**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

*дисциплина: Администрирование сетевых подсистем*

Студент: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

**МОСКВА**

2024 г.

# Цель работы:

# Целью данной работы является приобретение практических навыков по установке и базовому конфигурированию HTTP-сервера Apache.

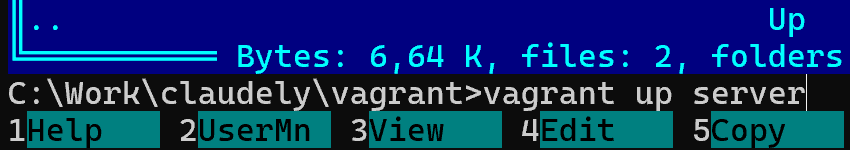
**Выполнение работы:**

Загрузим нашу операционную систему и перейдём в рабочий каталог с проектом:

cd /var/tmp/claudely/vagrant

Далее запустим виртуальную машину server (Рис. 1.1):

Vagrant up server

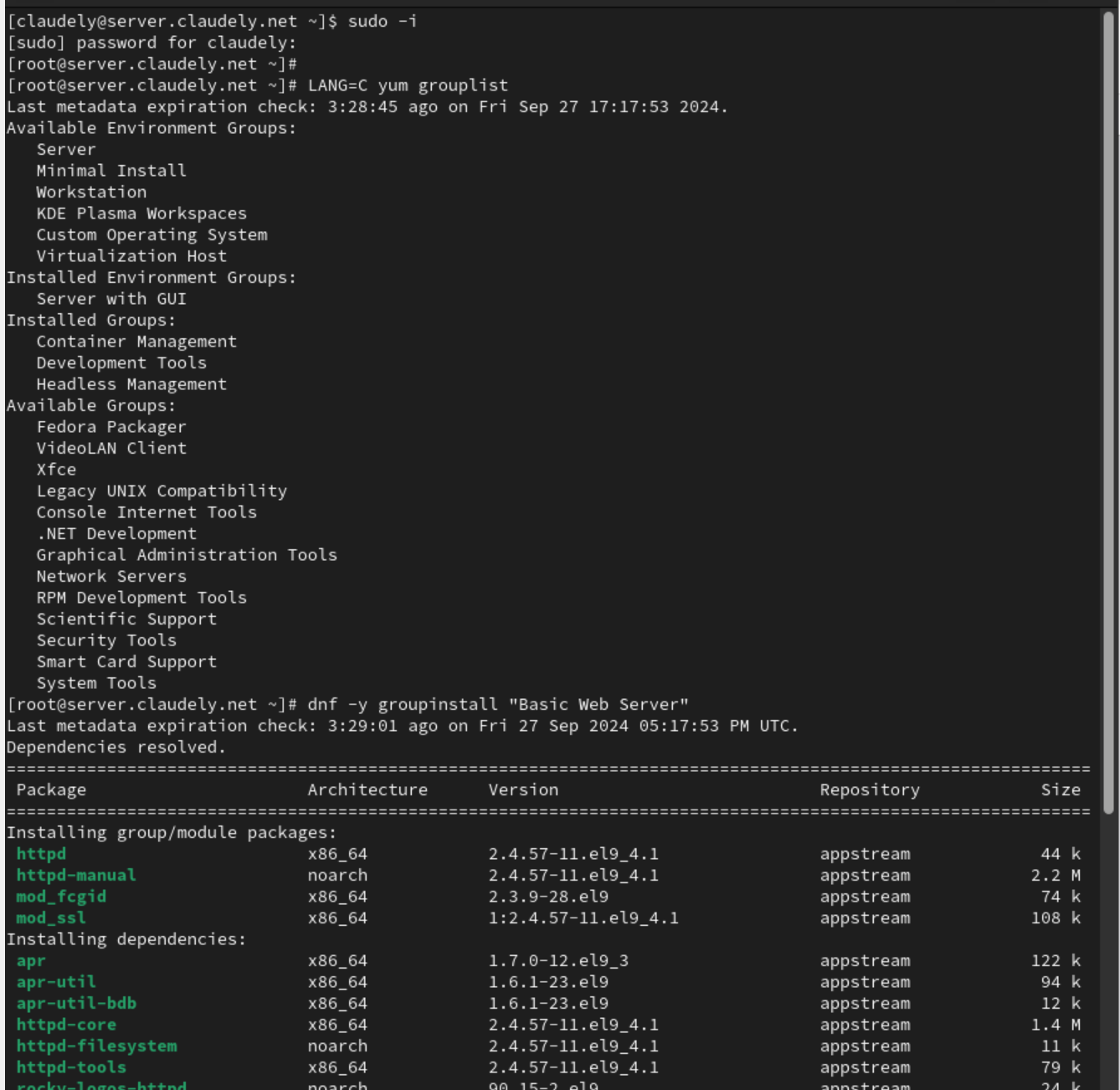
****

**Рис. 1.1.** Открытие рабочего каталога с проектом и запуск виртуальной машины server.

На виртуальной машине server войдём под нашим пользователем и откроем терминал. Далее перейдём в режим суперпользователя и установим из репозитория стандартный веб-сервер (HTTP-сервер и утилиты httpd, криптоутилиты и пр.) (Рис. 1.2):

LANG=C yum grouplist

dnf -y groupinstall "Basic Web Server"

