

Лабораторная работа №7

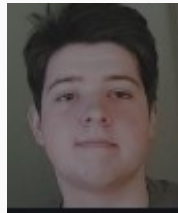
Артём Дмитриевич Петлин

2025-10-18

1. Информация
2. Цель работы
3. Задание
4. Теоретическое введение
5. Выполнение лабораторной работы
6. Выводы

1. Информация

- Петлин Артём Дмитриевич
- студент
- группа НПИбд-02-24
- Российский университет дружбы народов
- 1132246846@pfur.ru
- https://github.com/hikrim/study_2025-2026_os2



2. Цель работы

2.1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

3. Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с `journalctl` (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с `journald` (см. раздел 7.4.4).

4. Теоретическое введение

В системах на базе Unix/Linux важное место при администрировании занимает отслеживание системных событий (и в частности возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журналирование системных событий заключается в фиксировании с помощью сокета syslog в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы.

5. Выполнение лабораторной работы

5.1 Выполнение лабораторной работы

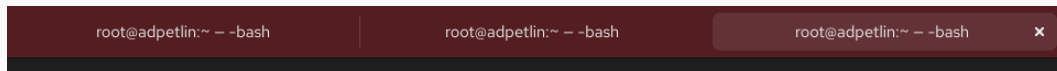


Рисунок 1: su -

Запускаем три вкладки терминала и в каждой из них получаем полномочия администратора.

5.2 Ход работы

```
root@adpetlin:~# tail -f /var/log/messages
Oct 18 19:39:11 adpetlin systemd-logind[935]: New session c3 of user root.
Oct 18 19:39:12 adpetlin systemd[1]: Started session-c3.scope - Session c3 of User root.
Oct 18 19:39:15 adpetlin systemd[5805]: Started run-p8578-i8878.scope - [systemd-run] /usr/bin/bash.
Oct 18 19:39:17 adpetlin systemd[1]: packagekit.service: Deactivated successfully.
Oct 18 19:39:17 adpetlin systemd[1]: packagekit.service: Consumed 15.555s CPU time, 759.9M memory peak.
Oct 18 19:39:20 adpetlin su[8605]: (to root) adpetlin on pts/2
Oct 18 19:39:20 adpetlin systemd-logind[935]: Existing logind session ID 3 used by new audit session, ignoring.
Oct 18 19:39:20 adpetlin systemd-logind[935]: New session c4 of user root.
Oct 18 19:39:20 adpetlin systemd[1]: Started session-c4.scope - Session c4 of User root.
Oct 18 19:39:24 adpetlin systemd[1]: fprintd.service: Deactivated successfully.
```

Рисунок 2: tail

На второй вкладке терминала запускаем мониторинг системных событий в реальном времени, отслеживая общий файл журнала.

5.3 Ход работы

```
Oct 18 19:40:02 adpetlin systemd-logind[935]: Session c4 logged out. Waiting for processes to exit.  
Oct 18 19:40:02 adpetlin systemd-logind[935]: Removed session c4.  
Oct 18 19:40:10 adpetlin systemd[1]: Starting fprintd.service - Fingerprint Authentication Daemon...  
Oct 18 19:40:10 adpetlin systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.  
Oct 18 19:40:14 adpetlin su[8677]: FAILED SU (to root) adpetlin on pts/2  
Oct 18 19:40:40 adpetlin systemd[1]: fprintd.service: Deactivated successfully.
```

Рисунок 3: ctrl + d

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя и пытаемся получить полномочия администратора, вводя неправильный пароль. Наблюдаем появление соответствующей записи во второй вкладке с мониторингом.

```
Oct 18 19:40:10 adpetlin systemd[1]: Started fprintd.service - Fingerprint Authentication Daemon.  
Oct 18 19:40:14 adpetlin su[8677]: FAILED SU (to root) adpetlin on pts/2  
Oct 18 19:40:40 adpetlin systemd[1]: fprintd.service: Deactivated successfully.  
Oct 18 19:41:00 adpetlin adpetlin[8740]: hello  
Oct 18 19:41:10 adpetlin systemd[1]: flatpak-system-helper.service: Deactivated successfully.
```

Рисунок 4: logger

Из оболочки пользователя отправляем тестовое сообщение в системный журнал.
Убеждаемся, что сообщение появляется в режиме реального времени в мониторинге.

