Лабораторная работа №7

Управление журналами событий в системе

Тукаев Тимур

9 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить навыки работы с журналами мониторинга различных событий в системе Linux, освоить использование служб `rsyslogd` и `journald`, а также методы фильтрации и анализа сообщений.

Ход выполнения работы

Мониторинг системных событий

Рис. 1: Мониторинг системных сообщений

Запуск `tail -f /var/log/messages` для просмотра событий ядра и служб в реальном времени.

Ошибка аутентификации root

Рис. 2: Ошибка при вводе пароля root

Попытка входа с неверным паролем приводит к записи `FAILED SU (to root)` в системный журнал.

Отправка пользовательского сообщения

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# tail -n 20 /var/log/secure
Oct  9 13:49:03 titukaev gdm-password]:[1994]: gkr-pam: stashed password to try later in open session
Oct  9 13:49:03 titukaev (systemd)[2005]: pam_unix(systemd-user:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)
Oct  9 13:49:03 titukaev gdm-password]:[1994]: pam_unix(gdm-password:session): session opened for user titukaev(uid=1000) by titukaev(uid=0)
Oct  9 13:49:03 titukaev gdm-password]:[1994]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Oct  9 13:49:09 titukaev gdm-launch-environment]:[1247]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Oct  9 13:49:41 titukaev (systemd)[3216]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct  9 13:49:41 titukaev su[3183]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 13:57:39 titukaev su[3183]: pam_unix(su:session): session closed for user root
Oct  9 13:58:16 titukaev (systemd)[4644]: pam_unix(systemd-user:session): session opened for user root(uid=0) by root(uid=0)
Oct  9 13:58:16 titukaev su[4619]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 14:05:19 titukaev su[4619]: pam_unix(su:session): session closed for user root
Oct  9 14:05:25 titukaev su[5649]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 14:10:14 titukaev su[5649]: pam_unix(su:session): session closed for user root
Oct  9 14:15:22 titukaev gdm-password]:[6995]: gkr-pam: unlocked login keyring
Oct  9 14:18:10 titukaev su[7376]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 14:18:17 titukaev su[7443]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 14:18:22 titukaev su[7503]: pam_unix(su:session): session opened for user root(uid=0) by titukaev(uid=1000)
Oct  9 14:18:36 titukaev su[7503]: pam_unix(su:session): session closed for user root
Oct  9 14:18:40 titukaev unix_chkpwd[7589]: password check failed for user (root)
Oct  9 14:18:40 titukaev su[7574]: pam_unix(su:auth): authentication failure; logname=titukaev uid=1000 euid=0 tty=/dev/pts/1 ruser=titukaev rh
ost=  user=root
root@titukaev:/home/titukaev#
```

Рис. 3: Регистрация пользовательского сообщения

Команда `logger hello` добавляет сообщение в `/var/log/messages`.

Рис. 4: Настройка передачи логов Apache в rsyslog

Добавлена строка `ErrorLog syslog:local1` в `/etc/httpd/conf/httpd.conf`.

Создание отдельного файла для логов Apache

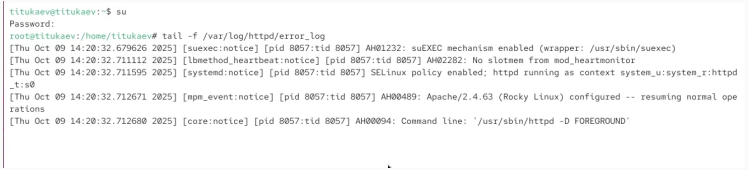

Рис. 5: Создание конфигурации rsyslog

Создан файл `/etc/rsyslog.d/httpd.conf` с правилом `local1.* -/var/log/httpd-error.log`.

Настройка отладочного журнала

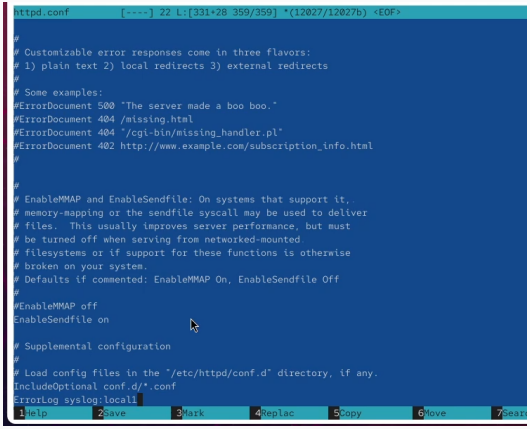

Рис. 6: Создание debug.conf для отладки

Добавлено правило `*.debug /var/log/messages-debug` для регистрации отладочной

Проверка работы rsyslog

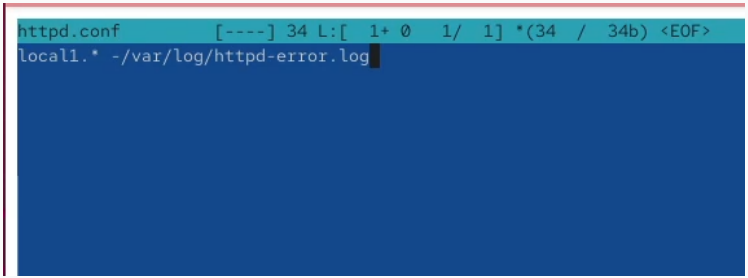

Рис. 7: Регистрация отладочного сообщения

Сообщение `Daemon Debug Message` успешно зафиксировано в `/var/log/messages-debug`.

Использование journalctl

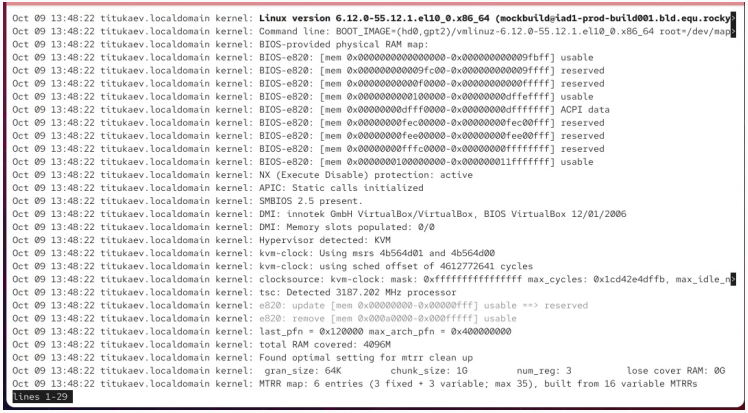

Рис. 8: Просмотр журнала через journalctl

Просмотр системных сообщений, фильтрация по UID и модулю `sshd.service`.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# mkdir -p /var/log/journal
root@titukaev:/home/titukaev# chown root:systemd-journal /var/log/journal/
root@titukaev:/home/titukaev# chmod 2755 /var/log/journal/
root@titukaev:/home/titukaev# killall -USR1 systemd-journald
root@titukaev:/home/titukaev#
```

Рис. 9: Создание каталога для постоянного хранения журнала

Создан каталог `/var/log/journal` и настроены права для обеспечения постоянного хранения логов.

Итоги работы

Вывод

В результате лабораторной работы изучены инструменты системного журналирования Linux.

Настроено взаимодействие служб `rsyslogd` и `journald`, реализовано хранение логов в постоянном режиме.

Получены навыки фильтрации, анализа и управления системными событиями.