Отчет по лабораторной работе №7

Отчет о мониторинге и настройке системных журналов

Лупупа Чилеше

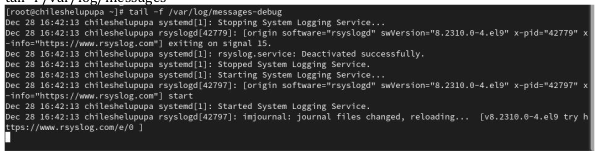
Содержание

# 1 Цель работы

Основными задачами этой лаборатории были: Отслеживайте журналы системных событий в режиме реального времени. Настройте rsyslog для регистрации ошибок веб-сервера. Используйте журналctl для эффективного мониторинга журналов. Включите постоянное хранилище для журналов Journald.

## 1.1 Мониторинг системных журналов в режиме

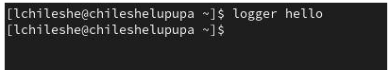
1. Запустил три терминальные сессии. Получил root-права на каждом терминале с помощью su. Во втором терминале инициирован мониторинг в реальном времени с помощью: tail -f /var/log/messages



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

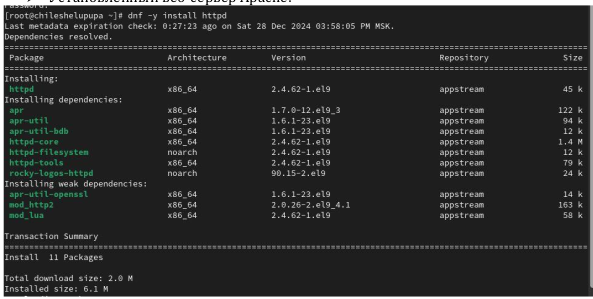
fig:

1. Зарегистрировал пользовательское сообщение, используя: logger hello



## 1.2 Настройка rsyslog для ведения журнала веб-сервера

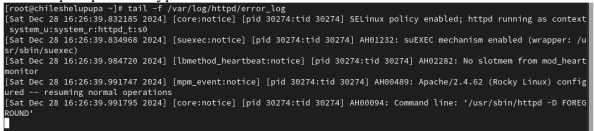
1. Установленный веб-сервер Apache:



1. Запустил и включил службу:

fig:

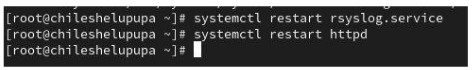
1. Проверенные журналы ошибок с:



1. Создал собственный файл конфигурации rsyslog /etc/rsyslog.d/httpd.conf: local1.\* -/var/log/httpd-error.log



1. Перезапустил rsyslog и Apache:

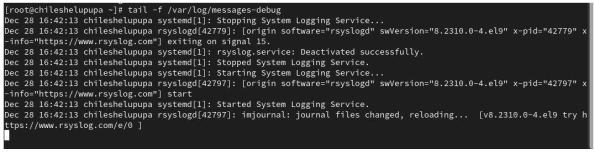


## 1.3 Ведение журнала отладки

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

fig:

1. Verified debug log monitoring: tail -f /var/log/messages-debug

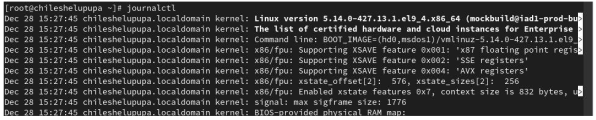


1. Протестировано с: logger -p daemon.debug “Daemon Debug Message”



## 1.4 Мониторинг с помощью Journalctl

1. Просмотрел полные логи: Journalctl



1. Мониторинг журналов в режиме реального времени: journalctl -f

## 1.5 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.

## 1.6 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.