Лабораторная работа №11

Настройка безопасного удалённого доступа по протоколу SSH

Студент: Пакавира Арсениу Висенте Луиш

Группа: НФИбд 02–23

дисциплина: **Администрирование сетевых подсистем (Lab 11)**

Цель работы

Целью данной работы является приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

Запрет удалённого доступа по SSH для пользователя root

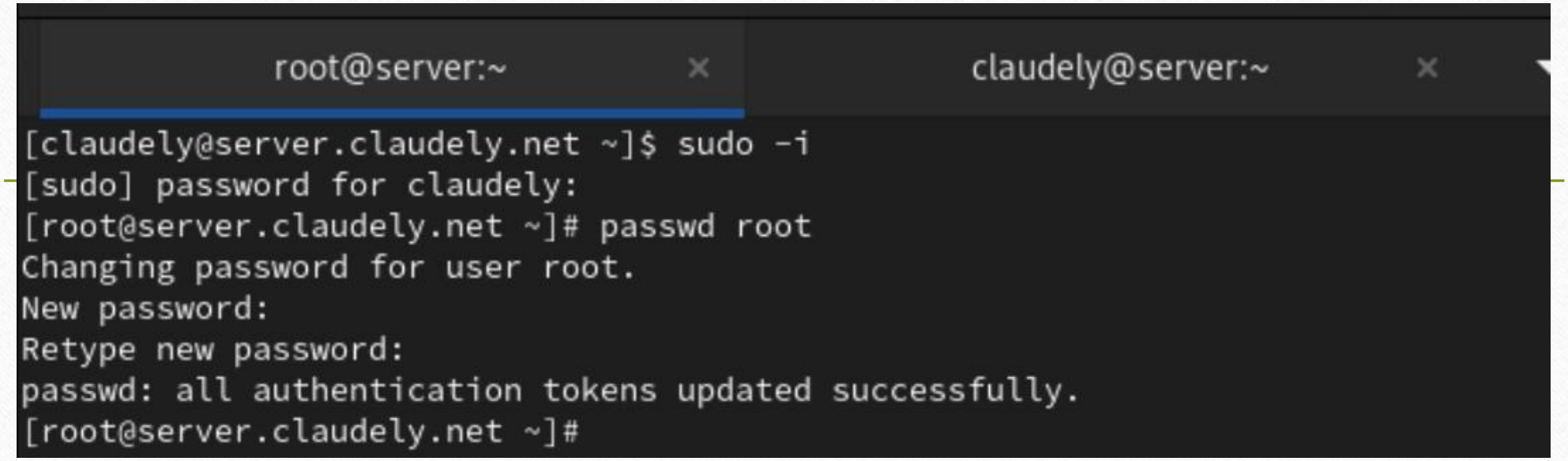