****

**Рис. 1.2.** Переход в режим суперпользователя и установка из репозитория стандартного веб-сервера.

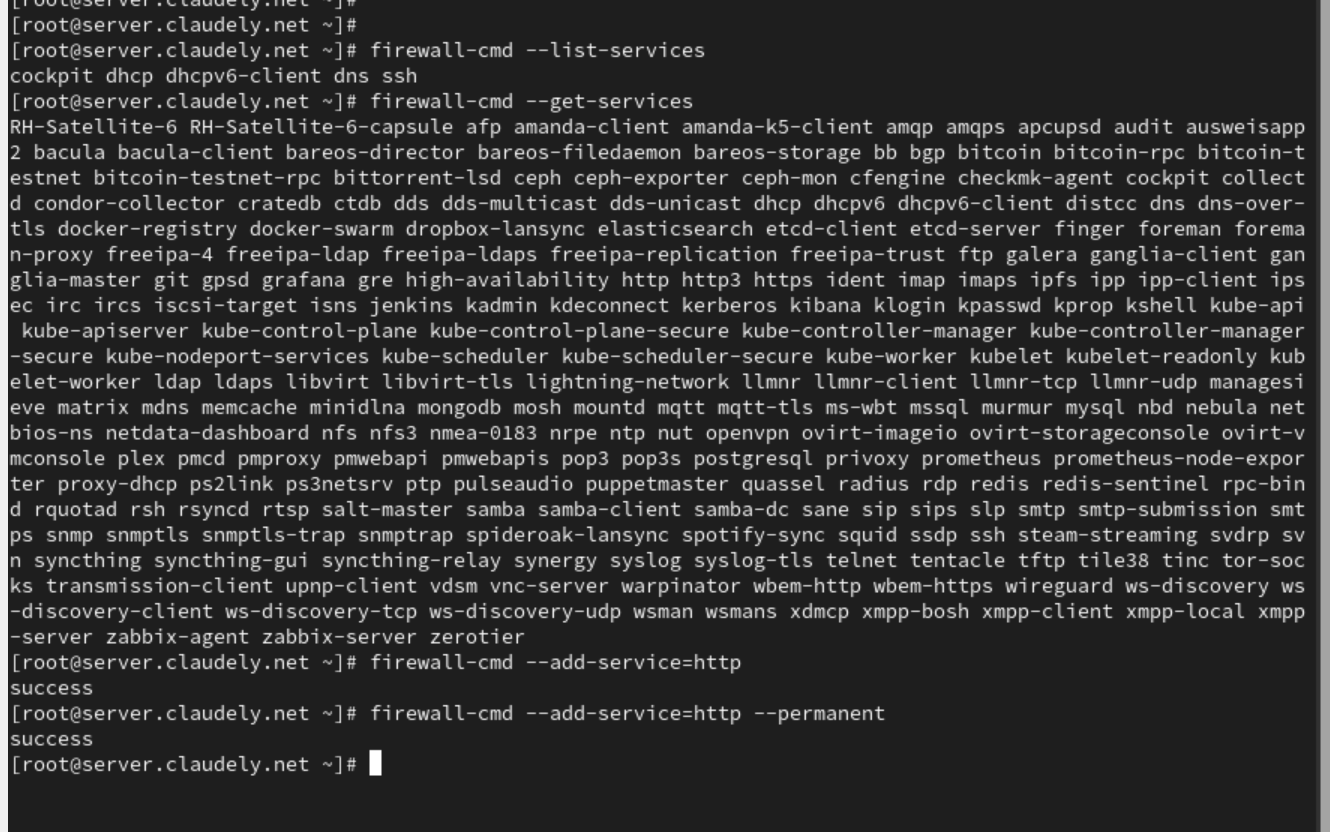
Внесём изменения в настройки межсетевого экрана узла server, разрешив работу с http:

firewall-cmd --list-services

firewall-cmd --get-services

firewall-cmd --add-service=http

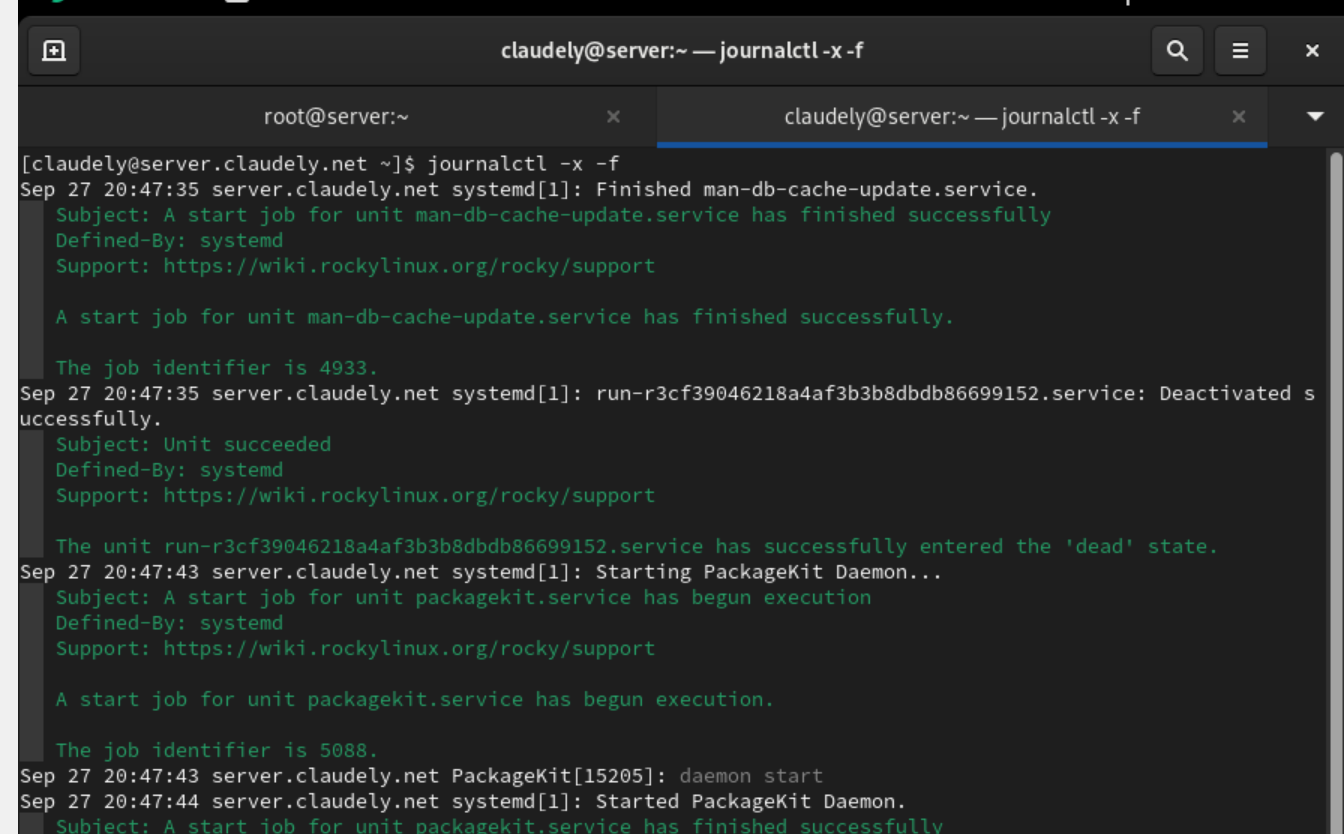
firewall-cmd --add-service=http --permanent (Рис. 2.2).

