

Лабораторная работа №7

Отчет

Зубов Иван Александрович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Использование journalctl	10
5	Постоянный журнал journald	12
6	Контрольные вопросы	13
7	Выводы	14

Список иллюстраций

3.1	Мониторинг системных событий в реальном времени	7
3.2	logger hello и увидим отображаемое сообщение	7
3.3	Устанавливаем Apache	8
3.4	Запускаем веб службу	8
3.5	Смотрим ошибки	8
3.6	Редактируем файл	8
3.7	Перезагружаем систему	9
3.8	Создаем файл и вводим информацию	9
3.9	Отладочная информация	9
4.1	Использование journalctl	11
4.2	Использование journalctl	11
5.1	Транслируем файл	12

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе

2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы
3. Продемонстрируйте навыки работы с `journalctl`
4. Продемонстрируйте навыки работы с `journal`

3 Выполнение лабораторной работы

Открываем три разных терминала. В первом входим в режим суперпользователя. На второй вкладке терминала запустите мониторинг системных событий в реальном времени. В третьей вкладке зайдём в режим суперпользователя и попробуем ввести неправильный пароль, в системных событиях увидим ошибку. Также в третьем терминале введём `logger hello` и увидим отображаемое сообщение

```
iazubov@iazubov ~]$ su -
Пароль:
root@iazubov ~)# tail -f /var/log/messages
Oct 1 17:22:53 iazubov packagekitd[1845]: Failed to get cache filename for gnome-control-center-filesystem
Oct 1 17:22:53 iazubov packagekitd[1845]: Failed to get cache filename for kernel
Oct 1 17:23:50 iazubov systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 1 17:23:50 iazubov systemd[1]: Started Fingerprint Authentication Daemon.
Oct 1 17:23:54 iazubov su[3197]: (to root) iazubov on pts/0
Oct 1 17:23:54 iazubov systemd[1]: Starting Hostname Service...
Oct 1 17:23:54 iazubov systemd[1]: Started Hostname Service.
Oct 1 17:24:06 iazubov systemd[2182]: Started VTE child process 3240 launched by gnome-terminal-server process 3103.
Oct 1 17:24:19 iazubov su[3267]: (to root) iazubov on pts/1
Oct 1 17:24:21 iazubov systemd[1]: fprintd.service: Deactivated successfully.
Oct 1 17:24:34 iazubov systemd[2182]: Started VTE child process 3310 launched by gnome-terminal-server process 3103.
Oct 1 17:24:43 iazubov systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 1 17:24:47 iazubov systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 1 17:24:47 iazubov systemd[1]: Started Fingerprint Authentication Daemon.
Oct 1 17:24:51 iazubov su[3346]: FAILED SU (to root) iazubov on pts/2
Oct 1 17:24:52 iazubov chronyd[869]: Selected source 193.106.93.116 (2.rocky.pool.ntp.org)
Oct 1 17:25:12 iazubov iazubov[3361]: hello
Oct 1 17:25:18 iazubov systemd[2182]: Created slice User Background Tasks Slice.
Oct 1 17:25:18 iazubov systemd[2182]: Starting Cleanup of User's Temporary Files and Directories...
Oct 1 17:25:18 iazubov systemd[2182]: Finished Cleanup of User's Temporary Files and Directories.
Oct 1 17:25:18 iazubov systemd[1]: fprintd.service: Deactivated successfully.
^C
```

Рис. 3.1: Мониторинг системных событий в реальном времени

```
iazubov@iazubov ~]$ su -
Пароль:
su: Сбой при проверке подлинности
iazubov@iazubov ~]$ logger hello
iazubov@iazubov ~]$
```

Рис. 3.2: `logger hello` и увидим отображаемое сообщение

В первой вкладке терминала установим Apache

```
[iazubov@iazubov ~]$ su -
Пароль:
[root@iazubov ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64                35 kB/s | 38 kB    00:01
Extra Packages for Enterprise Linux 9 - x86_64                2.2 MB/s | 20 MB    00:09
Rocky Linux 9 - BaseOS                                         551 B/s | 4.1 kB    00:07
Rocky Linux 9 - AppStream                                       310 B/s | 4.5 kB    00:14
Rocky Linux 9 - Extras                                         134 B/s | 2.9 kB    00:22
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
```

Рис. 3.3: Устанавливаем Apache

После окончания процесса установки запустим веб-службу

```
[root@iazubov ~]# systemctl start httpd
[root@iazubov ~]# systemctl enable httpd
```

