

Управление журналами событий в системе

Майоров Дмитрий Андреевич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Выводы	12

Список иллюстраций

2.1	6
2.2	6
2.3	7
2.4	7
2.5	7
2.6	7
2.7	8
2.8	8
2.9	8
2.10	8
2.11	8
2.12	9
2.13	9
2.14	9
2.15	9
2.16	9
2.17	10
2.18	10
2.19	10
2.20	10
2.21	10
2.22	11

Список таблиц

1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе

2 Выполнение лабораторной работы

Открываем три терминала и в каждом получаем полномочия администратора



Рисунок 2.1

На второй вкладке терминала запускаем мониторинг системных событий в реальном времени

```
root@mayorovda:~# tail -f /var/log/messages
Feb  2 16:22:28 mayorovda kernel: traps: VBoxClient[11237] trap int3 ip:4
1dc5b sp:7feb26c35cd0 error:0 in VBoxClient[1dc5b,400000+bb000]
Feb  2 16:22:28 mayorovda systemd-coredump[11238]: Process 11234 (VBoxCli
ent) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb  2 16:22:28 mayorovda systemd[1]: Started systemd-coredump@645-11238-
0.service - Process Core Dump (PID 11238/UID 0).
Feb  2 16:22:29 mayorovda systemd-coredump[11239]: Process 11234 (VBoxCli
```

Рисунок 2.2

В третьей вкладке терминала возвращаемся к учётной записи своего пользователя и пробуем получить полномочия администратора, но вводим неправильный пароль. Во второй вкладке терминала с мониторингом событий или ничего не отображается сообщение об ошибке

```

root@mayorovda:~# tail -f /var/log/messages
Feb 2 16:23:13 mayorovda kernel: traps: VBoxClient[11369] trap int3 ip:4
1dc5b sp:7feb26c35cd8 error:0 in VBoxClient[1dc5b,400000+b000]
Feb 2 16:23:15 mayorovda systemd[1]: Started systemd-coredump@654-11352-0.service
e: Deactivated successfully.
Feb 2 16:23:19 mayorovda su[11345]: FAILED SU (to root) mayorovda on pts/2
Feb 2 16:23:20 mayorovda kernel: traps: VBoxClient[11369] trap int3 ip:4
1dc5b sp:7feb26c35cd8 error:0 in VBoxClient[1dc5b,400000+b000]
Feb 2 16:23:20 mayorovda systemd-coredump[11370]: Process 11366 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb 2 16:23:21 mayorovda systemd[1]: Started systemd-coredump@655-11370-0.service - Process Core Dump (PID 11370/UID 0).

```

Рисунок 2.3

В третьей вкладке терминала из оболочки пользователя вводим logger hello.

Во второй вкладке терминала с мониторингом событий видим это же сообщение

```

root@mayorovda:~# tail -f /var/log/messages
Feb 2 16:23:36 mayorovda systemd[1]: Started systemd-coredump@658-11401-0.service
e: Deactivated successfully.
Feb 2 16:23:41 mayorovda mayorovda[11409]: hello
Feb 2 16:23:41 mayorovda kernel: traps: VBoxClient[11414] trap int3 ip:4
1dc5b sp:7feb26c35cd8 error:0 in VBoxClient[1dc5b,400000+b000]
Feb 2 16:23:41 mayorovda systemd-coredump[11415]: Process 11411 (VBoxClient) of user 1000 terminated abnormally with signal 5/TRAP, processing...
Feb 2 16:23:41 mayorovda systemd[1]: Started systemd-coredump@659-11415-0.service - Process Core Dump (PID 11415/UID 0).

