

Лабораторная работа №7

Презентация

Ермишина М. К.

17 октября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Ермишина Мария Кирилловна
- студент группы НПИбд-01-24
- Российский университет дружбы народов
- 1132230166@pfur.ru
- <https://github.com/ErmiMash>

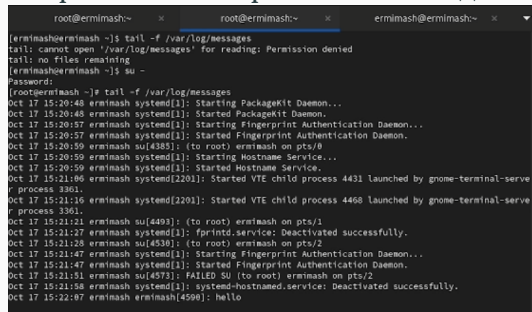
Элементы презентации

Целью данной лабораторной работы является получение навыков работы с журналами мониторинга различных событий в системе.

Выполнение лабораторной работы

Мониторинг журнала системных событий в реальном времени

Получив полномочия администратора на второй вкладке терминала запустите мониторинг системных событий в реальном времени: - `tail -f /var/log/messages`
В третьей вкладке терминала вернитесь к учётной записи своего пользователя и попробуйте получить полномочия администратора, но введите неправильный пароль. После введите “logger hello”



```
root@ermimash:~
ermimash@ermimash:~$ tail -f /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
tail: no files remaining
ermimash@ermimash:~$ su -
Password:
[root@ermimash ~]# tail -f /var/log/messages
Oct 17 15:20:48 ermimash systemd[1]: Starting PackageKit Daemon...
Oct 17 15:20:48 ermimash systemd[1]: Started PackageKit Daemon...
Oct 17 15:20:57 ermimash systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 15:20:57 ermimash systemd[1]: Started Fingerprint Authentication Daemon...
Oct 17 15:20:59 ermimash su[4385]: (to root) ermimash on pts/0
Oct 17 15:20:59 ermimash systemd[1]: Starting Hostname Service...
Oct 17 15:20:59 ermimash systemd[1]: Started Hostname Service...
Oct 17 15:21:06 ermimash systemd[2201]: Started VTE child process 4431 launched by gnome-terminal-serve
r process 3361.
Oct 17 15:21:16 ermimash systemd[2201]: Started VTE child process 4468 launched by gnome-terminal-serve
r process 3361.
Oct 17 15:21:21 ermimash su[4493]: (to root) ermimash on pts/1
Oct 17 15:21:27 ermimash systemd[1]: fprintd.service: Deactivated successfully.
Oct 17 15:21:28 ermimash su[4530]: (to root) ermimash on pts/2
Oct 17 15:21:47 ermimash systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 17 15:21:47 ermimash systemd[1]: Started Fingerprint Authentication Daemon...
Oct 17 15:21:51 ermimash su[4573]: FAILED SU (to root) ermimash on pts/2
Oct 17 15:21:58 ermimash systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 17 15:22:07 ermimash ermimash[4590]: hello
```