5.5 Ход работы

Останавливаем трассировку общего файла журнала и просматриваем последние записи в файле журнала безопасности, где находим сообщения о неудачной попытке авторизации.

```
^C
root@adpetlin:~# tail -n 20 /var/log/secure
Oct 10 21:08:48 adpetlin gdm-password][2414]: pam_unix(gdm-password:session): session opened for user adpetlin(uid=1000) by adpetlin(uid=0)
Oct 10 21:08:48 adpetlin gdm-password][2414]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 10 21:08:52 adpetlin gdm-launch-environment][1261]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 18 19:29:35 adpetlin sshd[1325]: Server listening on 0.0.0.0 port 22.
Oct 18 19:29:35 adpetlin sshd[1325]: Server listening on :: port 22.
Oct 18 19:29:35 adpetlin (systemd)[1376]: pam_unix(systemd-user:session): session opened for user gdm(uid=42) by gdm(uid=0)
Oct 18 19:29:35 adpetlin gdm-launch-environment][1369]: pam_unix(gdm-launch-environment:session): session opened for user gdm(uid=42) by (uid=0)
Oct 18 19:29:55 adpetlin gdm-password][5676]: gkr-pam: unable to locate daemon control file
Oct 18 19:29:55 adpetlin gdm-password][5676]: gkr-pam: stashed password to try later in open session
Oct 18 19:29:55 adpetlin (systemd)[5805]: pam_unix(systemd-user:session): session opened for user adpetlin(uid=1000) by adpetlin(uid=0)
Oct 18 19:29:55 adpetlin gdm-password][5676]: pam_unix(gdm-password:session): session opened for user adpetlin(uid=1000) by adpetlin(uid=0)
Oct 18 19:29:55 adpetlin gdm-password][5676]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct 18 19:30:00 adpetlin gdm-launch-environment][1369]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct 18 19:38:59 adpetlin (systemd)[8447]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct 18 19:39:00 adpetlin su[8429]: pam_unix(su-l:session): session opened for user root(uid=0) by adpetlin(uid=1000)
Oct 18 19:39:12 adpetlin su[8530]: pam_unix(su-l:session): session opened for user root(uid=0) by adpetlin(uid=1000)
Oct 18 19:39:20 adpetlin su[8605]: pam_unix(su-l:session): session opened for user root(uid=0) by adpetlin(uid=1000)
Oct 18 19:40:02 adpetlin su[8605]: pam_unix(su-l:session): session closed for user root
Oct 18 19:40:11 adpetlin unix_chkpwd[8686]: password check failed for user (root)
Oct 18 19:40:11 adpetlin su[8677]: pam_unix(su-l:auth): authentication failure; logname=adpetlin uid=1000 euid=0 tty=/dev/pts/2 ruser=adpetlin rhost= user=root
root@adpetlin:~#
```

Рисунок 5: tail

5.6 Ход работы

```
Installed:
  apr-1.7.5-2.el10.x86_64
  apr-util-lmdb-1.6.3-21.el10.x86_64
  httpd-2.4.63-1.el10_0.2.x86_64
  httpd-filesystem-2.4.63-1.el10_0.2.noarch
  mod_http2-2.0.29-2.el10_0.1.x86_64
  rocky-logos-httpd-100.4-7.el10.noarch
  apr-util-1.6.3-21.el10.x86_64
  apr-util-openssl-1.6.3-21.el10.x86_64
  httpd-core-2.4.63-1.el10_0.2.x86_64
  httpd-tools-2.4.63-1.el10_0.2.x86_64
  mod_lua-2.4.63-1.el10_0.2.x86_64

Complete!
root@adpetlin:~# systemctl start httpd
root@adpetlin:~# systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'
root@adpetlin:~# █
```

Рисунок 6: httpd

Устанавливаем веб-сервер Apache, если он не был установлен ранее. Запускаем веб-службу и добавляем её в автозагрузку.

