Лабораторная работа №15

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

Раздел 1

1. Цель работы

1.1 Цель работы

- Получение навыков по работе с журналами системных событий

Раздел 2

2. Выполнение лабораторной работы

2.1 Настройка сервера сетевого журнала

- Переход в каталог `/etc/rsyslog.d`
- Создание файла `netlog-server.conf`
- Подготовка конфигурации для сетевого хранения журналов

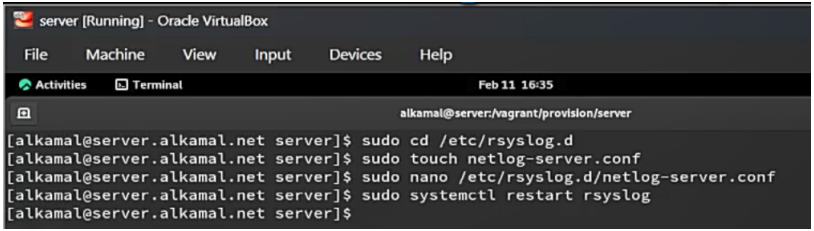


Рисунок 1: Создание файла конфигурации rsyslog netlog-server.conf

- Включён приём журналов по TCP-порту 514
- Загружен модуль `imtcp`
- Активирован сервер ввода `$InputTCPServerRun 514`

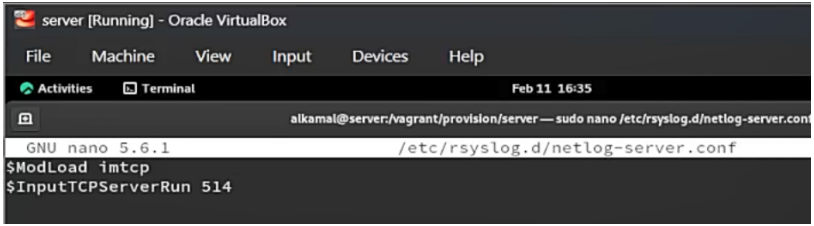


Рисунок 2: Настройка приёма журналов по TCP 514 в rsyslog

- Перезапущена служба `rsyslog`
- Выполнена проверка портов командой `lsof | grep TCP`
- Подтверждено состояние LISTEN для `rsyslog`

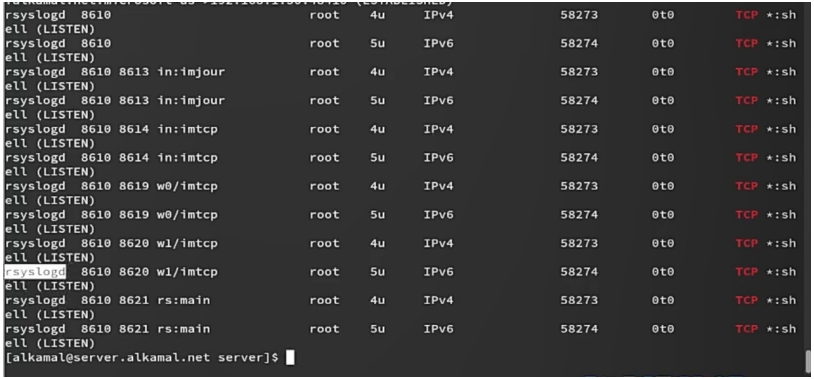


Рисунок 3: Проверка прослушиваемых TCP-портов службой rsyslog

- Открыт TCP-порт 514 в `firewalld`
- Добавлено временное и постоянное правило
- Разрешён приём сетевых сообщений журнала

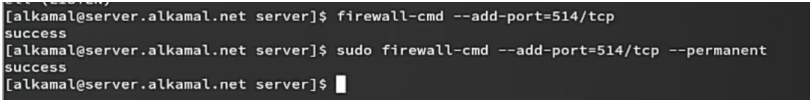


Рисунок 4: Настройка firewalld для открытия TCP-порта 514

2.2 Настройка клиента сетевого журнала

- Переход в каталог `/etc/rsyslog.d`
- Создание файла `netlog-client.conf`
- Подготовка конфигурации отправки журналов