Изменение правил rsyslog.conf

В первой вкладке терминала установите Apache, если он не был ранее инсталлирован: - `dnf -y install httpd - systemctl start httpd - systemctl enable`

```
Running scriptlet: mod_http2-2.0.26-4.el9.x86_64 11/11
Verifying      : apr-util-bdb-1.6.1-23.el9.x86_64 1/11
Verifying      : httpd-tools-2.4.62-4.el9_6.4.x86_64 2/11
Verifying      : httpd-2.4.62-4.el9_6.4.x86_64 3/11
Verifying      : apr-util-1.6.1-23.el9.x86_64 4/11
Verifying      : rocky-logos-httpd-90.16-1.el9.noarch 5/11
Verifying      : httpd-core-2.4.62-4.el9_6.4.x86_64 6/11
Verifying      : httpd-filesystem-2.4.62-4.el9_6.4.noarch 7/11
Verifying      : mod_lua-2.4.62-4.el9_6.4.x86_64 8/11
Verifying      : mod_http2-2.0.26-4.el9_6.1.x86_64 9/11
Verifying      : apr-util-openssl-1.6.1-23.el9.x86_64 10/11
Verifying      : apr-1.7.0-12.el9_3.x86_64 11/11

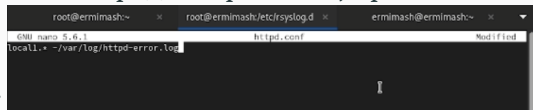
Installed:
apr-1.7.0-12.el9_3.x86_64          apr-util-1.6.1-23.el9.x86_64
apr-util-bdb-1.6.1-23.el9.x86_64 apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.62-4.el9_6.4.x86_64    httpd-core-2.4.62-4.el9_6.4.x86_64
httpd-filesystem-2.4.62-4.el9_6.4.noarch httpd-tools-2.4.62-4.el9_6.4.x86_64
mod_http2-2.0.26-4.el9_6.1.x86_64 mod_lua-2.4.62-4.el9_6.4.x86_64
rocky-logos-httpd-90.16-1.el9.noarch

Complete!
[root@ermimash ~]# systemctl start httpd
[root@ermimash ~]# systemctl enable httpd
```

httpd

В каталоге `/etc/rsyslog.d` создайте файл мониторинга событий веб-службы: `- cd /etc/rsyslog.d - touch httpd.conf` Открыв его на редактирование, пропишите в

нём: `- local1.* -/var/log/httpd-error.log`



Файл конфигурации для мониторинга отладочной информации

В третьей вкладке терминала создайте отдельный файл: - `cd /etc/rsyslog.d - touch debug.conf` В этом же терминале введите: - `echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf` А после: - `logger -p daemon.debug "Daemon Debug Message"`

```
[ermimash@ermimash rsyslog.d]$ su -
Password:
[root@ermimash ~]# touch debug.conf
[root@ermimash ~]# rm -r debug.conf
rm: remove regular empty file 'debug.conf'? y
[root@ermimash ~]# cd /etc/rsyslog.d
[root@ermimash rsyslog.d]# touch debug.conf
[root@ermimash rsyslog.d]# echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
-bash: syntax error near unexpected token `newline'
-bash: /etc/rsyslog.d/debug.conf: Permission denied
[root@ermimash rsyslog.d]#
logout
[ermimash@ermimash rsyslog.d]$ echo "*.debug /var/log/messages-debug" >
/etc/rsyslog.d/debug.conf
bash: syntax error near unexpected token `newline'
bash: /etc/rsyslog.d/debug.conf: Permission denied
[ermimash@ermimash rsyslog.d]$ echo "*.debug /var/log/messages-debug" >
bash: syntax error near unexpected token `newline'
[ermimash@ermimash rsyslog.d]$ echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
bash: /etc/rsyslog.d/debug.conf: Permission denied
[ermimash@ermimash rsyslog.d]$ su -
Password:
[root@ermimash ~]# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
[root@ermimash ~]# logger -p daemon.debug "Daemon Debug Message"
[root@ermimash ~]#
```

