

Отчет по лабораторной работе №7

Отчет о мониторинге и настройке системных журналов

Лупупа Чилеше

Цель работ

Основными задачами этой лаборатории были:

Отслеживайте журналы системных событий в режиме реального времени.

Настройте rsyslog для регистрации ошибок веб-сервера.

Используйте журналстl для эффективного мониторинга журналов.

Включите постоянное хранилище для журналов Journald.

Выполнение лабораторной работы

Мониторинг системных журналов в режиме реального времени

Запустил три терминальные сессии.

Получил root-права на каждом терминале с помощью su.

Во втором терминале инициирован мониторинг в реальном времени с помощью:

`tail -f /var/log/messages`

```
[root@chileshepupa ~]# tail -f /var/log/messages-debug
Dec 28 16:42:13 chileshepupa systemd[1]: Stopping System Logging Service...
Dec 28 16:42:13 chileshepupa rsyslogd[42779]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42779" x
-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 28 16:42:13 chileshepupa systemd[1]: rsyslog.service: Deactivated successfully.
Dec 28 16:42:13 chileshepupa systemd[1]: Stopped System Logging Service.
Dec 28 16:42:13 chileshepupa systemd[1]: Starting System Logging Service...
Dec 28 16:42:13 chileshepupa rsyslogd[42797]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42797" x
-info="https://www.rsyslog.com"] start
Dec 28 16:42:13 chileshepupa systemd[1]: Started System Logging Service.
Dec 28 16:42:13 chileshepupa rsyslogd[42797]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try h
ttps://www.rsyslog.com/e/0 ]
```

Попытка входа в систему с неправильным паролем с использованием su в третьем терминале, что вызвало запись в системном журнале.

- Проверено сообщение журнала событий «FAILED SU (to root)», появляющееся в контролируемом терминале.

```
Dec 28 15:39:58 chileshepupa su[3464]: FAILED SU (to root) lchileshe on pts/2
```

Зарегистрировал пользовательское сообщение, используя:

```
[lchileshe@chileshepupa ~]$ logger hello
[lchileshe@chileshepupa ~]$
```

2. Настройка rsyslog для ведения журнала веб-сервера

➤ Установленный веб-сервер Apache:

```
[root@chileshepupa ~]# dnf -y install httpd
Last metadata expiration check: 0:27:23 ago on Sat 28 Dec 2024 03:58:05 PM MSK.
Dependencies resolved.
=====
Package                                Architecture      Version            Repository          Size
=====
Installing:
  httpd                                x86_64            2.4.62-1.el9       appstream            45 k
Installing dependencies:
  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            2.4.62-1.el9       appstream            1.4 M
  httpd-filesystem                   noarch            2.4.62-1.el9       appstream            12 k
  httpd-tools                        x86_64            2.4.62-1.el9       appstream            79 k
  rocky-logos-httpd                 noarch            90.15-2.el9        appstream            24 k
Installing weak dependencies:
  apr-util-openssl                   x86_64            1.6.1-23.el9       appstream            14 k
  mod_http2                          x86_64            2.0.26-2.el9_4.1   appstream            163 k
  mod_lua                            x86_64            2.4.62-1.el9       appstream            58 k
=====
Transaction Summary
=====
Install 11 Packages

Total download size: 2.0 M
Installed size: 6.1 M
```

➤ Запустил и включил службу:

```
[root@chileshepupa ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@chileshepupa ~]#
```

➤ Проверенные журналы ошибок с:

```
[root@chileshepupa ~]# tail -f /var/log/httpd/error_log
[Sat Dec 28 16:26:39.832185 2024] [core:notice] [pid 30274:tid 30274] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Sat Dec 28 16:26:39.834968 2024] [suexec:notice] [pid 30274:tid 30274] AH01232: suEXEC mechanism enabled (wrapper: /u
sr/sbin/suexec)
[Sat Dec 28 16:26:39.984720 2024] [lbmethod_heartbeat:notice] [pid 30274:tid 30274] AH02282: No slotmem from mod_heart
monitor
[Sat Dec 28 16:26:39.991747 2024] [mpm_event:notice] [pid 30274:tid 30274] AH00489: Apache/2.4.62 (Rocky Linux) config
ured -- resuming normal operations
[Sat Dec 28 16:26:39.991795 2024] [core:notice] [pid 30274:tid 30274] AH00094: Command line: '/usr/sbin/httpd -D FOREG
ROUND'
```

- Отредактировал файл конфигурации /etc/httpd/conf/httpd.conf, добавив строку:

ErrorLog syslog:local1

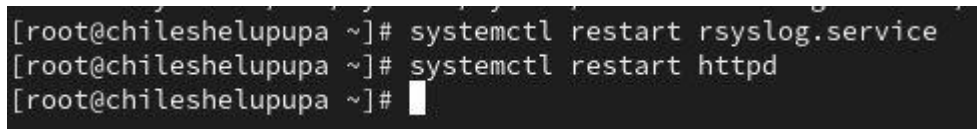
- Создал собственный файл конфигурации rsyslog /etc/rsyslog.d/httpd.conf:

local1.* -/var/log/httpd-error.log



```
GNU nano 5.6.1 httpd.conf
local1.* -/var/log/httpd-error.log
```

Перезапустил rsyslog и Apache:



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

3. Ведение журнала отладки

Создал и настроил файл журнала отладки /etc/rsyslog.d/debug.conf:



```
[root@chilesheLupupa rsyslog.d]# echo "*.debug /var/log/messages-debug" >/etc/rsyslog.d/debug.conf
[root@chilesheLupupa rsyslog.d]#
```

- Перезапустил rsyslog:

systemctl restart rsyslog.service

- Verified debug log monitoring:

tail -f /var/log/messages-debug

```
[root@chileshepupa ~]# tail -f /var/log/messages-debug
Dec 28 16:42:13 chileshepupa systemd[1]: Stopping System Logging Service...
Dec 28 16:42:13 chileshepupa rsyslogd[42779]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42779" x
-info="https://www.rsyslog.com"] exiting on signal 15.
Dec 28 16:42:13 chileshepupa systemd[1]: rsyslog.service: Deactivated successfully.
Dec 28 16:42:13 chileshepupa systemd[1]: Stopped System Logging Service.
Dec 28 16:42:13 chileshepupa systemd[1]: Starting System Logging Service...
Dec 28 16:42:13 chileshepupa rsyslogd[42797]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="42797" x
-info="https://www.rsyslog.com"] start
Dec 28 16:42:13 chileshepupa systemd[1]: Started System Logging Service.
Dec 28 16:42:13 chileshepupa rsyslogd[42797]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try h
tps://www.rsyslog.com/e/0 ]
```

Протестировано с:

logger -p daemon.debug "Daemon Debug Message"

```
Dec 28 15:37:13 chileshepupa systemd[1]: fprintd.service: Deactivated successfully.
Dec 28 15:37:13 chileshepupa systemd[1823]: Started VTE child process 3340 launched lchileshe@chileshepupa:~ process
2638.
Dec 28 15:37:31 chileshepupa systemd[1]: Starting Fingerprint Authentication Daemon...
Dec 28 15:37:31 chileshepupa systemd[1]: Started Fingerprint Authentication Daemon.
Dec 28 15:37:35 chileshepupa su[3382]: (to root) lchileshe on pts/2
Dec 28 15:38:01 chileshepupa systemd[1]: fprintd.service: Deactivated successfully.
Dec 28 15:38:05 chileshepupa systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Dec 28 15:38:37 chileshepupa systemd[1823]: Created slice User Background Tasks Slice.
Dec 28 15:38:37 chileshepupa systemd[1823]: Starting Cleanup of User's Temporary Files and Directories...
Dec 28 15:38:37 chileshepupa systemd[1823]: Finished Cleanup of User's Temporary Files and Directories.
Dec 28 15:39:53 chileshepupa systemd[1]: Starting Fingerprint Authentication Daemon...
Dec 28 15:39:53 chileshepupa systemd[1]: Started Fingerprint Authentication Daemon.
Dec 28 15:39:58 chileshepupa su[3464]: FAILED SU (to root) lchileshe on pts/2
Dec 28 15:40:23 chileshepupa systemd[1]: fprintd.service: Deactivated successfully.
Dec 28 15:41:18 chileshepupa systemd[1]: Starting Fingerprint Authentication Daemon...
Dec 28 15:41:19 chileshepupa systemd[1]: Started Fingerprint Authentication Daemon.
Dec 28 15:41:49 chileshepupa systemd[1]: fprintd.service: Deactivated successfully.
Dec 28 15:42:57 chileshepupa systemd[1]: Starting Cleanup of Temporary Directories...
Dec 28 15:42:57 chileshepupa systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Dec 28 15:42:57 chileshepupa systemd[1]: Finished Cleanup of Temporary Directories.
Dec 28 15:42:57 chileshepupa systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated suc
cessfully.
```

4. Мониторинг с помощью Journalctl

- Просмотрел полные логи:

Journalctl

```
[root@chileshelepupa ~]# journalctl
Dec 28 15:27:45 chileshelepupa.localdomain kernel: Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-bu>
Dec 28 15:27:45 chileshelepupa.localdomain kernel: The list of certified hardware and cloud instances for Enterprise >
Dec 28 15:27:45 chileshelepupa.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_>
Dec 28 15:27:45 chileshelepupa.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regis>
Dec 28 15:27:45 chileshelepupa.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Dec 28 15:27:45 chileshelepupa.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Dec 28 15:27:45 chileshelepupa.localdomain kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Dec 28 15:27:45 chileshelepupa.localdomain kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, u>
Dec 28 15:27:45 chileshelepupa.localdomain kernel: signal: max sigframe size: 1776
Dec 28 15:27:45 chileshelepupa.localdomain kernel: BIOS-provided physical RAM map:
```

- Мониторинг журналов в режиме реального времени:

journalctl -f

Результаты и наблюдения

Успешно отслеживал системные события и входы пользователей в режиме реального времени.

Настроен rsyslog для регистрации ошибок веб-сервера Apache.

Проверено правильность хранения отладочных и пользовательских сообщений журнала.

Включено и протестировано постоянное ведение журналов.

Заключение

В ходе этой лабораторной работы был предоставлен практический опыт мониторинга системных журналов, настройки пользовательских правил ведения журналов и эффективного управления системными журналами с помощью Journald и rsyslog. Овладение этими методами необходимо для эффективного системного администрирования и устранения неполадок.