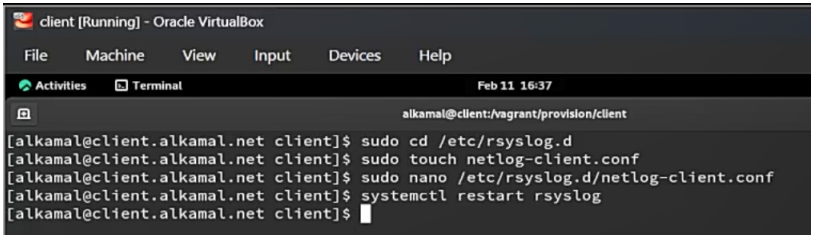


Рисунок 5: Создание файла конфигурации netlog-client.conf на клиенте

- Настроено перенаправление `*.* @@server.alkamal.net:514`
- Использован протокол TCP (@@)
- Организована передача всех сообщений на сервер
- Перезапущена служба `rsyslog`
- Применена новая конфигурация клиента

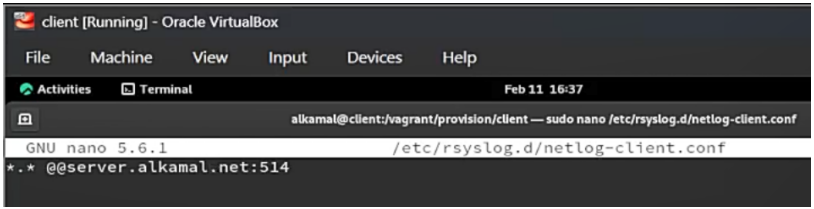


Рисунок 6: Настройка перенаправления журналов на сервер по TCP 514

2.3 Просмотр журнала

- Выполнен просмотр `/var/log/messages` с помощью `tail -f`
- Отображаются записи `server` и `client`
- Подтверждён приём удалённых журналов

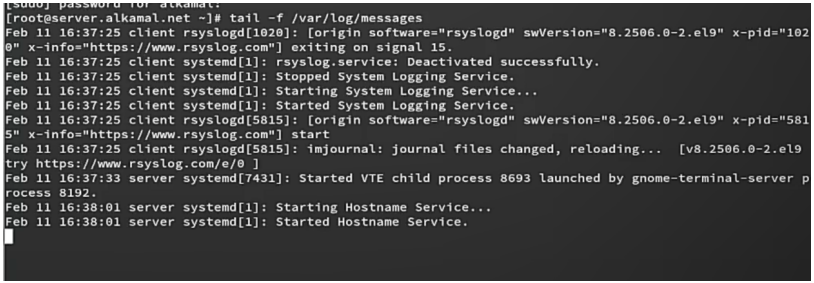
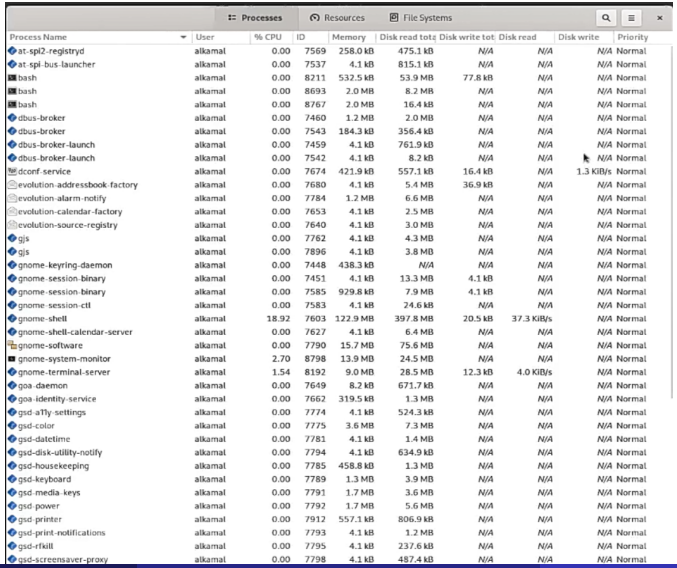