Использование journalctl

Во второй вкладке терминала посмотрите содержимое журнала с событиями с момента последнего запуска системы: - journalctl Просмотр содержимого журнала без использования пейджера: - journalctl -no-pager Режим просмотра журнала в реальном времени: - journalctl -f

```
Oct 17 15:27:03 ermimash.localdomain systemd[1]: Starting Hostname Service...
Oct 17 15:27:03 ermimash.localdomain systemd[1]: Started Hostname Service.
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Stopping System Logging Service...
Oct 17 15:27:18 ermimash.localdomain rsyslogd[43996]: [origin software="rsyslogd" swVersion="8.2412.0-1
.el9" x-pid="43996" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 17 15:27:18 ermimash.localdomain systemd[1]: rsyslog.service: Deactivated successfully.
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Stopped System Logging Service.
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Starting System Logging Service...
Oct 17 15:27:18 ermimash.localdomain rsyslogd[44372]: [origin software="rsyslogd" swVersion="8.2412.0-1
.el9" x-pid="44372" x-info="https://www.rsyslog.com"] start
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Started System Logging Service.
Oct 17 15:27:18 ermimash.localdomain rsyslogd[44372]: imjournal: journal files changed, reloading... [
v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]
Oct 17 15:27:32 ermimash.localdomain systemd[1]: fprintd.service: Deactivated successfully.
Oct 17 15:27:33 ermimash.localdomain systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Oct 17 15:27:41 ermimash.localdomain root[44394]: Daemon Debug Message
Oct 17 15:28:08 ermimash.localdomain PackageKit[4375]: daemon quit
Oct 17 15:28:08 ermimash.localdomain systemd[1]: packagekit.service: Deactivated successfully.
[root@ermimash rsyslog.d]# journalctl -f
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Stopped System Logging Service.
Oct 17 15:27:18 ermimash.localdomain systemd[1]: Starting System Logging Service...
Oct 17 15:27:18 ermimash.localdomain rsyslogd[44372]: [origin software="rsyslogd" swVersion="8.2412.0-1
```

Для использования фильтрации просмотра конкретных параметров журнала введите - journalctl и дважды нажмите клавишу Tab

```
CURRENT_USE_PRETTY=
CPU_USAGE_NSEC=
CURRENT_USE=
CURRENT_USE_PRETTY=
DBUS_BROKER_LOG_DROPPED=
DBUS_BROKER_MESSAGE_DESTINATION=
DBUS_BROKER_MESSAGE_INTERFACE=
DBUS_BROKER_MESSAGE_MEMBER=
DBUS_BROKER_MESSAGE_PATH=
DBUS_BROKER_MESSAGE_SERIAL=
DBUS_BROKER_MESSAGE_SIGNATURE=
DBUS_BROKER_MESSAGE_TYPE=
DBUS_BROKER_MESSAGE_UNIX_FDS=
DBUS_BROKER_METRICS_DISPATCH_AVG=
DBUS_BROKER_METRICS_DISPATCH_COUNT=
DBUS_BROKER_METRICS_DISPATCH_MAX=
DBUS_BROKER_METRICS_DISPATCH_MIN=
DBUS_BROKER_METRICS_DISPATCH_STDDEV=
DBUS_BROKER_POLICY_TYPE=
DBUS_BROKER_RECEIVER_SECURITY_LABEL=
DBUS_BROKER_RECEIVER_UNIQUE_NAME=
DBUS_BROKER_RECEIVER_WELL_KNOWN_NAME_0=
NM_DEVICE=
NM_LOG_DOMAINS=
NM_LOG_LEVEL=
_PID=
PRIORITY=
REALMD_OPERATION=
_RUNTIME_SCOPE=
SEAT_ID=
_SELINUX_CONTEXT=
SESSION_ID=
_SOURCE_MONOTONIC_TIMESTAMP=
_SOURCE_REALTIME_TIMESTAMP=
SSSD_DOMAIN=
SSSD_PRG_NAME=
_STREAM_ID=
SYSLOG_FACILITY=
SYSLOG_IDENTIFIER=
SYSLOG_PID=
SYSLOG_RAW=
SYSLOG_TIMESTAMP=
_SYSTEMD_CGROUP=
_SYSTEMD_INVOCATION_ID=
```

Команды для работы

Просмотрите события для UID0: - `journalctl _UID=0` Для отображения последних 20 строк журнала введите: - `journalctl -n 20` Для просмотра только сообщений об ошибках введите: - `journalctl -p err` Для просмотра всех сообщений со вчерашнего дня введите: - `journalctl --since yesterday`

```
[root@ermimash rsyslog.d]# journalctl -p err
Oct 17 14:10:38 ermimash.localdomain kernel: Warning: Unmaintained driver is detected: e1000
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be run
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is
Oct 17 14:10:38 ermimash.localdomain kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a sup
Oct 17 14:10:49 ermimash.localdomain alsactl[876]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error:
Oct 17 14:10:59 ermimash.localdomain kernel: Warning: Unmaintained driver is detected: ip_set
Oct 17 14:11:32 ermimash.localdomain gdm-password[2186]: gkr-pam: unable to locate daemon control fil
Oct 17 14:11:35 ermimash.localdomain systemd[2201]: Failed to start Application launched by gnome-ssu
```