Рис. 1.1. Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

Запрет удалённого доступа по SSH для пользователя root

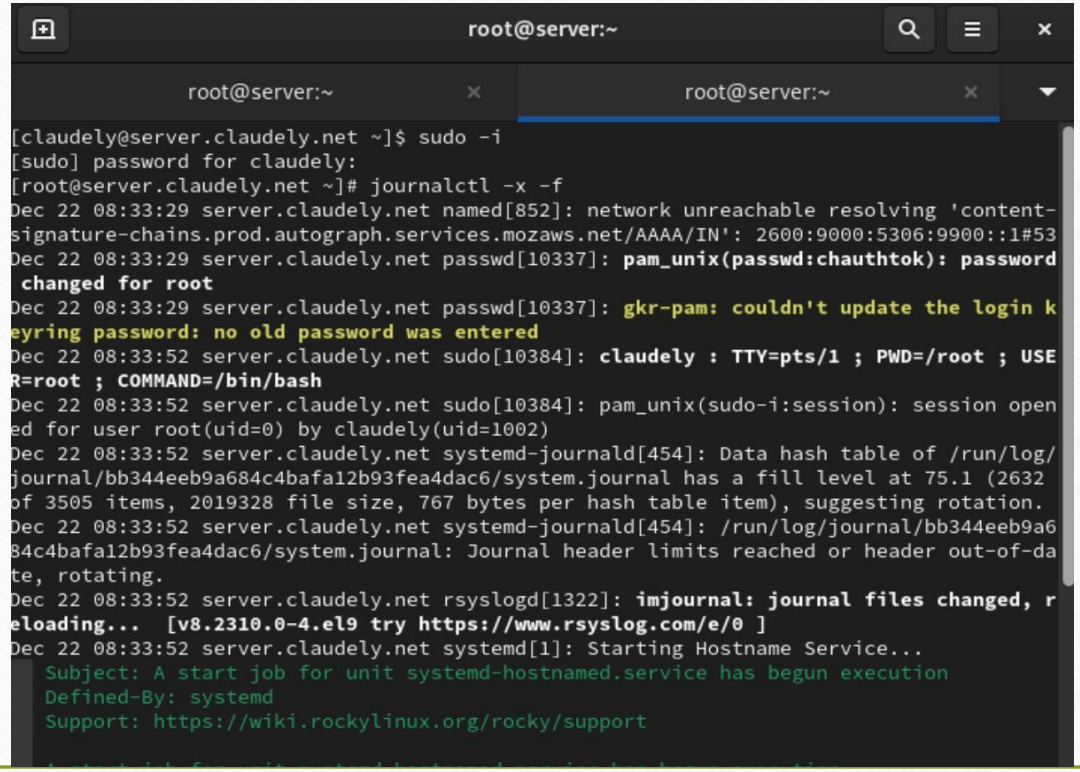
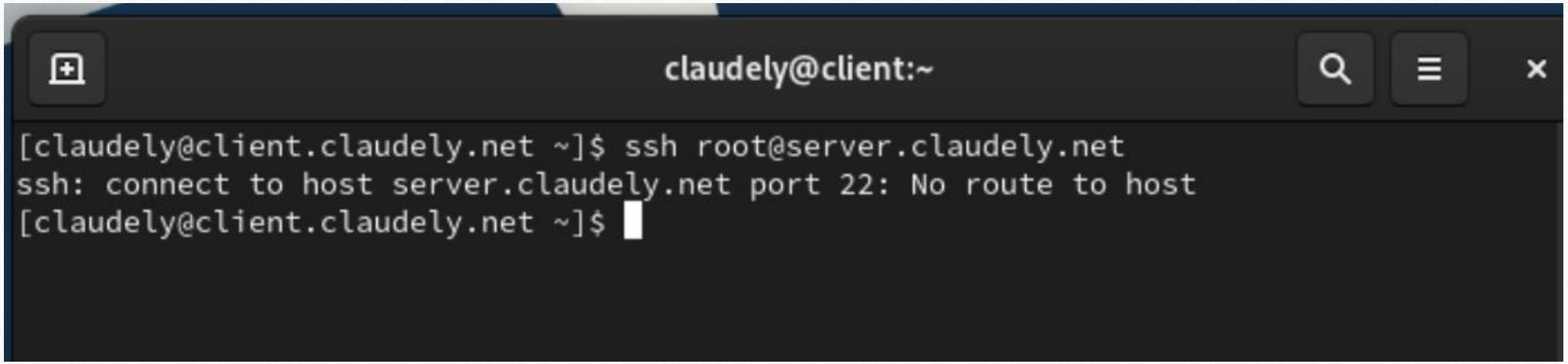


Рис. 1.2. Запуск в дополнительном терминале мониторинга системных событий.

Запрет удалённого доступа по SSH для пользователя root



Запрет удалённого доступа по SSH для

Рис. 1.3. Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.