Рисунок 7: Просмотр журнала /var/log/messages на сервере

- Запущена программа `gnome-system-monitor`
- Отображены процессы, PID, использование CPU и памяти



- Установлен пакет `lnav` через `dnf`
- Подтверждена успешная установка версии `0.11.1-1.el9`

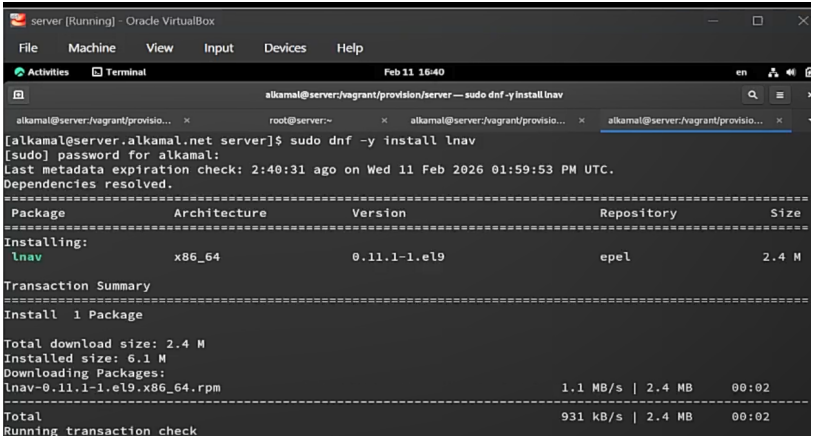
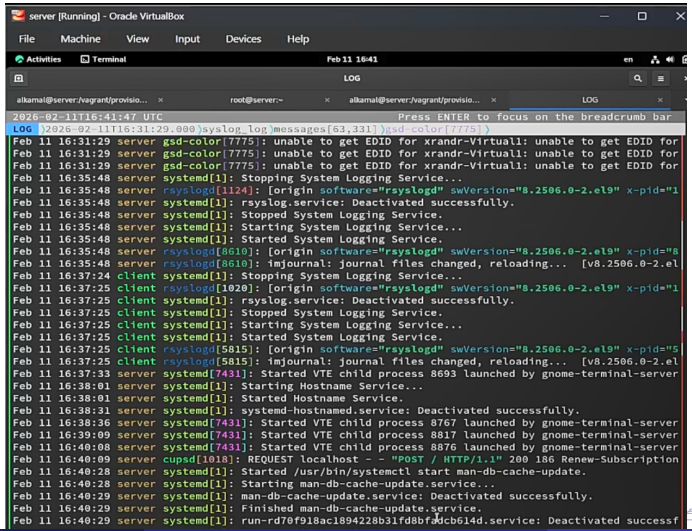


Рисунок 9: Установка lnav на сервере

- Выполнен просмотр журналов с помощью `lnav`
- Отображаются записи сервера и клиента
- Видны сообщения `systemd`, `rsyslog`, `cupsd`