Скорректируйте права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию: - `chown root:systemd-journal /var/log/journal` - `chmod 2755 /var/log/journal` Для принятия изменений необходимо или перезагрузить систему: - `killall -USR1 systemd-journald`

```
[ermimash@ermimash rsyslog.d]$ su -  
Password:  
[root@ermimash ~]# mkdir -p /var/log/journal  
[root@ermimash ~]# chown root:systemd-journal /var/log/journal  
chmod 2755 /var/log/journal  
[root@ermimash ~]# killall -USR1 systemd-journald  
[root@ermimash ~]#
```

Журнал с момента посл. перезагрузки

Если вы хотите видеть сообщения журнала с момента последней перезагрузки, используйте: - journalctl -b

```
Oct 17 14:10:38 ermimash.localdomain kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-provided physical RAM map:
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009bfff] us>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] re>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x000000000000bf000-0x000000000000fffff] re>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dffff] us>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x00000000dffff0000-0x00000000dffffff] AC>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec08fff] re>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee08fff] re>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] re>
Oct 17 14:10:38 ermimash.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x000000029ffffff] us>
Oct 17 14:10:38 ermimash.localdomain kernel: NX (Execute Disable) protection: active
Oct 17 14:10:38 ermimash.localdomain kernel: APIC: Static calls initialized
Oct 17 14:10:38 ermimash.localdomain kernel: SMBIOS 2.5 present.
Oct 17 14:10:38 ermimash.localdomain kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox b
Oct 17 14:10:38 ermimash.localdomain kernel: Hypervisor detected: KVM
Oct 17 14:10:38 ermimash.localdomain kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Oct 17 14:10:38 ermimash.localdomain kernel: kvm-clock: using sched offset of 5170905296 cycles
Oct 17 14:10:38 ermimash.localdomain kernel: clocksource: kvm-clock: mask: 0xffffffffffffff max_cycl>
Oct 17 14:10:38 ermimash.localdomain kernel: tsc: Detected 3693.066 MHz processor
Oct 17 14:10:38 ermimash.localdomain kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserv>
Oct 17 14:10:38 ermimash.localdomain kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Oct 17 14:10:38 ermimash.localdomain kernel: last_pfn = 0x2a0000 max_arch_pfn = 0x400000000
Oct 17 14:10:38 ermimash.localdomain kernel: total RAM covered: 10240M
Oct 17 14:10:38 ermimash.localdomain kernel: Found optimal setting for mtrr clean up
Oct 17 14:10:38 ermimash.localdomain kernel: gran_size: 64K chunk_size: 64K num_reg: >
Oct 17 14:10:38 ermimash.localdomain kernel: MTRR map: 5 entries (3 fixed + 2 variable; max 35), built>
Oct 17 14:10:38 ermimash.localdomain kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC->
Oct 17 14:10:38 ermimash.localdomain kernel: e820: update [mem 0xe0000000-0xffffffff] usable ==> reserv>
Oct 17 14:10:38 ermimash.localdomain kernel: last_pfn = 0xe0000 max_arch_pfn = 0x400000000
Oct 17 14:10:38 ermimash.localdomain kernel: found SMP WP-table at [mem 0x0009fbf0-0x0009fbff]
Oct 17 14:10:38 ermimash.localdomain kernel: RAMDISK: [mem 0x30cc1000-0x34658fff]
Oct 17 14:10:38 ermimash.localdomain kernel: ACPI: Early table checksum verification disabled
```

Получены навыки работы с журналами мониторинга различных событий в системе.