Запрет удалённого доступа по SSH для пользователя root

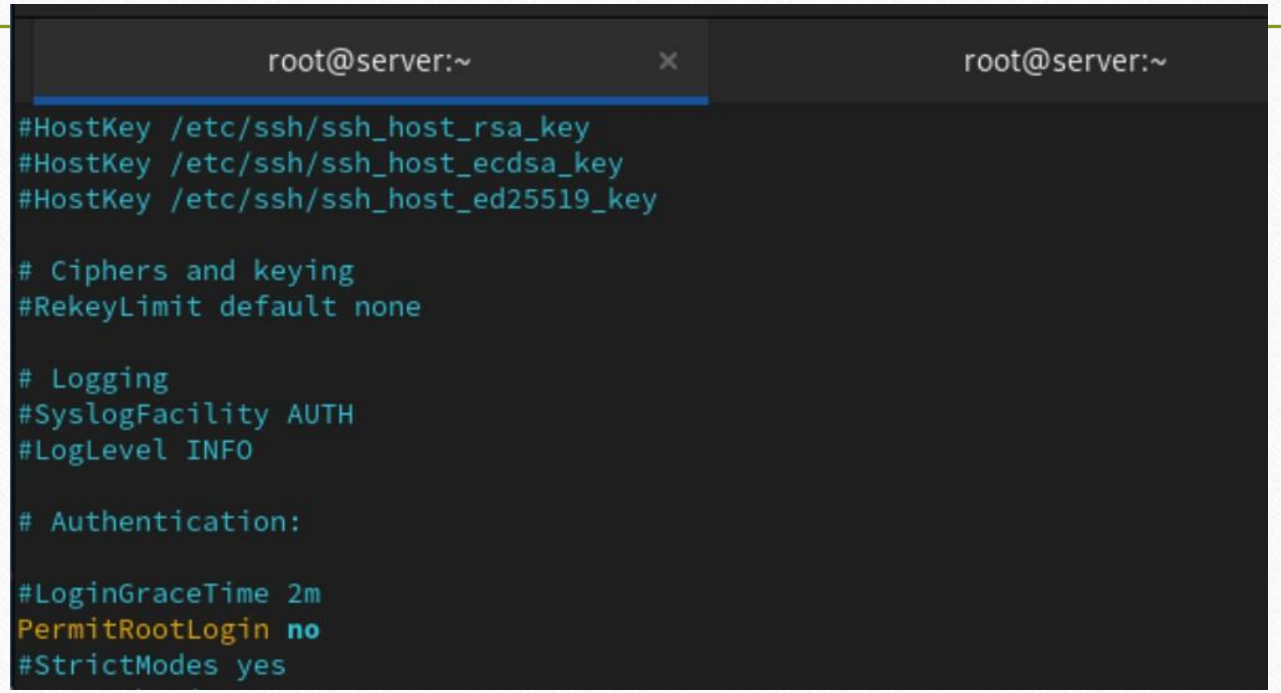


Рис. 1.4. Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd для редактирования и запрет входа на сервер пользователю root.

Запрет удалённого доступа по SSH для пользователя root

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 1.5. Перезапуск sshd.