- Установлен пакет `lnav` на клиенте
- Подтверждена подготовка к установке

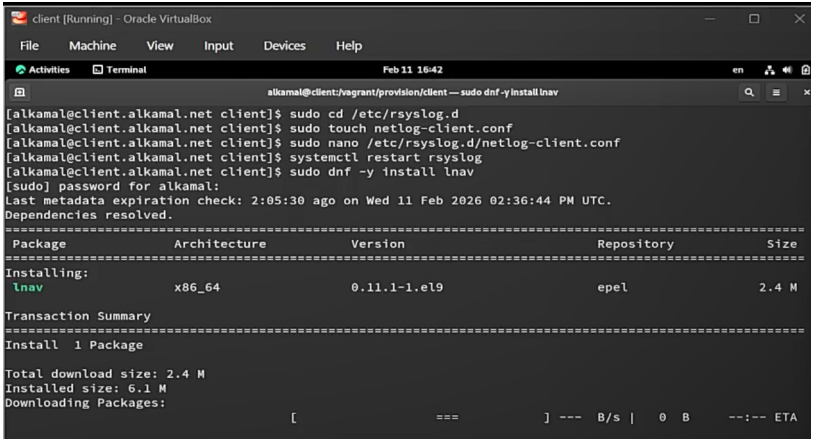
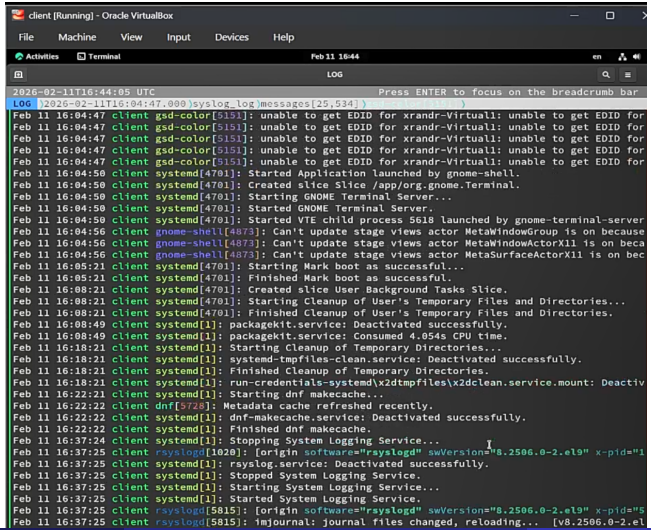


Рисунок 11: Установка lnav на клиенте

- Выполнен просмотр журналов клиента через `lnav`
- Отображаются записи `systemd`, `rsyslog`, `packagekit`
- Подтверждена корректная работа логирования



2.4 Внесение изменений в настройки внутреннего

- Переход в `/vagrant/provision/server`
- Создание каталога `netlog/etc/rsyslog.d`
- Копирование `netlog-server.conf`
- Подготовка структуры provisioning

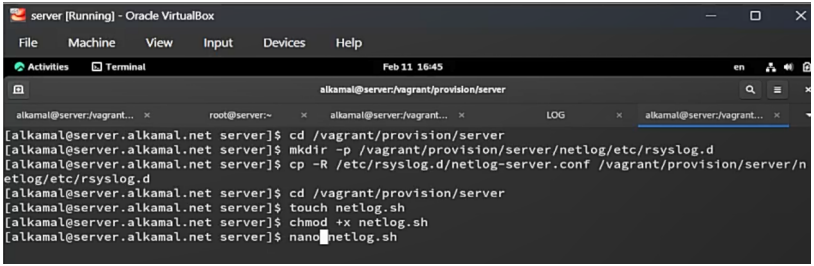
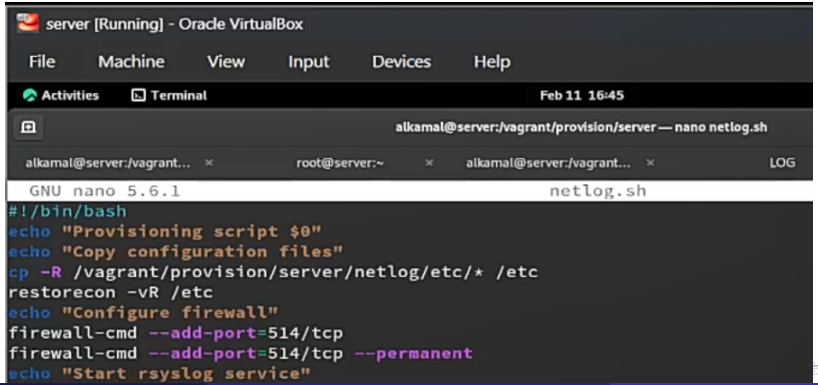


Рисунок 13: Создание каталога netlog и копирование конфигурации rsyslog

- Создан исполняемый скрипт `netlog.sh`
- Назначены права выполнения
- Добавлена автоматическая настройка
- Копирование файлов в `/etc`
- Восстановление контекстов SELinux
- Открытие порта 514
- Перезапуск `rsyslog`



- Переход в `/vagrant/provision/client`
- Создание каталога `netlog/etc/rsyslog.d`
- Копирование `netlog-client.conf`

