEMPT_DYNAMIC Fri May 23 22:47:01 UTC 2025
окт 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red 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_vbox-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 RAM map:
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x00000000000fffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000fffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000007ffffff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000000007fff0000-0x0000000007fffffff] ACPI data
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec0ffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000]
```

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.el9) #1 SMP PREEMPT_DYNAMIC Fri May 23 22:47:01 UTC 2025
окт 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red 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_vbox-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 RAM map:
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000fbfff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x00000000000fffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x00000000000fffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000007ffffff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000007fff0000-0x0000000007fffffff] ACPI data
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec0ffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000]
```

Рис. 2.6: Просмотр

Также можем просмотреть детальную информацию(рис. 2.7).

```
[root@khokhlacheva ~]# journalctl -o verbose
Fri 2025-10-17 19:17:41.335961 MSK [s=fb4dacb346264f40ac80241dc110defb;id=]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  MESSAGE=Linux version 5.14.0-570.17.1.el9_6.x86_64 (mockbuild@iad1-p)
  _BOOT_ID=c375cf8e9fb405a96295b84782d8ea9
  _MACHINE_ID=8b12d8eb752448548fde50cfa17ea003
  _HOSTNAME=khokhlacheva.localdomain
  _RUNTIME_SCOPE=initrd
Fri 2025-10-17 19:17:41.335988 MSK [s=fb4dacb346264f40ac80241dc110defb;id=]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=c375cf8e9fb405a96295b84782d8ea9
  _MACHINE_ID=8b12d8eb752448548fde50cfa17ea003
  _HOSTNAME=khokhlacheva.localdomain
  _RUNTIME_SCOPE=initrd
```

Рис. 2.7: Детальная информация

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

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

Рис. 2.8: Права доступа

Просмотр сообщений журнала(рис. 2.9).

```
[root@khokhlacheva ~]# journalctl -b
OKT 17 19:17:41 khokhlacheva.localdomain kernel: Linux version 5.14.0-57
OKT 17 19:17:41 khokhlacheva.localdomain kernel: The list of certified h
OKT 17 19:17:41 khokhlacheva.localdomain kernel: Command line: BOOT_IMAGE>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-provided physical >
OKT 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x00000>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: NX (Execute Disable) pr>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: APIC: Static calls init>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: SMBIOS 2.5 present.
OKT 17 19:17:41 khokhlacheva.localdomain kernel: DMI: innotek GmbH Virtu>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: Hypervisor detected: KVM
OKT 17 19:17:41 khokhlacheva.localdomain kernel: kvm-clock: Using msrs 4>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: kvm-clock: using sched >
OKT 17 19:17:41 khokhlacheva.localdomain kernel: clocksource: kvm-clock:>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: tsc: Detected 2995.200 >
OKT 17 19:17:41 khokhlacheva.localdomain kernel: e820: update [mem 0x000>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: e820: remove [mem 0x000>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: last_pfn = 0x80000 max_>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: MTRR map: 3 entries (3 >
OKT 17 19:17:41 khokhlacheva.localdomain kernel: x86/PAT: Configuration >
OKT 17 19:17:41 khokhlacheva.localdomain kernel: CPU MTRRs all blank - v>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: found SMP MP-table at [>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: RAMDISK: [mem 0x30a7900>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: ACPI: Early table check>
OKT 17 19:17:41 khokhlacheva.localdomain kernel: ACPI: RSDP 0x000000000000>
```

Рис. 2.9: Просмотр

## **3 Выводы**

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