

Лабораторная работа №7

Управление журналами событий в системе

Хохлачева Полина Дмитриевна

Российский университет дружбы народов, Москва, Россия

Информация

- Хохлачева Полина Дмитриевна
- Российский университет дружбы народов
- Номер студенческого билета- 1132242473
- [1132242473@pfur.ru]

Вводная часть

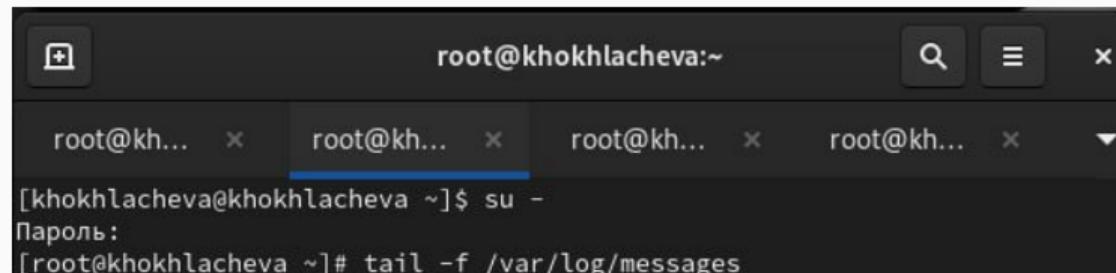
Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

Выполнение лабораторной работы

Выполнение лабораторной работы

Открываем три терминала и во втором терминале запускаем мониторинг в реальном времени(рис. (fig:001?)).



```
root@khokhlacheva:~  
root@kh... x root@kh... x root@kh... x root@kh... x ▾  
[khokhlacheva@khokhlacheva ~]$ su -  
Пароль:  
[root@khokhlacheva ~]# tail -f /var/log/messages
```

Рис. 1: Запуск мониторинга

Выполнение лабораторной работы

Устанавливаем Apache (рис. (fig:002?)).

```
[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
```

Выполнение лабораторной работы

В файл конфигурации добавляем строку(рис. (fig:003?)).

```
# Brought to you by Apache.
# 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. 3: Добавляем строку

Выполнение лабораторной работы

Создаём отдельный файл и вводим строку(рис. (fig:004?)).

```
[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. 4: Вводим строку

Выполнение лабораторной работы

Смотрим содержания журнала(рис. (fig:005?)).

```
[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 0x000000
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. 5: Просмотр

Выполнение лабораторной работы

Просмотр содержания журнала без использования пейджера(рис. (fig:006?)).

```
[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 0x0000000
0000000000-0x0000000000009fbff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000
000009fc00-0x0000000000009ffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000
00000f0000-0x000000000000ffff] reserved
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000
0000100000-0x0000000007ffeffff] usable
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000
007fff0000-0x0000000007fffffff] ACPI data
окт 17 19:17:41 khokhlacheva.localdomain kernel: BIOS-e820: [mem 0x0000000
```

Выполнение лабораторной работы

Также можем просмотреть детальную информацию(рис. (fig:007?)).

```
[root@khokhlacheva ~]# journalctl -o verbose
Fri 2025-10-17 19:17:41.335961 MSK [s=fb4dacb346264f40ac80241dc110defb;id=1]
  _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=8b12d8eb752448548fde50cf17ea003
  _HOSTNAME=khokhlacheva.localdomain
  _RUNTIME_SCOPE=initrd
Fri 2025-10-17 19:17:41.335988 MSK [s=fb4dacb346264f40ac80241dc110defb;id=2]
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=c375cf8e9fb405a96295b84782d8ea9
  _MACHINE_ID=8b12d8eb752448548fde50cf17ea003
  _HOSTNAME=khokhlacheva.localdomain
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of available log levels is:
  _SOURCE_MONOTONIC_TIMESTAMP=0
  _TRANSPORT=kernel
  PRIORITY=5
  SYSLOG_FACILITY=0
  SYSLOG_IDENTIFIER=kernel
  _BOOT_ID=c375cf8e9fb405a96295b84782d8ea9
  _MACHINE_ID=8b12d8eb752448548fde50cf17ea003
  _HOSTNAME=khokhlacheva.localdomain
  _RUNTIME_SCOPE=initrd
  MESSAGE=The list of available log levels is:
```

Выполнение лабораторной работы

Получаем полномочия администратора, создаем каталог для хранения журнала, корректируем права доступа(рис. (fig:008?)).

```
[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. 8: Корректируем права доступа

Выполнение лабораторной работы

Просмотр сообщений журнала(рис. (fig:009?)).

```
[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: 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>
```

Выводы

Выводы

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