Рис. 3.4: Запускаем веб службу

Во второй вкладке терминала посмотрим журнал сообщений об ошибках веб-службы

```
[root@iazubov ~]# tail -f /var/log/httpd/error_log
[Wed Oct 01 17:29:00.276390 2025] [core:notice] [pid 4100:tid 4100] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Oct 01 17:29:00.281639 2025] [suexec:notice] [pid 4100:tid 4100] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Oct 01 17:29:00.356775 2025] [lbmethod_heartbeat:notice] [pid 4100:tid 4100] AH02282: No slotmem from mod_heartbeat
[Wed Oct 01 17:29:00.375781 2025] [mpm_event:notice] [pid 4100:tid 4100] AH00489: Apache/2.4.62 (Rocky Linux) configured -- r assuming normal operations
[Wed Oct 01 17:29:00.376051 2025] [core:notice] [pid 4100:tid 4100] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
^C
[root@iazubov ~]# tail -f /var/log/messages-debug
Oct 1 17:34:28 iazubov systemd[1]: Stopping System Logging Service...
Oct 1 17:34:28 iazubov rsyslogd[4382]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4382" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 1 17:34:28 iazubov systemd[1]: rsyslog.service: Deactivated successfully.
Oct 1 17:34:28 iazubov systemd[1]: Stopped System Logging Service.
Oct 1 17:34:28 iazubov systemd[1]: Starting System Logging Service...
Oct 1 17:34:28 iazubov rsyslogd[4599]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4599" x-info="https://www.rsyslog.com"] start
Oct 1 17:34:28 iazubov rsyslogd[4599]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 1 17:34:28 iazubov systemd[1]: Started System Logging Service.
Oct 1 17:35:11 iazubov root[4605]: Daemon Debug Message
^C
```

Рис. 3.5: Смотрим ошибки

В каталоге /etc/rsyslog.d создаем файл мониторинга событий веб-службы. Редактируем его, прописывая в нем строку local1.* -/var/log/httpd-error.log

```
[root@iazubov ~]# cd /etc/rsyslog.d
[root@iazubov rsyslog.d]# touch httpd.conf
[root@iazubov rsyslog.d]# nano httpd.conf
[root@iazubov rsyslog.d]#
```

Рис. 3.6: Редактируем файл

Переходим в первую вкладку терминала и перезагрузим конфигурацию rsyslogd и веб-службу

```
root@iazubov ~]# systemctl restart rsyslog.service
root@iazubov ~]# systemctl restart httpd
```

Рис. 3.7: Перезагружаем систему

В третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации. Вводим в терминале `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf` и перезапустим систему

```
root@iazubov rsyslog.d]# cd /etc/rsyslog.d
root@iazubov rsyslog.d]# touch debug.conf
root@iazubov rsyslog.d]# nano debug.conf
root@iazubov rsyslog.d]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@iazubov rsyslog.d]# logger -p daemon.debug "Daemon Debug Message"
root@iazubov rsyslog.d]#
```

Рис. 3.8: Создаем файл и вводим информацию

В третьей вкладке терминала введем `logger -p daemon.debug "Daemon Debug Message"`, а во второй вкладке увидим выведенное сообщение на отладочной информации

```
root@iazubov ~]# tail -f /var/log/messages-debug
Oct 1 17:34:28 iazubov systemd[1]: Stopping System Logging Service...
Oct 1 17:34:28 iazubov rsyslogd[4382]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4382" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 1 17:34:28 iazubov systemd[1]: rsyslog.service: Deactivated successfully.
Oct 1 17:34:28 iazubov systemd[1]: Stopped System Logging Service.
Oct 1 17:34:28 iazubov systemd[1]: Starting System Logging Service...
Oct 1 17:34:28 iazubov rsyslogd[4599]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="4599" x-info="https://www.rsyslog.com"] start
Oct 1 17:34:28 iazubov rsyslogd[4599]: imjournal: journal files changed, reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 1 17:34:28 iazubov systemd[1]: Started System Logging Service.
Oct 1 17:35:11 iazubov root[4605]: Daemon Debug Message
```

