# Лабораторная работа №15

## Настройка сетевого журналирования

Газизянов Владислав Альбертович

2025-12-13

# Содержание I

# 1. Цели и задачи

**Цель:** Получение навыков работы с журналами системных событий и настройки централизованного журналирования
**Задачи:** - Настройка сервера сетевого журналирования - Конфигурация клиентов для передачи логов - Использование инструментов анализа журналов - Автоматизация развертывания системы

# 2. Настройка сервера журналирования

**Конфигурация rsyslog:** - Создание конфигурационных файлов - Активация TCP-приёмника на порту 514 - Перезапуск службы rsyslog - Проверка работы сервера

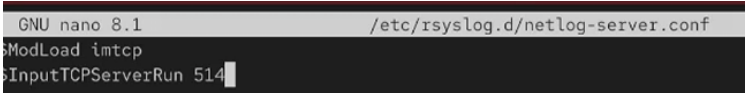



Рисунок 1: Конфигурация TCP-приёмника rsyslog

# 3. Сетевая безопасность

**Настройка firewall:** - Открытие TCP-порта 514 - Добавление постоянных правил - Проверка доступности сервера - Обеспечение защищённого обмена

```
 *:shell (LISTEN)
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рисунок 2: Настройка firewall для сетевого журналирования

# 4. Клиентская конфигурация

**Перенаправление логов:** - Создание клиентских конфигураций - Настройка отправки сообщений на сервер - Перезапуск клиентских служб - Проверка соединения с сервером


Рисунок 3: Настройка перенаправления логов на сервер

# 5. Мониторинг журналов в реальном времени

**Отслеживание событий:** - Использование команды tail -f - Анализ сообщений от разных хостов - Выявление системных проблем - Мониторинг работы служб

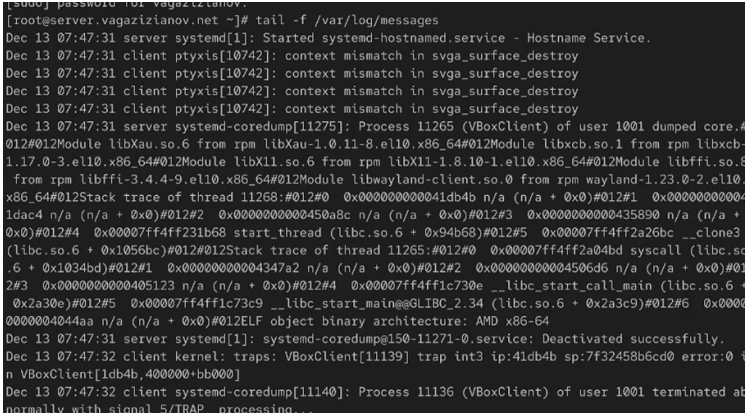
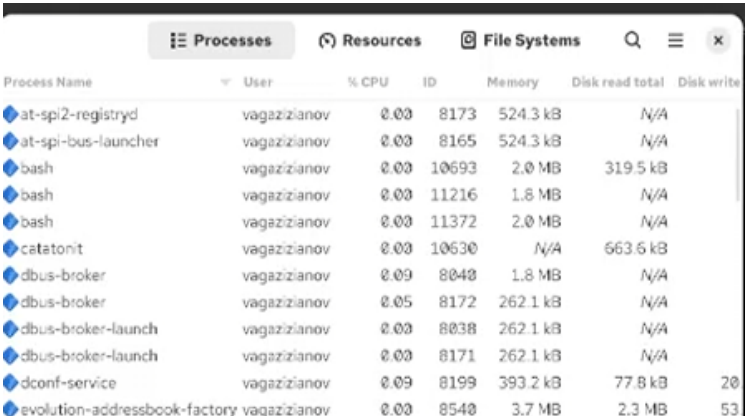



Рисунок 4: Мониторинг журнала сообщений в реальном времени

# 6. Графические инструменты анализа

**Использование системного монитора:** - Запуск gnome-system-monitor - Просмотр различных категорий событий - Анализ сообщений от клиентов - Визуализация системной информации



# 7. Установка специализированных инструментов

**Расширенные возможности анализа:** - Установка просмотрщика lnav - Настройка цветового выделения - Использование фильтров и поиска - Анализ структурированных логов

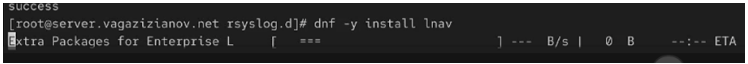
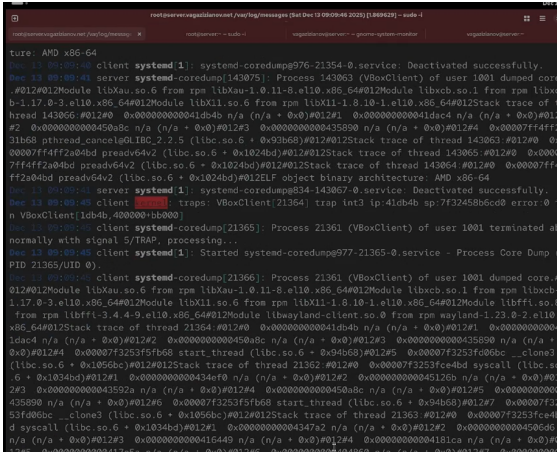



Рисунок 6: Установка просмотрщика журналов lnav

# 8. Продвинутый анализ журналов

**Работа с lnav:** - Просмотр и фильтрация сообщений - Анализ временных меток - Поиск ошибок и предупреждений - Мониторинг сетевой активности



# 9. Автоматизация развертывания

**Скрипты provisioning:** - Разработка скриптов для сервера и клиентов - Автоматическая настройка конфигураций - Интеграция с системой виртуализации - Тестирование работы автоматизации

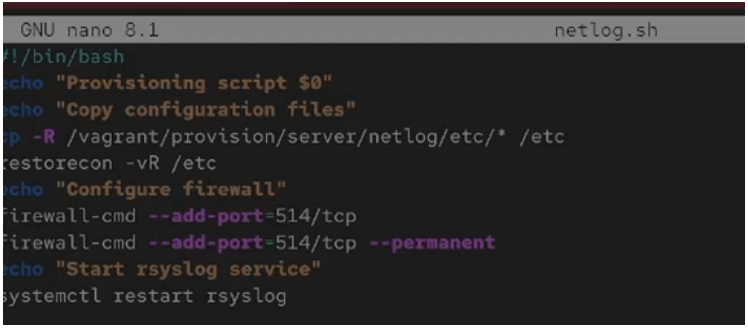



Рисунок 8: Скрипт настройки сервера журналирования

# 10. Выводы

**Результаты работы:** - Освоена настройка сервера сетевого журналирования - Приобретён опыт конфигурации клиентских устройств - Изучены инструменты анализа системных логов - Разработана система автоматизации развертывания - Освоены методы диагностики на основе журналов - Получены навыки обеспечения безопасности журналирования