****

**Рис. 2.2.** Внесение изменений в настройки межсетевого экрана узла server, разрешив работу с http.

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы (Рис. 2.3):

journalctl -x -f

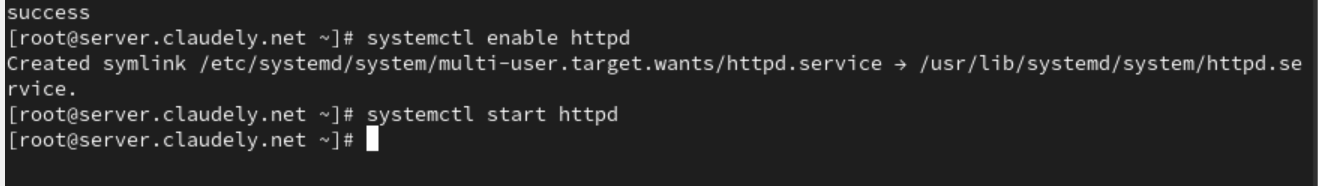
****

**Рис. 2.3.** Запуск в дополнительном терминале в режиме реального времени расширенного лога системных сообщений для проверки корректности работы системы.

В первом терминале активируем и запустим HTTP-сервер (Рис. 2.4):

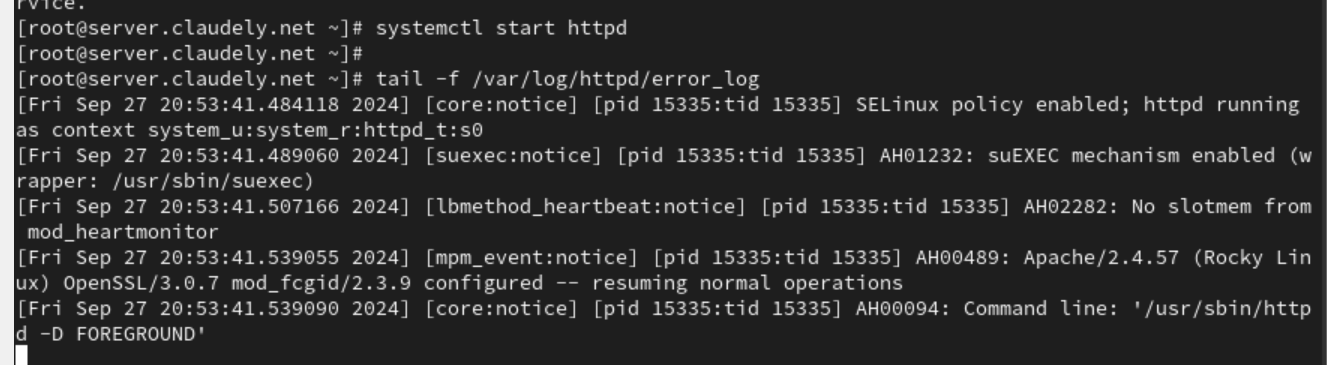
systemctl enable httpd

systemctl start httpd

****

**Рис. 2.4.** Активация и запуск HTTP-сервера.

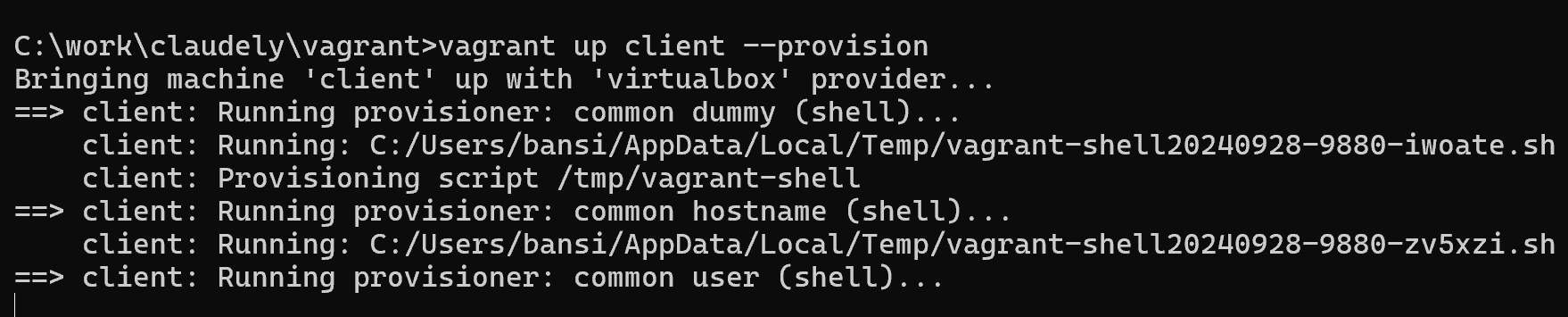
Просмотрим расширенный лог системных сообщений, убедимся, что веб-сервер успешно запустился (Рис. 2.5):