5.7 Ход работы

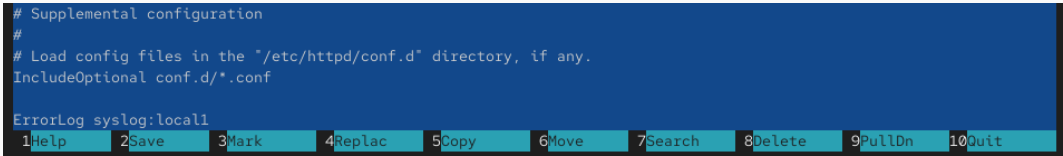
```
root@adpetlin:~# tail -f /var/log/httpd/error_log
[Sat Oct 18 19:43:56.478753 2025] [suexec:notice] [pid 9146:tid 9146] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fe5d:66f3%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 18 19:43:56.500035 2025] [lbmethod_heartbeat:notice] [pid 9146:tid 9146] AH02282: No slotmem from mod_heartmonitor
[Sat Oct 18 19:43:56.500978 2025] [systemd:notice] [pid 9146:tid 9146] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 18 19:43:56.504551 2025] [mpm_event:notice] [pid 9146:tid 9146] AH00489: Apache/2.4.63 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 18 19:43:56.504637 2025] [core:notice] [pid 9146:tid 9146] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'

^C
root@adpetlin:~#
```

Рисунок 7: tail

Просматриваем стандартный журнал ошибок веб-службы в режиме реального времени.

5.8 Ход работы



```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

ErrorLog syslog:local1
```

Рисунок 8: httpd.conf

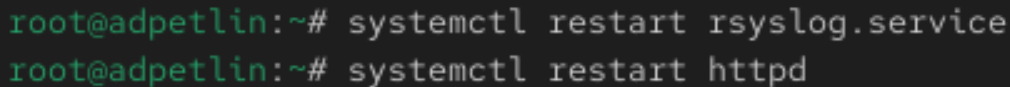
В конфигурационном файле веб-сервера изменяем параметр логирования, чтобы перенаправить сообщения об ошибках в системный журнал, используя специальный локальный объект.



```
/etc/rsyslog.d/httpd.conf  
local1.* -/var/log/httpd-error.log
```

Рисунок 9

В каталоге конфигурации системного журналирования создаём отдельный файл конфигурации для веб-службы. В этом файле указываем правило, которое все сообщения для выбранного локального объекта записывает в отдельный файл.



```
root@adpetlin:~# systemctl restart rsyslog.service
root@adpetlin:~# systemctl restart httpd
```

Рисунок 10: restart

Перезапускаем службу системного журналирования и веб-сервер, чтобы применить новые настройки.

```
root@adpetlin:~# cd /etc/rsyslog.d
root@adpetlin:/etc/rsyslog.d# touch debug.conf
root@adpetlin:/etc/rsyslog.d# echo "*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf
root@adpetlin:/etc/rsyslog.d#
```

Рисунок 11: debug.conf

Создаём ещё один файл конфигурации для системного журналирования, в котором настраиваем запись всех отладочных сообщений в отдельный файл.

```
root@adpetlin:~# systemctl restart rsyslog.service  
root@adpetlin:~#
```

Рисунок 12: echo | restart

Снова перезапускаем службу системного журналирования.