Ограничение списка пользователей для удалённого доступа по SSH

Ограничение списка пользователей для

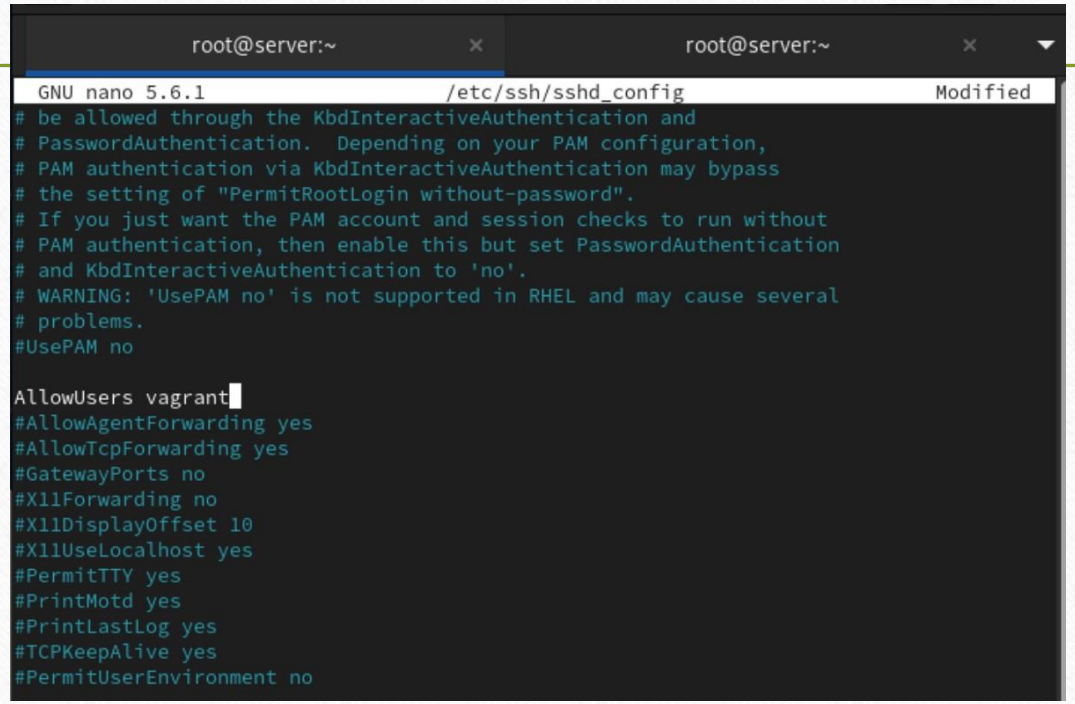


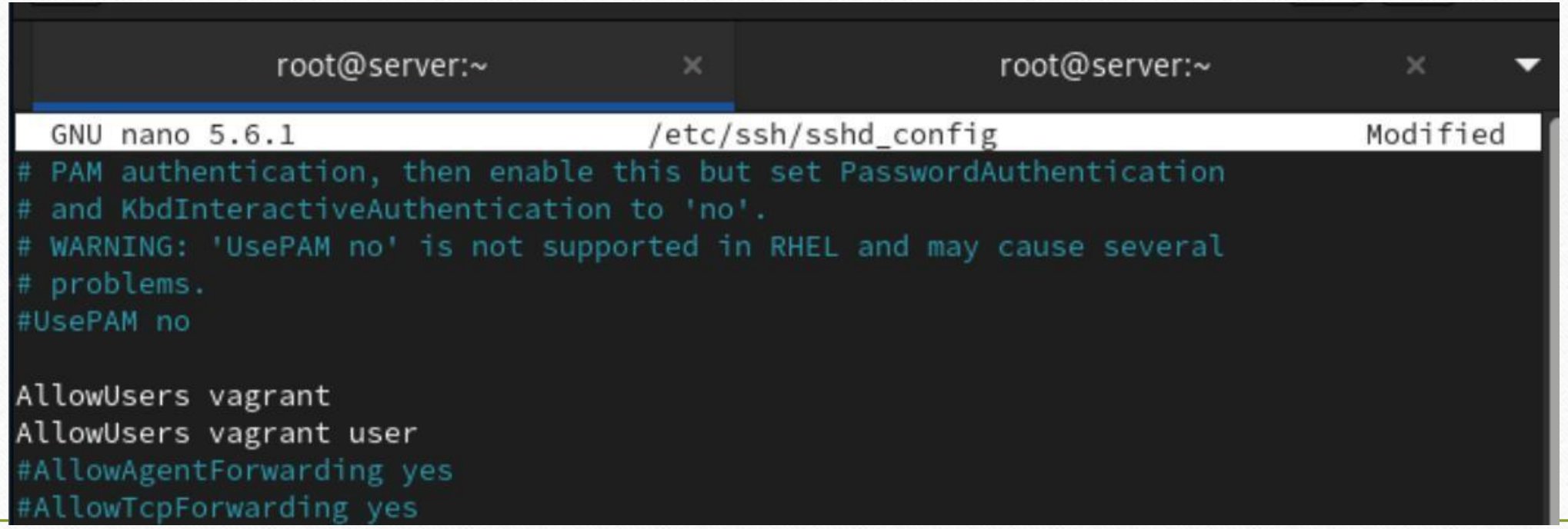
Рис. 2.2. Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd на редактирование и добавление нужной строки.

Ограничение списка пользователей для удалённого доступа по SSH

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 2.3. Перезапуск sshd.

Ограничение списка пользователей для удалённого доступа по SSH



Ограничение списка пользователей для

Рис. 2.5. Внесение изменения в файле /etc/ssh/sshd_config конфигурации sshd.