****

**Рис. 2.5.** Просмотр расширенного лога системных сообщений.

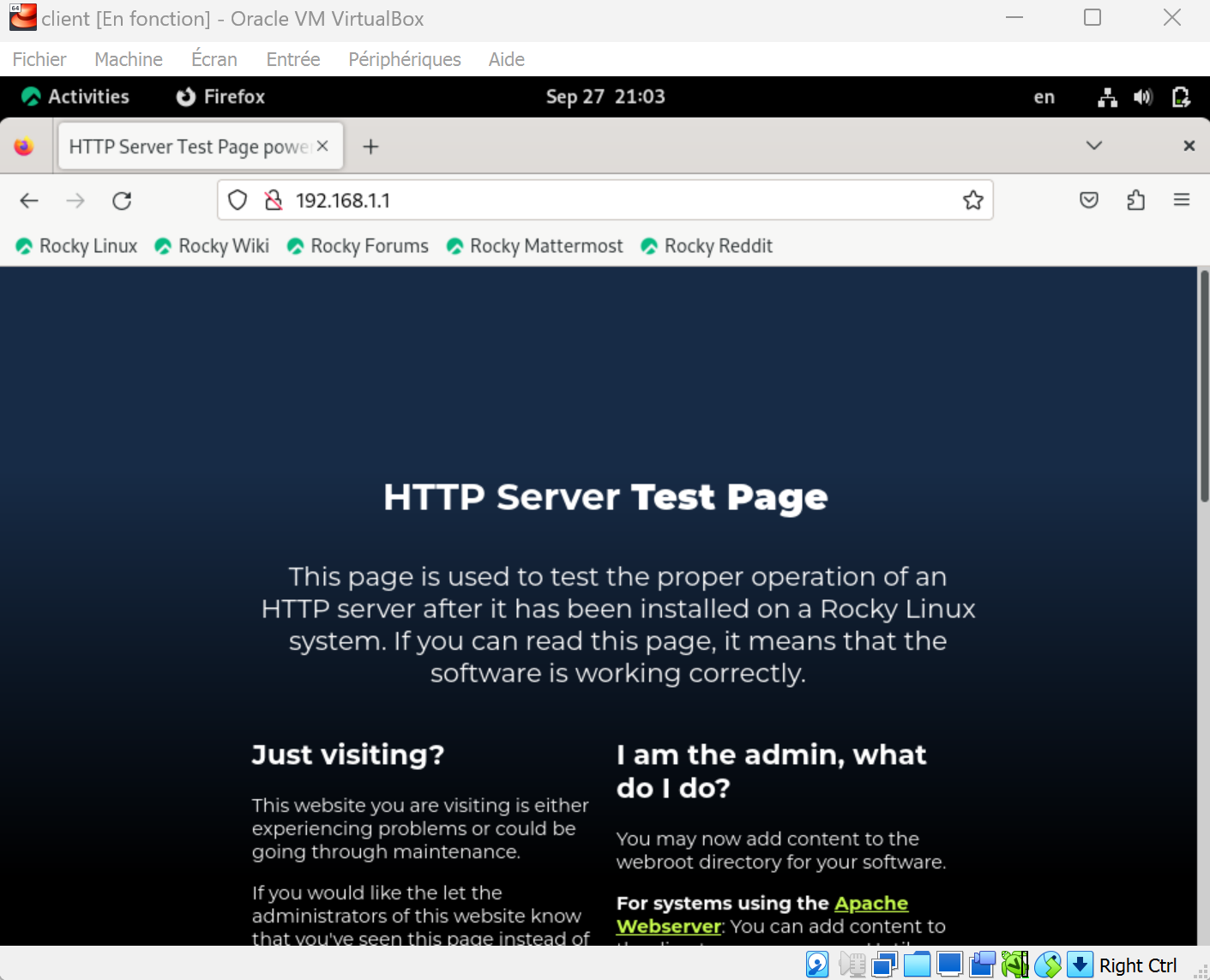
Запустим виртуальную машину client (Рис. 3.1):

make client-up

****

**Рис. 3.1.** Запуск виртуальной машины client.

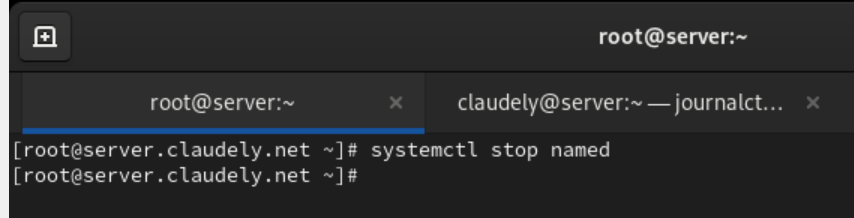
На виртуальной машине client запустим браузер и в адресной строке введём 192.168.1.1 (Рис. 3.3):

****

**Рис. 3.3.** Запуск браузера на виртуальной машине client и ввод в адресной строке 192.168.1.1.

Остановим работу DNS-сервера для внесения изменений в файлы описания DNS-зон (рис. 4.1):

systemctl stop named

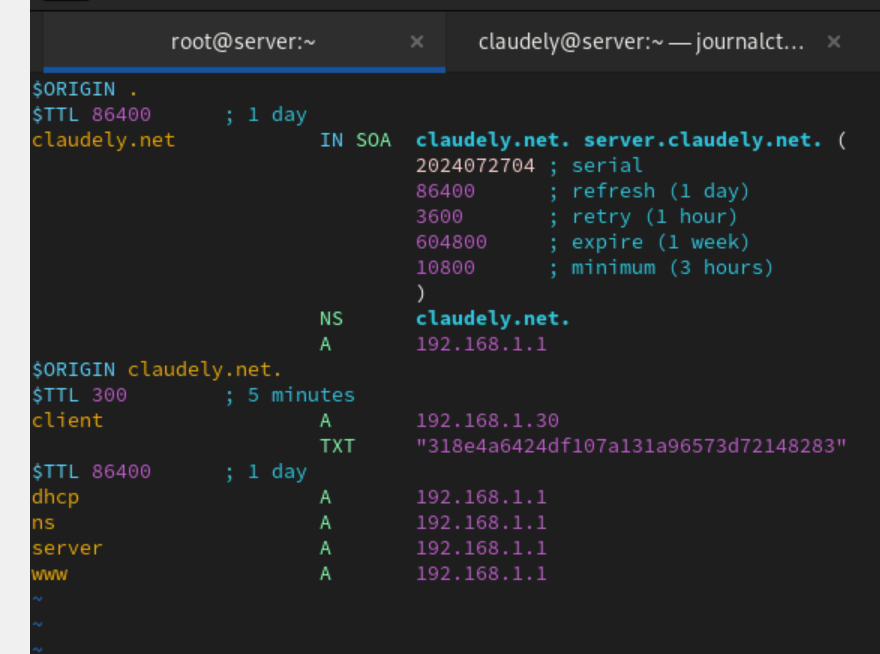
****

**Рис. 4.1.** Остановка работы DNS-сервера для внесения изменений в файлы описания DNS-зон.

Теперь добавим запись для HTTP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/claudely.net (рис. 4.2):