Рис. 3.9: Отладочная информация

4 Использование journalctl

1. Во второй вкладке терминала посмотрим содержимое журнала с событиями с момента последнего запуска системы: `journalctl`
2. Просмотр содержимого журнала без использования пейджера: `journalctl -no-pager`
3. Режим просмотра журнала в реальном времени: `journalctl -f`
4. Для использования фильтрации просмотра конкретных параметров журнала введите `journalctl`
5. Просмотрите события для UID0: `journalctl _UID=0`
6. Для отображения последних 20 строк журнала введите `journalctl -n 20`
7. Для просмотра только сообщений об ошибках введите `journalctl -p err`
8. Если мы хотим просмотреть сообщения журнала, записанные за определённый период времени, вы можете использовать параметры `-since` и `-until`.
`YYYY-MM-DD hh:mm:ss`
9. Если мы хотим показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используйте `journalctl -since yesterday -p err`
10. Если нам нужна детальная информация, то используем `journalctl -o verbose`
11. Для просмотра дополнительной информации о модуле `sshd` введём `journalctl _SYSTEMD_UNIT=sshd.service`

```

root@iazubov ~]# journalctl
PKT 01 17:19:09 iazubov.localdomain kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ
PKT 01 17:19:09 iazubov.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be
PKT 01 17:19:09 iazubov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.39.1.el9_6.x86_64 root=
PKT 01 17:19:09 iazubov.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-provided physical RAM map:
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000009ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x000000000000ffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] ACPI data
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fee0ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x0000000000ffffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000010ffffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: NX (Execute Disable) protection: active
PKT 01 17:19:09 iazubov.localdomain kernel: APIC: Static calls initialized
PKT 01 17:19:09 iazubov.localdomain kernel: SMBIOS 2.5 present.
PKT 01 17:19:09 iazubov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
PKT 01 17:19:09 iazubov.localdomain kernel: Hypervisor detected: KVM
PKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
PKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: using sched offset of 6848895889 cycles
PKT 01 17:19:09 iazubov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_
PKT 01 17:19:09 iazubov.localdomain kernel: tsc: Detected 2096.062 MHz processor
PKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
PKT 01 17:19:09 iazubov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
PKT 01 17:19:09 iazubov.localdomain kernel: total RAM covered: 4096M
PKT 01 17:19:09 iazubov.localdomain kernel: Found optimal setting for mtrr clean up
PKT 01 17:19:09 iazubov.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RA
PKT 01 17:19:09 iazubov.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
PKT 01 17:19:09 iazubov.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
PKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> reserved
PKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
PKT 01 17:19:09 iazubov.localdomain kernel: found SMP MP-table at [mem 0x0009f0b0-0x0009fbff]
PKT 01 17:19:09 iazubov.localdomain kernel: RAMDISK: [mem 0x30b0c000-0x3457dfff]
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: Early table checksum verification disabled
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: XSDT 0x0000000000000000 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: FACP 0x0000000000000000 0000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000001)
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: DSDT 0x0000000000000000 002353 (v02 VBOX VBOXBIOS 00000002 VBOX 000298F4)
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: FACS 0x0000000000000000 000040
PKT 01 17:19:09 iazubov.localdomain kernel: ACPI: PAFS 0x0000000000000000 000040

```

Рис. 4.1: Использование journalctl

```

root@iazubov ~]# journalctl --no-pager
PKT 01 17:19:09 iazubov.localdomain kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iad1-prod-build001.bld.equ
PKT 01 17:19:09 iazubov.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be
PKT 01 17:19:09 iazubov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.39.1.el9_6.x86_64 root=
PKT 01 17:19:09 iazubov.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-provided physical RAM map:
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000009ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x000000000000ffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000ffff] ACPI data
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fee00000-0x0000000000fee0ffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x0000000000ffffff] reserved
PKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000001000000000-0x0000000010ffffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: NX (Execute Disable) protection: active
PKT 01 17:19:09 iazubov.localdomain kernel: APIC: Static calls initialized
PKT 01 17:19:09 iazubov.localdomain kernel: SMBIOS 2.5 present.
PKT 01 17:19:09 iazubov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
PKT 01 17:19:09 iazubov.localdomain kernel: Hypervisor detected: KVM
PKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
PKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: using sched offset of 6848895889 cycles
PKT 01 17:19:09 iazubov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_
PKT 01 17:19:09 iazubov.localdomain kernel: tsc: Detected 2096.062 MHz processor
PKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
PKT 01 17:19:09 iazubov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
PKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
PKT 01 17:19:09 iazubov.localdomain kernel: total RAM covered: 4096M
PKT 01 17:19:09 iazubov.localdomain kernel: Found optimal setting for mtrr clean up
PKT 01 17:19:09 iazubov.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RAM
PKT 01 17:19:09 iazubov.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
PKT 01 17:19:09 iazubov.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
PKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> reserved
PKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
PKT 01 17:19:09 iazubov.localdomain kernel: found SMP MP-table at [mem 0x0009f0b0-0x0009fbff]