5.13 Ход работы

```
root@adpetlin:~# tail -f /var/log/messages-debug
Oct 18 19:50:49 adpetlin systemd[1]: Stopping rsyslog.service - System Logging Service...
Oct 18 19:50:49 adpetlin rsyslogd[10477]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="10477" x-info="https://www.rsyslog.com"] exiting on signal 15.
Oct 18 19:50:49 adpetlin systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 19:50:49 adpetlin systemd[1]: Stopped rsyslog.service - System Logging Service.
Oct 18 19:50:49 adpetlin systemd[1]: Starting rsyslog.service - System Logging Service...
Oct 18 19:50:49 adpetlin rsyslogd[10782]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="10782" x-info="https://www.rsyslog.com"] start
Oct 18 19:50:49 adpetlin rsyslogd[10782]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Oct 18 19:50:49 adpetlin systemd[1]: Started rsyslog.service - System Logging Service.
```

Рисунок 13: tail

Запускаем мониторинг нового файла с отладочными сообщениями.


```
root@adpetlin:/etc/rsyslog.d# logger -p daemon.debug "Daemon Debug Message"
root@adpetlin:/etc/rsyslog.d#
```

Рисунок 14: logger

```
Oct 18 19:50:49 adpetlin rsyslogd[10782]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="10782" x-info="https://www.rsyslog.com"] start
Oct 18 19:50:49 adpetlin rsyslogd[10782]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https://www.rsyslog.com/e/0 ]
Oct 18 19:50:49 adpetlin systemd[1]: Started rsyslog.service - System Logging Service.
Oct 18 19:51:43 adpetlin root[10846]: Daemon Debug Message
```

Рисунок 15: tail

Отправляем тестовое отладочное сообщение и проверяем его появление в мониторинге.

5.15 Ход работы

```
root@adpetlin:~# journalctl
Oct 18 19:29:26 adpetlin kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro>
Oct 18 19:29:26 adpetlin kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/>
Oct 18 19:29:26 adpetlin kernel: BIOS-provided physical RAM map:
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000100000-0x00000000000dffffffffff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000dffff0000-0x00000000000dffffffffff] ACPI data
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000fec00000-0x00000000000fec00ffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000fee00000-0x00000000000fee00ffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000fffc0000-0x00000000000fffffffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000100000000-0x000000000019ffffffffff] usable
Oct 18 19:29:26 adpetlin kernel: NX (Execute Disable) protection: active
Oct 18 19:29:26 adpetlin kernel: APIC: Static calls initialized
Oct 18 19:29:26 adpetlin kernel: SMBIOS 2.5 present.
Oct 18 19:29:26 adpetlin kernel: DMI: innopetk GmbH VirtualBox/VirtualBox BIOS VirtualBox 12/01/2006
```

Рисунок 16: journalctl

Просматриваем всё содержимое журнала systemd с момента последней загрузки системы, используя постраничный просмотр.

5.16 Ход работы

```
Oct 18 19:53:32 adpetlin dnf[11169]: Extra Packages for Enterprise Linux 10 - x86_64 143 kB/s | 39 kB      00:00
Oct 18 19:53:32 adpetlin dnf[11169]: Rocky Linux 10 - BaseOS                        12 kB/s | 4.3 kB      00:00
Oct 18 19:53:33 adpetlin dnf[11169]: Rocky Linux 10 - AppStream                   14 kB/s | 4.3 kB      00:00
Oct 18 19:53:54 adpetlin dnf[11169]: Rocky Linux 10 - CRB                        0.0 B/s | 0 B         00:21
Oct 18 19:53:54 adpetlin dnf[11169]: Errors during downloading metadata for repository 'crb':
Oct 18 19:53:54 adpetlin dnf[11169]:   - Curl error (7): Could not connect to server for https://mirror.yandex.ru/rockylinux/10.0/CRB/x86_64/os/repodata/repomd.xml [Failed to connect to mirror.yandex.ru port 443 after 21085 ms: Could not connect to server]
Oct 18 19:53:54 adpetlin dnf[11169]: Error: Failed to download metadata for repo 'crb': Cannot download repomd.xml: C
url error (7): Could not connect to server for https://mirror.yandex.ru/rockylinux/10.0/CRB/x86_64/os/repodata/repomd
.xml [Failed to connect to mirror.yandex.ru port 443 after 21085 ms: Could not connect to server]
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Main process exited, code=exited, status=1/FAILURE
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
Oct 18 19:53:54 adpetlin systemd[1]: Failed to start dnf-makecache.service - dnf makecache.
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Consumed 357ms CPU time, 72.4M memory peak.
root@adpetlin:~#
```

Рисунок 17: journalctl

Выводим содержимое журнала без использования пейджера.