Server A 192.168.1.1

www A 192.168.1.1

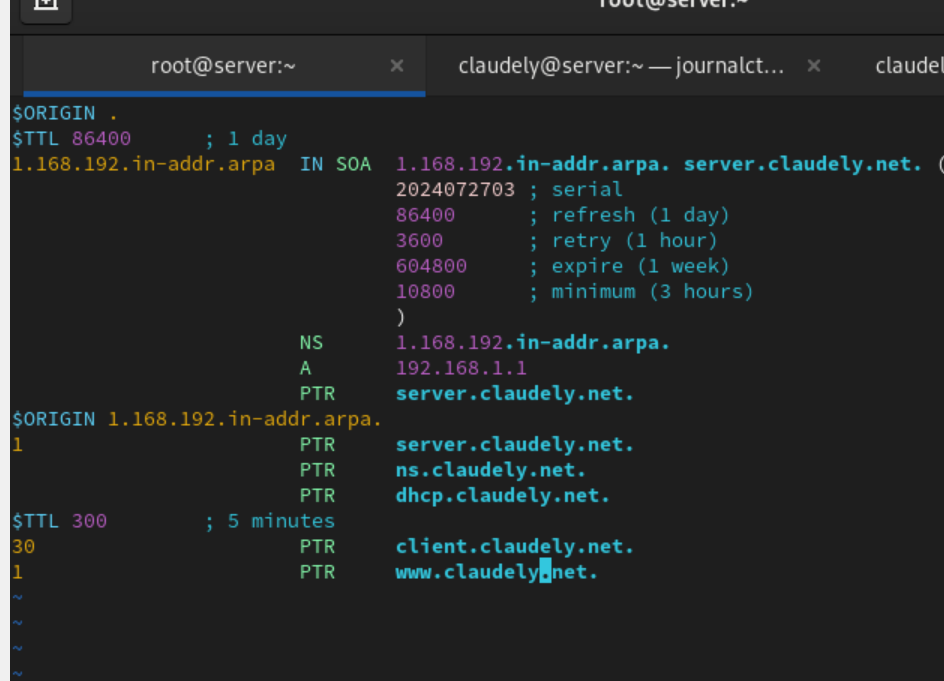
****

**Рис. 4.2.** Добавление записи для HTTP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/claudely.net.

Также в конце файла обратной зоны /var/named/master/rz/192.168.1 (рис. 4.3):

1 PTR server.claudely.net.

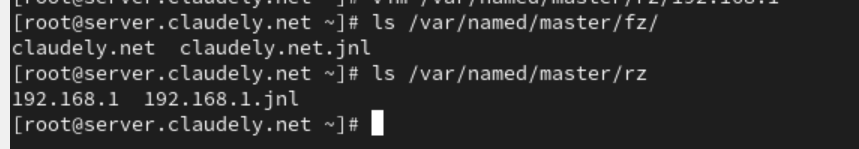
1 PTR www.claudely.net.

****

**Рис. 4.3.** Добавление записи для HTTP-сервера в конце файла обратной DNS-зоны /var/named/master/rz/192.168.1.

Нам требуется из соответствующих каталогов удалить файлы журналов DNS (рис. 4.4):

claudely.net.jnl и 192.168.1.jnl. (рис. 4.4):

****

**Рис. 4.4.** Удаление файлов журналов DNS.

Перезапустим DNS-сервер:

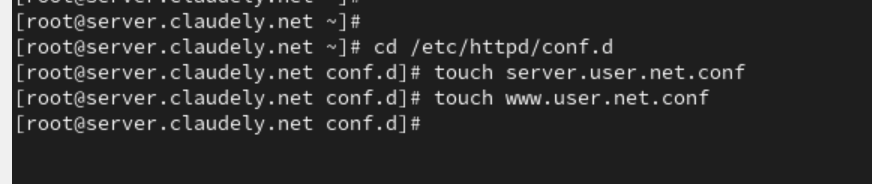
systemctl start named

В каталоге /etc/httpd/conf.d создадим файлы server.claudely.net.conf и www.claudely.net.conf (рис. 4.5):

cd /etc/httpd/conf.d

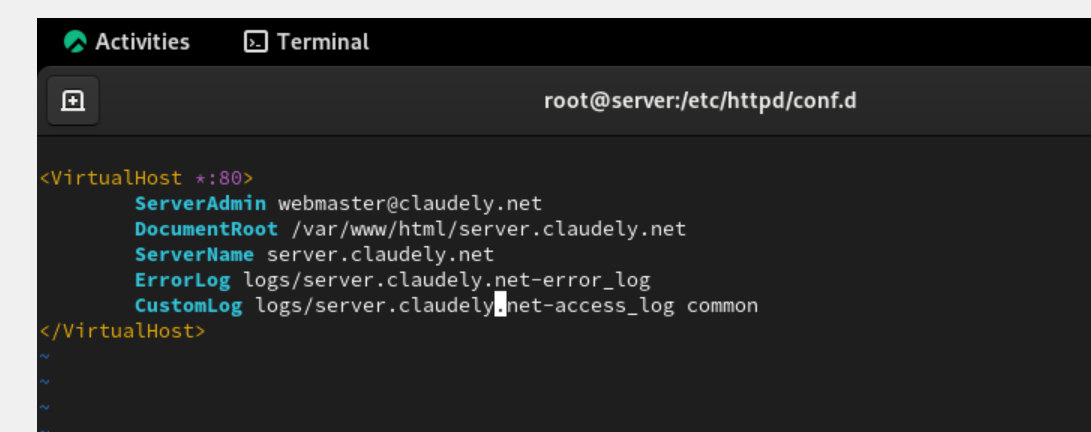
touch server.user.net.conf

touch www.user.net.conf

****

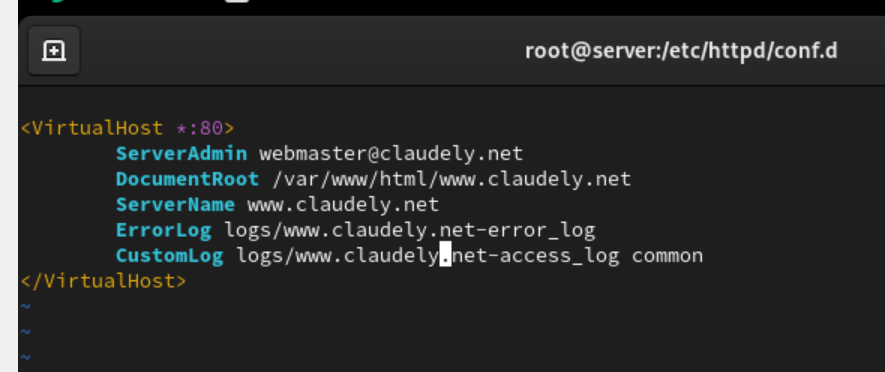
**Рис. 4.5.** Перезапуск DNS-сервера и создание в каталоге /etc/httpd/conf.d файлов server.claudely.net.conf и www.claudely.net.conf.