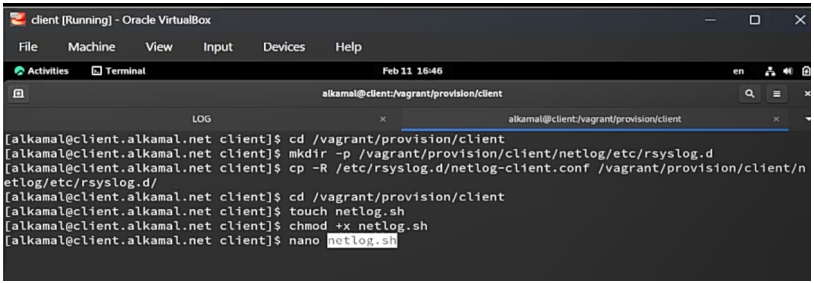
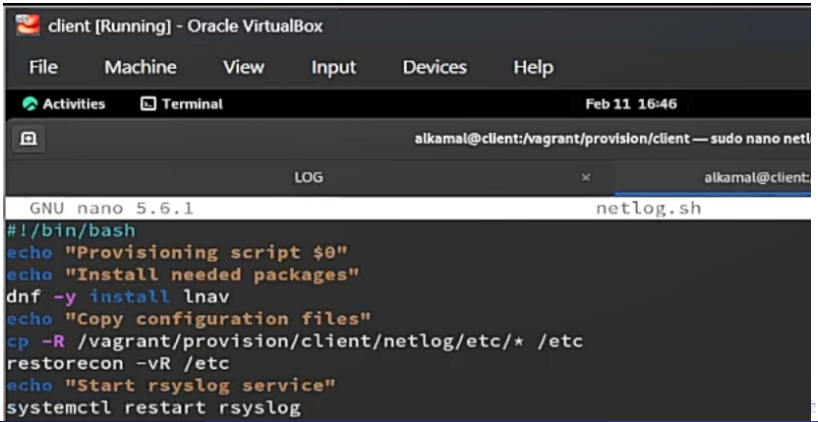


Рисунок 15: Создание каталога netlog и копирование конфигурации клиента

- Создан исполняемый файл `netlog.sh`
- Добавлен сценарий автоматической настройки клиента
- Установка `lnav`
- Копирование файлов в `/etc`
- Восстановление контекстов SELinux
- Перезапуск `rsyslog`



- В `Vagrantfile` добавлен блок provisioning для сервера
- Указан скрипт `provision/server/netlog.sh`
- Сохранена последовательность выполнения

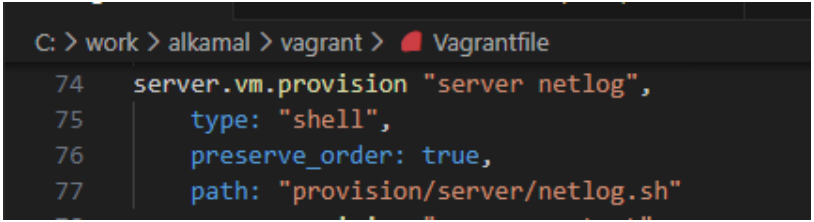


Рисунок 17: Добавление provisioning для сервера в Vagrantfile

- Добавлен аналогичный блок для клиента
- Указан скрипт `provision/client/netlog.sh`
- Обеспечена автоматическая настройка при запуске ВМ

C: > work > alkamal > vagrant > Vagrantfile

```
135   client.vm.provision "client netlog",
136       type: "shell",
137       preserve_order: true,
138       path: "provision/client/netlog.sh"
```

Рисунок 18: Добавление provisioning для клиента в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Настроено централизованное журналирование на базе `rsyslog`
- Организован приём журналов по TCP 514 на сервере
- Реализовано перенаправление сообщений с клиента
- Подтверждена корректность работы через `/var/log/messages` и `lnav`
- Реализована автоматизация через provisioning-скрипты
- Обеспечена воспроизводимость конфигурации
- Создана функционирующая система централизованного сбора журналов