5.17 Ход работы

```
root@adpetlin:~# journalctl -f
Oct 18 19:53:32 adpetlin dnf[11169]: Rocky Linux 10 - BaseOS           12 kB/s | 4.3 kB      00:00
Oct 18 19:53:33 adpetlin dnf[11169]: Rocky Linux 10 - AppStream      14 kB/s | 4.3 kB      00:00
Oct 18 19:53:54 adpetlin dnf[11169]: Rocky Linux 10 - CRB           0.0 B/s | 0 B        00:21
Oct 18 19:53:54 adpetlin dnf[11169]: Errors during downloading metadata for repository 'crb':
Oct 18 19:53:54 adpetlin dnf[11169]:   - Curl error (7): Could not connect to server for https://mirror.yandex.ru/rockylinux/10.0/CRB/x86_64/os/repodata/repomd.xml [Failed to connect to mirror.yandex.ru port 443 after 21085 ms: Could not connect to server]
Oct 18 19:53:54 adpetlin dnf[11169]: Error: Failed to download metadata for repo 'crb': Cannot download repomd.xml: C
url error (7): Could not connect to server for https://mirror.yandex.ru/rockylinux/10.0/CRB/x86_64/os/repodata/repomd
.xml [Failed to connect to mirror.yandex.ru port 443 after 21085 ms: Could not connect to server]
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Main process exited, code=exited, status=1/FAILURE
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
Oct 18 19:53:54 adpetlin systemd[1]: Failed to start dnf-makecache.service - dnf makecache.
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Consumed 357ms CPU time, 72.4M memory peak.
^C
root@adpetlin:~#
```

Рисунок 18: journalctl

Запускаем режим просмотра журнала в реальном времени.

```
root@adpetlin:~# journalctl  
Display all 135 possibilities? (y or n)
```

Рисунок 19: journalctl

Изучаем доступные параметры фильтрации для утилиты journalctl.

5.19 Ход работы

```
Oct 18 19:29:27 adpetlin systemd[1]: Finished modprobe@configfs.service - Load Kernel Module configfs.  
Oct 18 19:29:27 adpetlin systemd[1]: Received SIGRTMIN+20 from PID 458 (plymouthd).  
Oct 18 19:29:27 adpetlin systemd[1]: Started plymouth-start.service - Show Plymouth Boot Screen.  
Oct 18 19:29:27 adpetlin systemd[1]: systemd-ask-password-console.path - Dispatch Password Requests to Console Direct  
Oct 18 19:29:27 adpetlin systemd[1]: Started systemd-ask-password-plymouth.path - Forward Password Requests to Plymo  
Oct 18 19:29:27 adpetlin systemd[1]: Reached target paths.target - Path Units.  
Oct 18 19:29:27 adpetlin (udev-worker)[467]: vboxguest: /etc/udev/rules.d/60-vboxadd.rules:1 NAME="vboxguest": Only  
lines 1-43
```

Рисунок 20: journalctl

Просматриваем события, связанные с определённым идентификатором пользователя(UID).