Откроем на редактирование файл server.claudely.net.conf и внесём туда следующее содержание (рис. 4.6):

****

**Рис. 4.6.** Открытие на редактирование файла server.claudely.net.conf и добавление содержания из лабораторной работы.

Откроем на редактирование файл www.claudely.net.conf и внесём туда следующее содержание (рис. 4.7):

****

**Рис. 4.7.** Открытие на редактирование файла www.claudely.net.conf и добавление содержания из лабораторной работы.

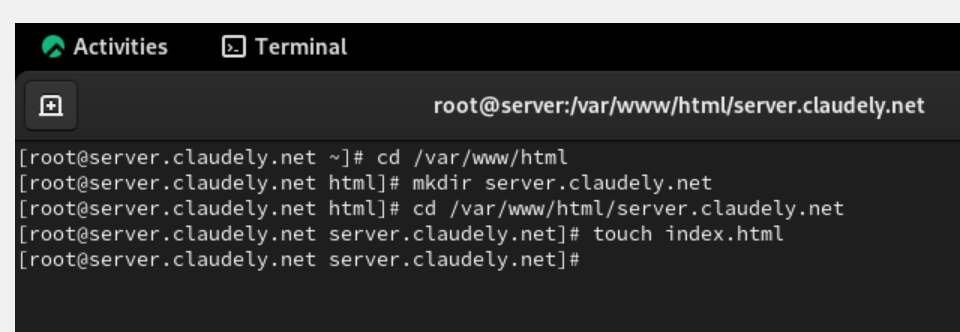
Перейдём в каталог /var/www/html, в котором находятся файлы с содержимым (контентом) веб-серверов, и создадим тестовые страницы для виртуальных веб-серверов server.claudely.net и www.claudely.net. Для виртуального веб-сервера server.claudely.net:

cd /var/www/html

mkdir server.claudely.net

cd /var/www/html/server.claudely.net

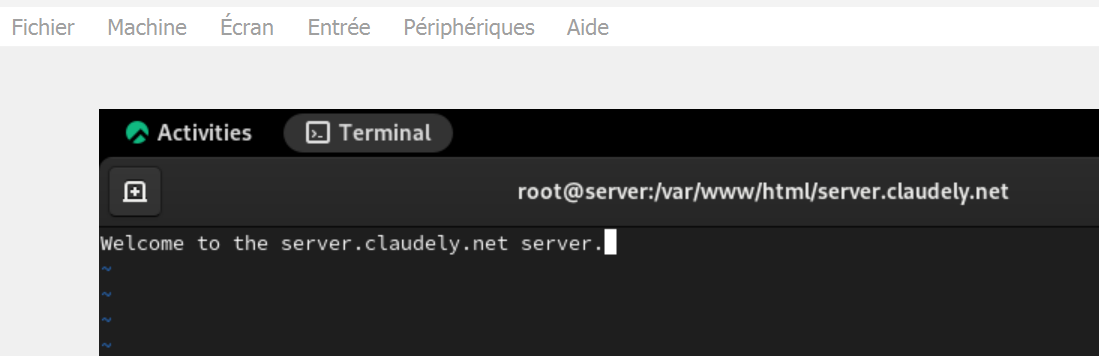
touch index.html (рис. 4.8):

****

**Рис. 4.8.** Открытие каталога /var/www/html и создание тестовой страницы для виртуального веб-сервера server.claudely.net.

Откроем на редактирование файл index.html и внесём следующее содержание (рис. 4.9):

Welcome to the server.claudely.net server.

****

**Рис. 4.9.** Открытие на редактирование файла index.html и внесение содержания.

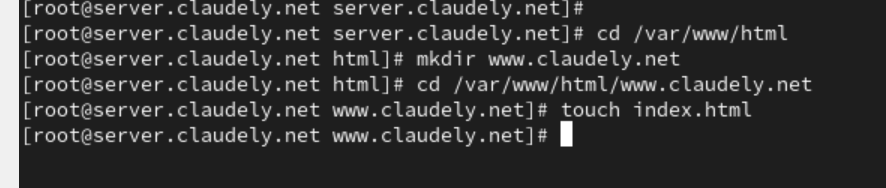
Для виртуального веб-сервера www.claudely.net (рис. 4.10):

cd /var/www/html

mkdir www.claudely.net

cd /var/www/html/www.claudely.net

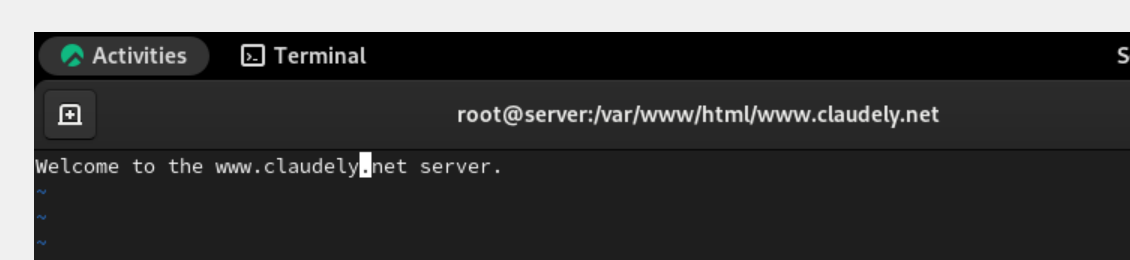
touch index.html

****

**Рис. 4.10.** Открытие каталога /var/www/html и создание тестовой страницы для виртуального веб-сервера www.claudely.net.

Откроем на редактирование файл index.html и внесём следующее содержание (рис. 4.11):

Welcome to the www.claudely.net server.

****

**Рис. 4.11.** Открытие на редактирование файла index.html и внесение содержания.

Скорректируем права доступа в каталог с веб-контентом:

chown -R apache:apache /var/www

Далее восстановим контекст безопасности в SELinux:

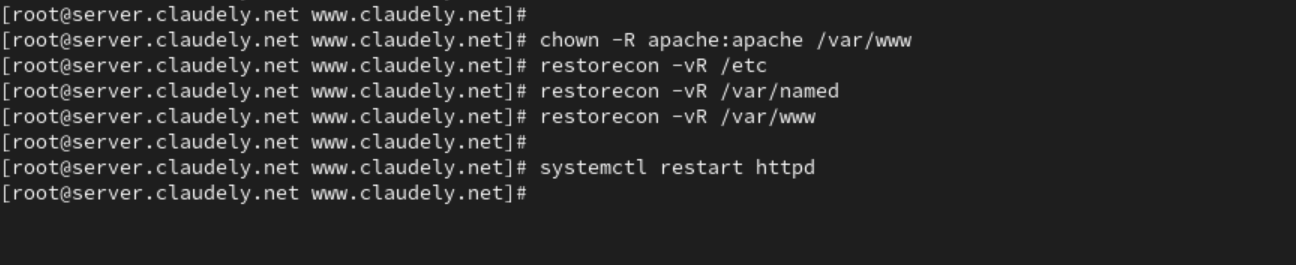
restorecon -vR /etc/named

restorecon -vR /var/named

restorecon -vR /var/www

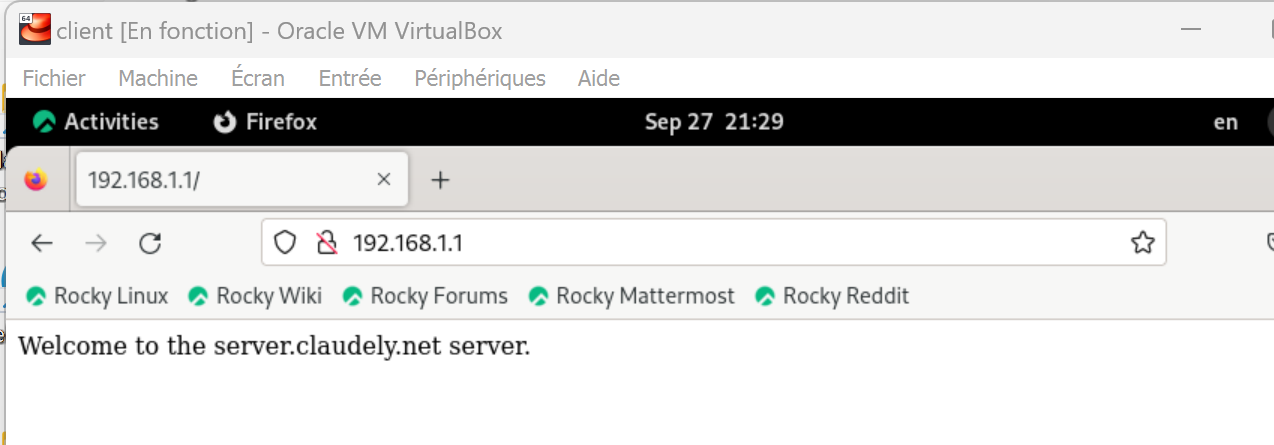
Теперь перезапустим HTTP-сервер (рис. 4.12):

systemctl restart httpd

****

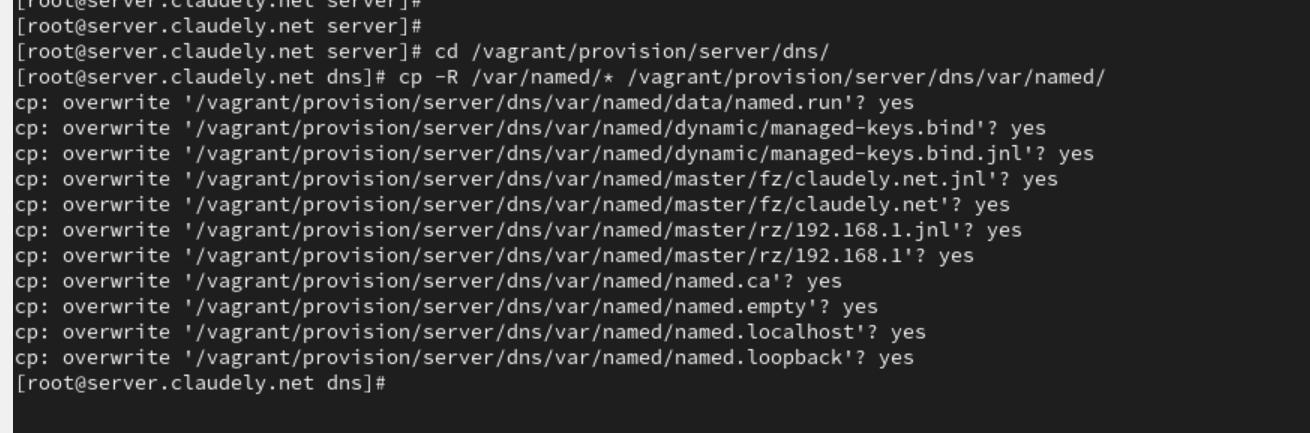
**Рис. 4.12.** Исправление прав доступа в каталог с веб-контентом, восстановление контекста безопасности в SELinux и перезапуск HTTP-сервера.

На виртуальной машине client убедимся в корректном доступе к веб-серверу по адресам server.claudely.net (рис. 4.13) и www.claudely.net (рис. 4.14) в адресной строке веб-браузера.

****

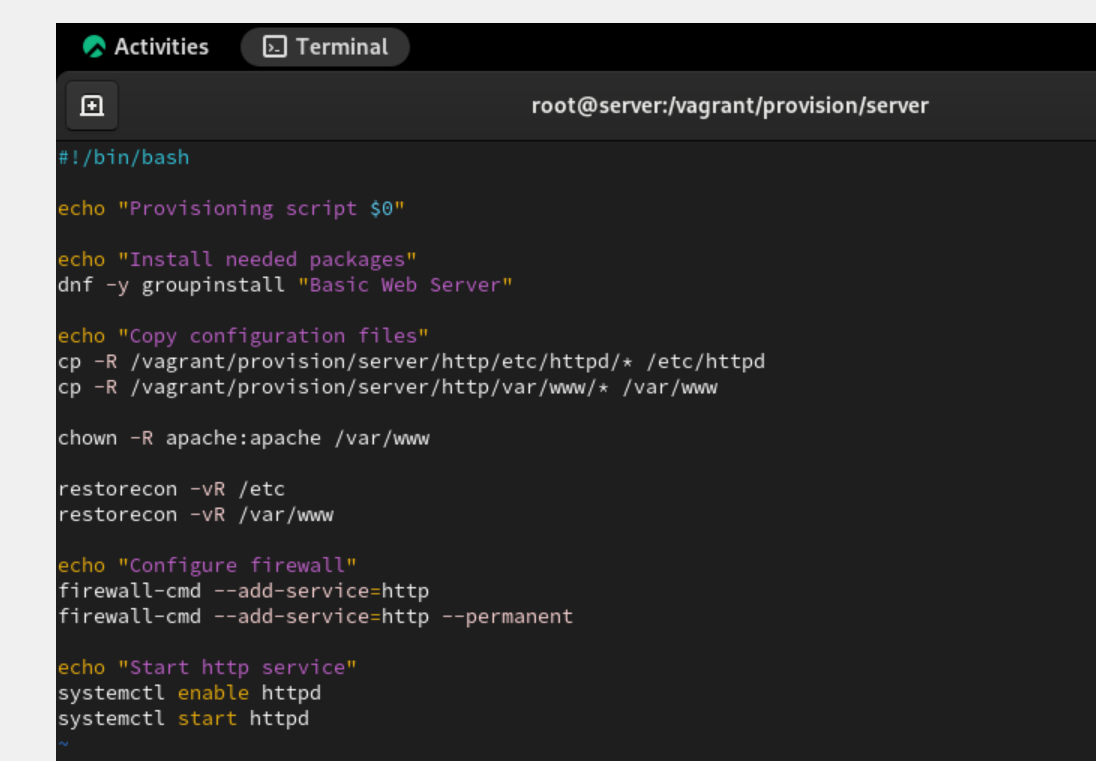
**Рис. 4.13.** Проверка корректного доступа на виртуальной машине client к веб-серверу по адресу server.claudely.net.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог http, в который поместим в соответствующие подкаталоги конфигурационные файлы HTTP-сервера. Теперь заменим конфигурационные файлы DNS-сервера. В каталоге /vagrant/provision/server создадим исполняемый файл http.sh (рис. 5.1):