```

Рисунок 2.4

Во второй вкладке терминала запускаем мониторинг сообщений безопасности

```

root@mayorovda:~# tail -n 20 /var/log/secure
Feb 2 14:32:21 mayorovda gdm-launch-environment][1418]: pam_unix(gdm
nch-environment:session): session closed for user gdm

```

Рисунок 2.5

В первой вкладке терминала устанавливаем Apache

```

root@mayorovda:~# dnf -y install httpd

```

Рисунок 2.6

Запускаем веб-службу

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

Рисунок 2.7

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

```
root@mayorovda:~# tail -f /var/log/httpd/error_log
[Mon Feb 02 16:24:44.939361 2026] [suexec:notice] [pid 11796:tid 11796] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
```

Рисунок 2.8

Открываем файл /etc/httpd/conf/httpd.conf для редактирования и вводим в конце следующую строку

```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ErrorLog syslog:local1
```

Рисунок 2.9

В каталоге /etc/rsyslog.d создаем файл мониторинга событий веб-службы

```
root@mayorovda:~# cd /etc/rsyslog.d
root@mayorovda:/etc/rsyslog.d# touch httpd.conf
```

Рисунок 2.10

Открываем его для редактирования и прописываем там следующую строку

```
GNU nano 8.1                                     httpd.conf
local1.* -/var/log/httpd-error.log
```

Рисунок 2.11

В первой вкладке терминала перезагружаем конфигурацию rsyslogd и веб-службу

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

Рисунок 2.12

В третьей вкладке терминала создаем отдельный файл конфигурации для мониторинга отладочной информации и вводим туда нужную команду

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

Рисунок 2.13

первой вкладке терминала снова перезапускаем rsyslogd

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

Рисунок 2.14

Во второй вкладке терминала запускаем мониторинг отладочной информации, а в третьей вкладке терминала вводим следующую команду. В терминале с мониторингом смотрим сообщение отладки

```
root@mayorovda:~# tail -f /var/log/messages-debug
```

Рисунок 2.15

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

Рисунок 2.16

Во второй вкладке терминала смотрим содержимое журнала с событиями с момента последнего запуска системы

```
root@mayorovda:~# journalctl  
Feb 02 14:31:57 mayorovda.localdomain kernel: Linux version 6.12.0-124.8  
Feb 02 14:31:57 mayorovda.localdomain kernel: Command line: BOOT_IMAGE=(  
Feb 02 14:31:57 mayorovda.localdomain kernel: BTAC_maintenance_start DARM
```

Рисунок 2.17

Смотрим содержимое журнала без пейджера

```
root@mayorovda:~# journalctl --no-pager
```

Рисунок 2.18

Смотрим журнал в реальном времени

```
root@mayorovda:~# journalctl -f
```

Рисунок 2.19

Смотрим последние 20 строк журнала, сообщения об ошибках, все сообщения со вчерашнего дня, детальную информацию и доп. информацию о модуле sshd

```
root@mayorovda:~# journalctl _UID=0
```

Рисунок 2.20

```
root@mayorovda:~# journalctl -p err  
Feb 02 14:31:57 mayorovda.localdomain kernel: RETBleed: WARNING: Spectre  
Feb 02 14:31:57 mayorovda.localdomain kernel: Warning: Unmaintained driv  
Feb 02 14:31:57 mayorovda.localdomain kernel: Warning: Unmaintained driv
```

Рисунок 2.21

Создаем каталог для хранения записей журнала. Корректируем права доступа для каталога /var/log/journal, чтобы journald смог записывать в него информацию. Используем команду для принятия изменений. Смотрим сообщения журнала с момента перезагрузки

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Mon Feb  2 16:30:22 MSK 2026 on pts/5
root@mayorovda:~# mkdir -p /var/log/journal
root@mayorovda:~# chown root:systemd-journal /var/log/journal
root@mayorovda:~# chmod 2755 /var/log/journal
root@mayorovda:~# killall -USR1 systemd-journald
root@mayorovda:~# journalctl -b
Feb 02 14:31:57 mayorovda.localdomain kernel: Linux version 6.12.0-124.8
Feb 02 14:31:57 mayorovda.localdomain kernel: Command line: ROOT TIMAGE=/
```

Рисунок 2.22

3 Выводы

Получены навыки работы с журналами мониторинга различных событий в системе