5.20 Ход работы

Ограничиваем вывод журнала,
показывая только последние записи.

```
root@adpetlin:~# journalctl -n 20
Oct 18 19:50:49 adpetlin systemd[1]: rsyslog.service: Deactivated successfully.
Oct 18 19:50:49 adpetlin systemd[1]: Stopped rsyslog.service - System Logging Service.
Oct 18 19:50:49 adpetlin systemd[1]: Starting rsyslog.service - System Logging Service...
Oct 18 19:50:49 adpetlin rsyslogd[10782]: [origin software="rsyslogd" swVersion="8.2412.0-1.el10" x-pid="10782" x-inp
Oct 18 19:50:49 adpetlin rsyslogd[10782]: imjournal: journal files changed, reloading... [v8.2412.0-1.el10 try https
Oct 18 19:50:49 adpetlin systemd[1]: Started rsyslog.service - System Logging Service.
Oct 18 19:51:43 adpetlin root[10846]: Daemon Debug Message
Oct 18 19:53:31 adpetlin systemd[1]: Starting dnf-makecache.service - dnf makecache...
Oct 18 19:53:32 adpetlin dnf[11169]: ELRepo.org Community Enterprise Linux Repository 6.0 kB/s | 3.0 kB 00:00
Oct 18 19:53:32 adpetlin dnf[11169]: Extra Packages for Enterprise Linux 10 - x86_64 143 kB/s | 39 kB 00:00
Oct 18 19:53:32 adpetlin dnf[11169]: Rocky Linux 10 - BaseOS 12 kB/s | 4.3 kB 00:00
Oct 18 19:53:33 adpetlin dnf[11169]: Rocky Linux 10 - AppStream 14 kB/s | 4.3 kB 00:00
Oct 18 19:53:54 adpetlin dnf[11169]: Rocky Linux 10 - CRB 0.0 B/s | 0 B 00:21
Oct 18 19:53:54 adpetlin dnf[11169]: Errors during downloading metadata for repository 'crb':
Oct 18 19:53:54 adpetlin dnf[11169]: - Curl error (7): Could not connect to server for https://mirror.yandex.ru/ro
Oct 18 19:53:54 adpetlin dnf[11169]: Error: Failed to download metadata for repo 'crb': Cannot download repomd.xml: 0
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Main process exited, code=exit, status=1/FAILURE
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Failed with result 'exit-code'.
Oct 18 19:53:54 adpetlin systemd[1]: Failed to start dnf-makecache.service - dnf makecache.
Oct 18 19:53:54 adpetlin systemd[1]: dnf-makecache.service: Consumed 357ms CPU time, 72.4M memory peak.
lines 1-20/20 (END)
```

Рисунок 21: journalctl

5.21 Ход работы

```
root@adpetlin:~# journalctl -p err
Oct 18 19:29:26 adpetlin kernel: RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to RETbleed attacks,>
Oct 18 19:29:27 adpetlin systemd-udevd[432]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignoring.
Oct 18 19:29:27 adpetlin systemd-udevd[432]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignoring.
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hyp>
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to >
Oct 18 19:29:33 adpetlin kernel: Warning: Unmaintained driver is detected: e1000
Oct 18 19:29:33 adpetlin alsactl[960]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use>
Oct 18 19:29:55 adpetlin gdm-password[5676]: gkr-pam: unable to locate daemon control file
Oct 18 19:53:54 adpetlin systemd[1]: Failed to start dnf-makecache.service - dnf makecache.
lines 1-10/10 (END)
```

Рисунок 22: journalctl

Фильтруем сообщения журнала, отображая только сообщения с уровнем ошибки.

5.22 Ход работы

```
root@adpetlin:~# journalctl --since yesterday
Oct 18 19:29:26 adpetlin kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro>
Oct 18 19:29:26 adpetlin kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/>
Oct 18 19:29:26 adpetlin kernel: BIOS-provided physical RAM map:
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff] ACPI data
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000100000000-0x000000019fffffff] usable
```

Рисунок 23: journalctl

Используем временные интервалы для фильтрации записей журнала, например, просматриваем все сообщения за вчерашний день.