Настройка дополнительных портов для удалённого доступа по SSH

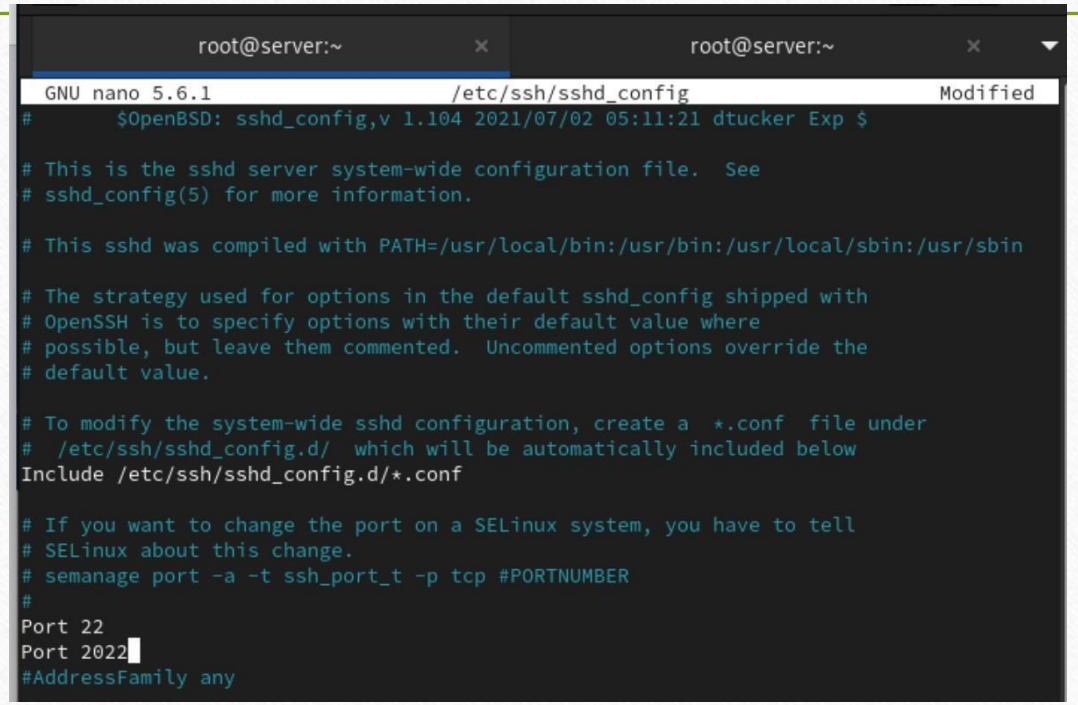


Рис. 3.1. Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.