****

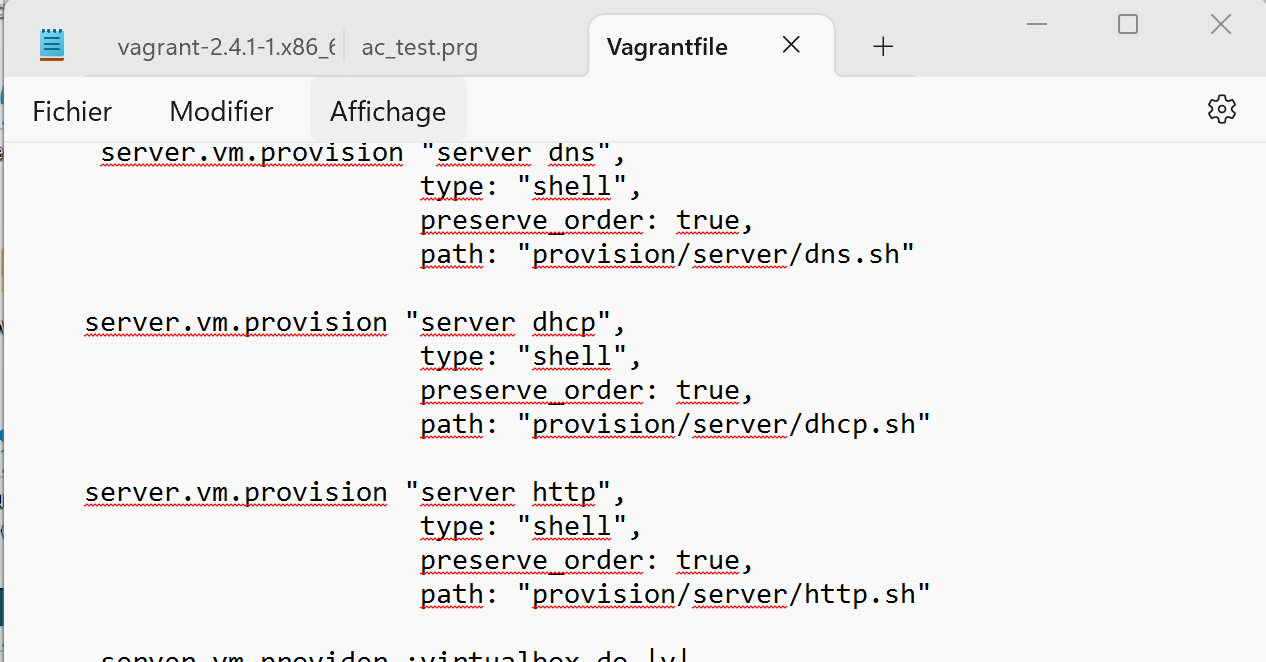
**Рис. 5.1.** Открытие на виртуальной машине server каталога для внесения изменений в настройки внутреннего окружения, создание в нём каталога http. Замена конфигурационных файлов DNS-сервера и создание исполняемого файла http.sh.

Откроем созданный файл на редактирование и пропишем в нём скрипт (рис. 5.2):

****

**Рис. 5.2.** Открытие созданного файла на редактирование и прописывание скрипта.

Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile добавим в конфигурации сервера следующую запись (рис. 5.3):

****

**Рис. 5.3.** Добавление записи для отработки созданного скрипта во время загрузки виртуальных машин.

**Вывод:**

# В ходе выполнения лабораторной работы были приобретены практические навыки по установке и базовому конфигурированию HTTP-сервера Apache.

**Ответы на контрольные вопросы:**

1. Через какой порт по умолчанию работает Apache? - **По умолчанию, Apache работает через порт 80 для HTTP и порт 443 для HTTPS.**
2. Под каким пользователем запускается Apache и к какой группе относится этот пользователь? - **Apache обычно запускается от имени пользователя www-data (или apache, в зависимости от дистрибутива) и относится к группе с тем же именем.**
3. Где располагаются лог-файлы веб-сервера? Что можно по ним отслеживать? - **Лог-файлы веб-сервера обычно располагаются в директории логов. Например, в Ubuntu логи Apache хранятся в /var/log/apache2/, а в CentOS - в /etc/httpd/logs/. Лог-файлы содержат информацию о запросах к серверу, ошибки, статусы запросов и другие события, что позволяет администраторам отслеживать активность и выявлять проблемы.**
4. Где по умолчанию содержится контент веб-серверов? - **Контент веб-серверов по умолчанию обычно находится в директории, называемой "DocumentRoot". Например, в Apache на Linux DocumentRoot по умолчанию установлен в /var/www/html/. В этой директории содержатся файлы, которые веб-сервер отдает при запросах.**
5. Каким образом реализуется виртуальный хостинг? Что он даёт? - **Виртуальный хостинг в Apache позволяет хостить несколько сайтов на одном сервере. Это можно сделать двумя способами:**

**Базовый виртуальный хостинг: Разные сайты обслуживаются на одном сервере с использованием разных директорий DocumentRoot.**

**Name-based (или Host-based) виртуальный хостинг: Разные сайты обслуживаются на одном IP-адресе, но на разных доменных именах. Это основывается на значении заголовка "Host" в HTTP-запросе, который используется для определения, какой виртуальный хост должен обработать запрос.**

**Виртуальный хостинг позволяет хозяину сервера размещать несколько сайтов на одном физическом сервере, управлять ими независимо, и предоставлять услуги хостинга для различных клиентов или проектов.**