5.23 Ход работы

```
root@adpetlin:~# journalctl --since yesterday -p err
Oct 18 19:29:26 adpetlin kernel: RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to RETbleed attacks,>
Oct 18 19:29:27 adpetlin systemd-udevd[432]: /etc/udev/rules.d/60-vboxadd.rules:1 Unknown user 'vboxadd', ignoring.
Oct 18 19:29:27 adpetlin systemd-udevd[432]: /etc/udev/rules.d/60-vboxadd.rules:2 Unknown user 'vboxadd', ignoring.
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hyp>
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
Oct 18 19:29:27 adpetlin kernel: vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to >
Oct 18 19:29:33 adpetlin kernel: Warning: Unmaintained driver is detected: e1000
Oct 18 19:29:33 adpetlin alsactl[960]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw:0 use>
Oct 18 19:29:55 adpetlin gdm-password[5676]: gkr-pam: unable to locate daemon control file
Oct 18 19:53:54 adpetlin systemd[1]: Failed to start dnf-makecache.service - dnf makecache.
lines 1-10/10 (END)
```

Рисунок 24: journalctl

Комбинируем фильтры, просматривая сообщения об ошибках за определённый период.

5.24 Ход работы

```
Sat 2025-10-18 19:29:26.953387 MSK [s=c2c7f1abcb604b108a2688e7ca499fd0;i=1;b=f5937ea3343e4cffa290f197b06f4655;m=2089>
_SOURCE_BOOTTIME_TIMESTAMP=0
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
PRIORITY=5
SYSLOG_FACILITY=0
SYSLOG_IDENTIFIER=kernel
MESSAGE=Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (6>
_BOOT_ID=f5937ea3343e4cffa290f197b06f4655
_MACHINE_ID=e8e6acddfb1248ed931b45f2e426c7b2
_HOSTNAME=adpetlin
_RUNTIME_SCOPE=initrd
```

Рисунок 25: journalctl

Включаем подробный формат вывода для просмотра детальной информации о записях журнала.

```
root@adpetlin:~# journalctl _SYSTEMD_UNIT=sshd.service
Oct 18 19:29:35 adpetlin (sshd)[1325]: sshd.service: Referenced but unset environment variable evaluates to an empty>
Oct 18 19:29:35 adpetlin sshd[1325]: Server listening on 0.0.0.0 port 22.
Oct 18 19:29:35 adpetlin sshd[1325]: Server listening on :: port 22.
root@adpetlin:~#
```

Рисунок 26: journalctl

Для просмотра дополнительной информации о модуле sshd вводим.

5.26 Ход работы

```
password:
Last login: Sat Oct 18 19:45:35 MSK 2025 on pts/2
root@adpetlin:~# mkdir -p /var/log/journal
root@adpetlin:~# chown root:systemd-journal /var/log/journal
root@adpetlin:~# chmod 2755 /var/log/journal
root@adpetlin:~# killall -USR1 systemd-journald
root@adpetlin:~# journalctl -b
Oct 18 19:29:26 adpetlin kernel: Linux version 6.12.0-55.37.1.el10_0.x86_64 (mockbuild@iad1-prod-build001.bld.equ.ro
Oct 18 19:29:26 adpetlin kernel: Command line: BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-55.37.1.el10_0.x86_64 root=/dev/
Oct 18 19:29:26 adpetlin kernel: BIOS-provided physical RAM map:
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x0000000000dfff0000-0x0000000000dfffffff] ACPI data
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff] reserved
Oct 18 19:29:26 adpetlin kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000019fffffffff] usable
Oct 18 19:29:26 adpetlin kernel: NX (Execute Disable) protection: active
Oct 18 19:29:26 adpetlin kernel: APIC: Static calls initialized
Oct 18 19:29:26 adpetlin kernel: SMBIOS 2.5 present.
```

Рисунок 27: journald

6. Выводы

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

Список литературы

1. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: <http://wiki.opennet.ru/Systemd>.
2. Емельянов А. Управление логгированием в systemd. — 2015. — URL: <https://blog.selectel.ru/upravlenie-loggirovaniem-v-systemd/>.
3. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
4. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017.
5. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.