Настройка дополнительных портов для удалённого доступа по SSH

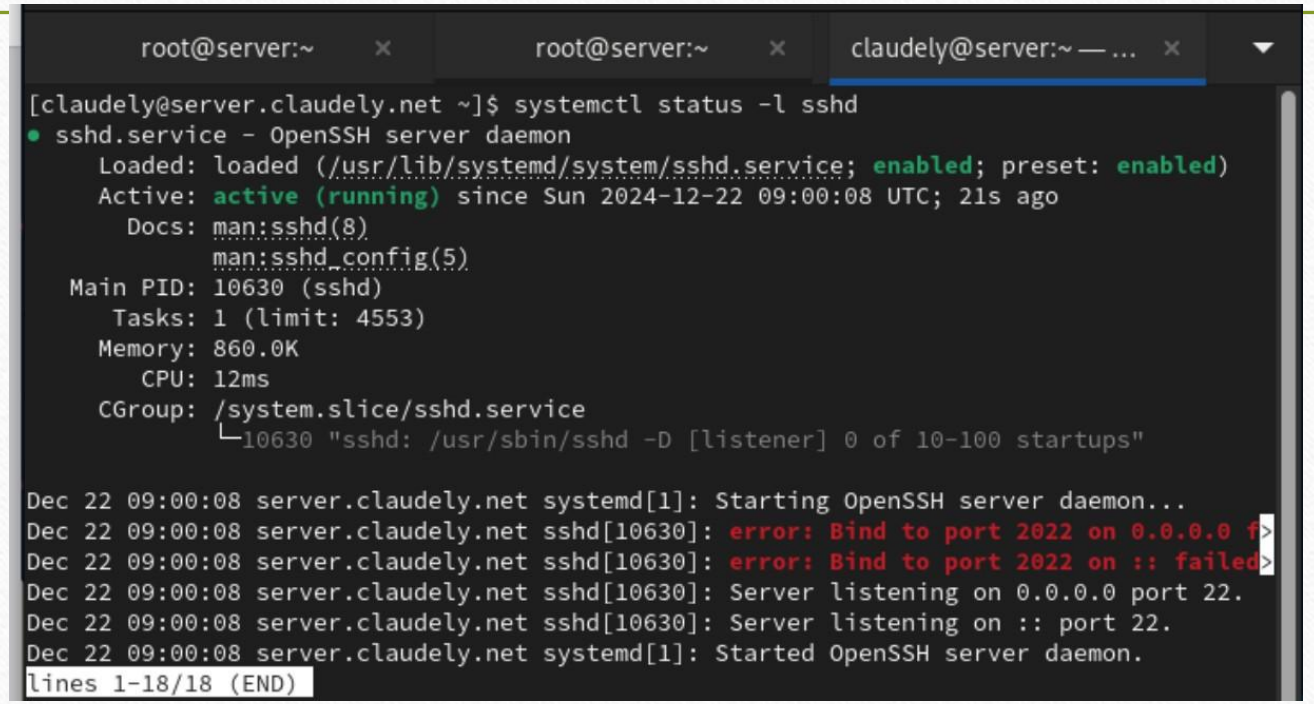


Рис. 3.2. Перезапуск sshd и просмотр расширенного статуса работы.

Настройка дополнительных портов для удалённого доступа по SSH

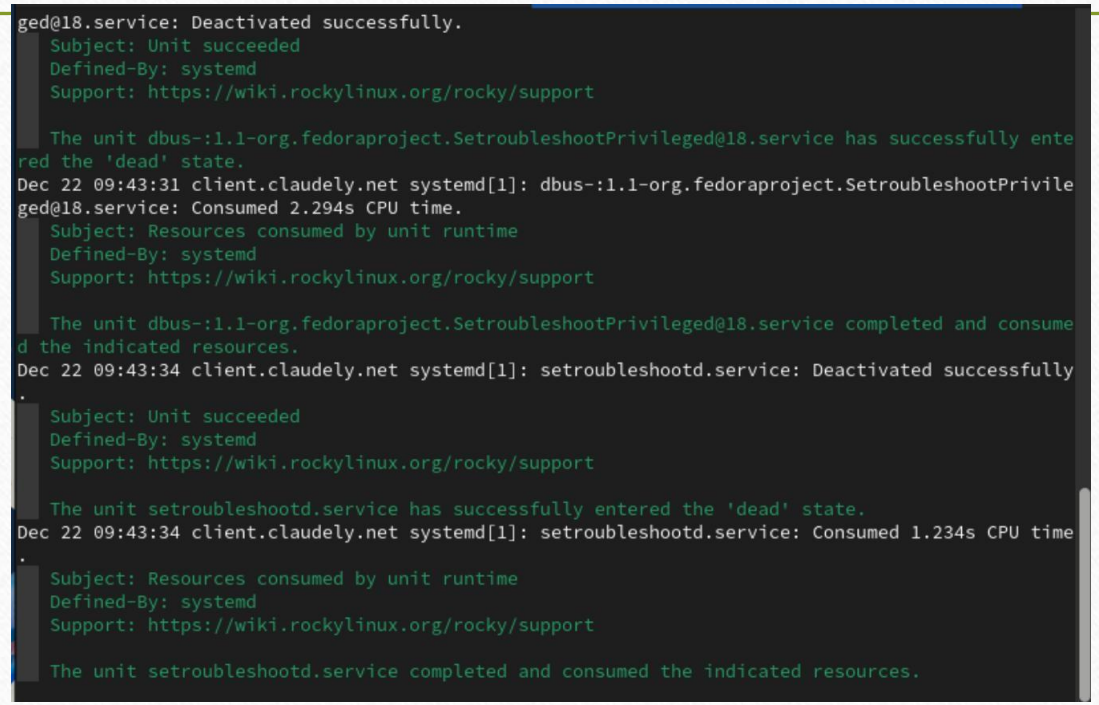


Рис. 3.3. Просмотр сообщения в терминале с мониторингом системных событий.

Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.claudely.net ~]#
```

```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.claudely.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.claudely.net ~]#
```

Рис. 3.4. Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

Настройка удалённого доступа по SSH по ключу

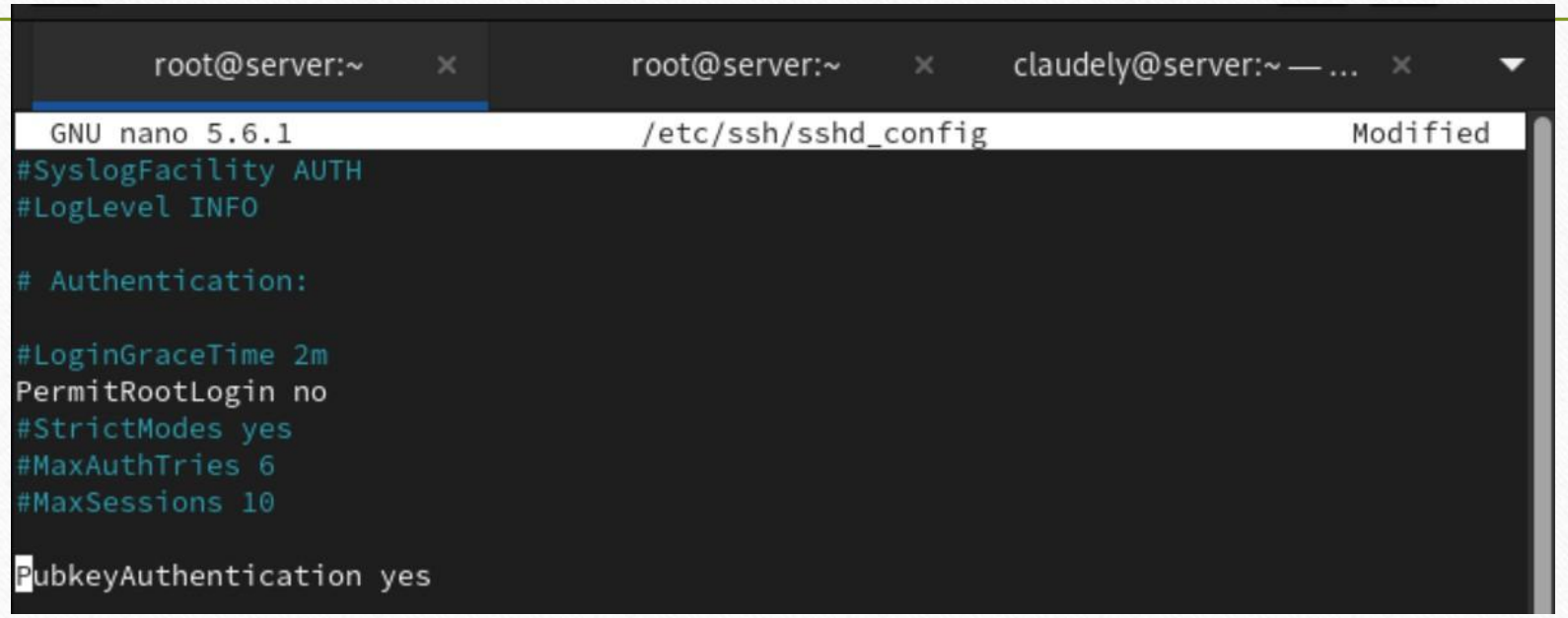


Рис. 4.1. Настройка параметра на сервере в конфигурационном файле /etc/ssh/sshd_config, разрешающего аутентификацию по ключу.