```

Рис. 4.2: Использование journalctl

5 Постоянный журнал journald

Создаем каталог для хранения записей журнала. Скорректируем права доступа для каталога. Перезагрузим систему и посмотрим сообщения с момента последней перезагрузки.

```
root@iazubov ~]# mkdir -p /var/log/journal
root@iazubov ~]# chown root:systemd-journal /var/log/journal
root@iazubov ~]# chmod 2755 /var/log/journal
root@iazubov ~]# killall -USR1 systemd-journald
root@iazubov ~]# journalctl -b
OKT 01 17:19:09 iazubov.localdomain kernel: Linux version 5.14.0-570.39.1.el9_6.x86_64 (mockbuild@iadi-prod-build001.bld.equ
OKT 01 17:19:09 iazubov.localdomain kernel: The list of certified hardware and cloud instances for Enterprise Linux 9 can be
OKT 01 17:19:09 iazubov.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-570.39.1.el9_6.x86_64 root=
OKT 01 17:19:09 iazubov.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-provided physical RAM map:
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x00000000000ff000-0x00000000000fffff] reserved
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000dfff000-0x000000000dfffff] ACPI data
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000fee0000-0x000000000fec00ff] reserved
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000fee0000-0x000000000fee00ff] reserved
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x000000000fffc000-0x000000000fffffff] reserved
OKT 01 17:19:09 iazubov.localdomain kernel: BIOS-e820: [mem 0x0000000010000000-0x000000001ffffff] usable
OKT 01 17:19:09 iazubov.localdomain kernel: NX (Execute Disable) protection: active
OKT 01 17:19:09 iazubov.localdomain kernel: APIC: Static calls initialized
OKT 01 17:19:09 iazubov.localdomain kernel: SMBIOS 2.5 present.
OKT 01 17:19:09 iazubov.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
OKT 01 17:19:09 iazubov.localdomain kernel: Hypervisor detected: KVM
OKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
OKT 01 17:19:09 iazubov.localdomain kernel: kvm-clock: using sched offset of 6848895889 cycles
OKT 01 17:19:09 iazubov.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycles: 0x1cd42e4dffb, max_
OKT 01 17:19:09 iazubov.localdomain kernel: tsc: Detected 2096.062 MHz processor
OKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0x00000000-0x000000ff] usable ==> reserved
OKT 01 17:19:09 iazubov.localdomain kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
OKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
OKT 01 17:19:09 iazubov.localdomain kernel: total RAM covered: 4096M
OKT 01 17:19:09 iazubov.localdomain kernel: Found optimal setting for mtrr clean up
OKT 01 17:19:09 iazubov.localdomain kernel: gran_size: 64K chunk_size: 1G num_reg: 3 lose cover RA
OKT 01 17:19:09 iazubov.localdomain kernel: MTRR map: 6 entries (3 fixed + 3 variable; max 35), built from 16 variable MTRRs
OKT 01 17:19:09 iazubov.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
OKT 01 17:19:09 iazubov.localdomain kernel: e820: update [mem 0x00000000-0xffffffff] usable ==> reserved
OKT 01 17:19:09 iazubov.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
OKT 01 17:19:09 iazubov.localdomain kernel: found SMP MP-table at [mem 0x0009fbf0-0x0009fbff]
OKT 01 17:19:09 iazubov.localdomain kernel: RAMDISK: [mem 0x30b0c000-0x34570fff]
OKT 01 17:19:09 iazubov.localdomain kernel: ACPI: Early table checksum verification disabled
OKT 01 17:19:09 iazubov.localdomain kernel: ACPI: RSDP 0x000000000000E000 000024 (v02 VBOX )
OKT 01 17:19:09 iazubov.localdomain kernel: ACPI: XSDT 0x000000000000FF00 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
```

Рис. 5.1: Транслируем файл

6 Контрольные вопросы

1. Какой файл используется для настройки rsyslogd? `/etc/rsyslog.conf`
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией? `/var/log/secure`
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов? 1 неделя
4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом `info` в файл `/var/log/messages.info`? `*.info /var/log/messages.info`
5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени? `tail -f /var/log/messages` или `journalctl -f`
6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00? `journalctl _PID=1 --since="09:00" --until="15:00"`
7. Какая команда позволяет вам видеть сообщения `journald` после последней перезагрузки системы? `journalctl -b`
8. Какая процедура позволяет сделать журнал `journald` постоянным? Создать директорию `/var/log/journal` и перезапустить `systemd-journald`

7 Выводы

Я получил навыки работы с журналами мониторинга различных событий в системе.