Настройка удалённого доступа по SSH по ключу

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 4.2. Перезапуск sshd.

Настройка удалённого доступа по SSH по ключу

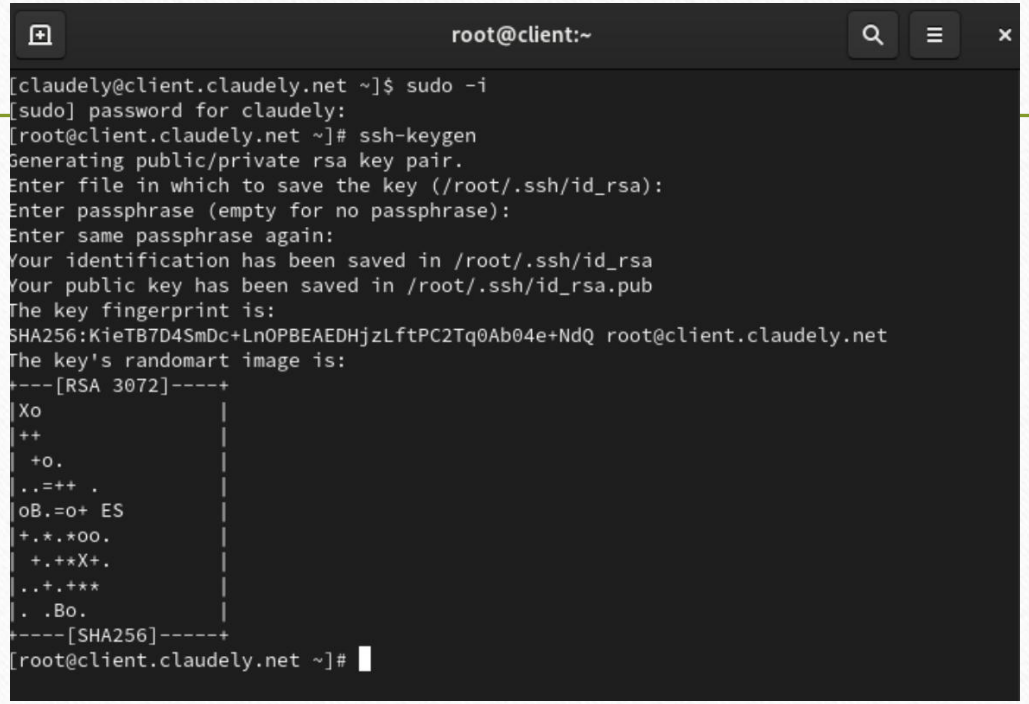


Рис. 4.3. Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.

Организация туннелей SSH, перенаправление TCP-портов

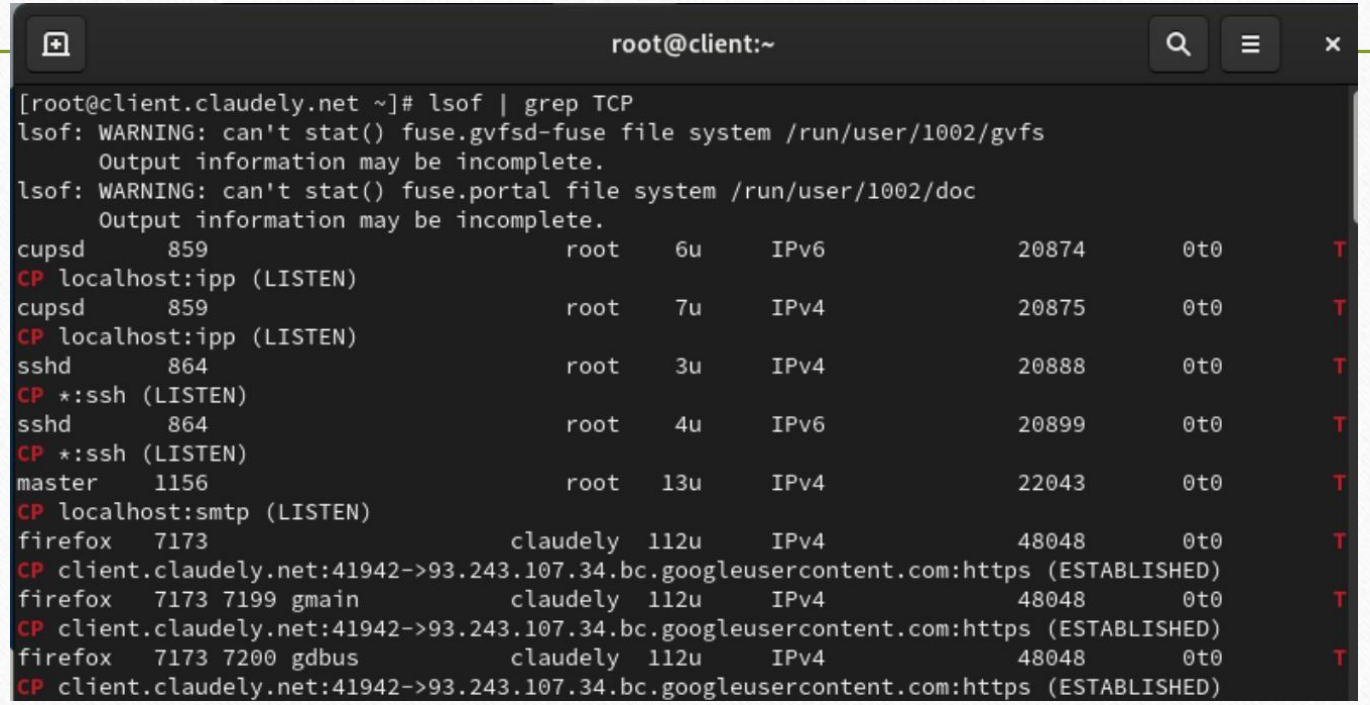


Рис. 5.1. Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.claudely.net на порт 8080 на локальной машине.

Запуск графических приложений через SSH (X11Forwarding)

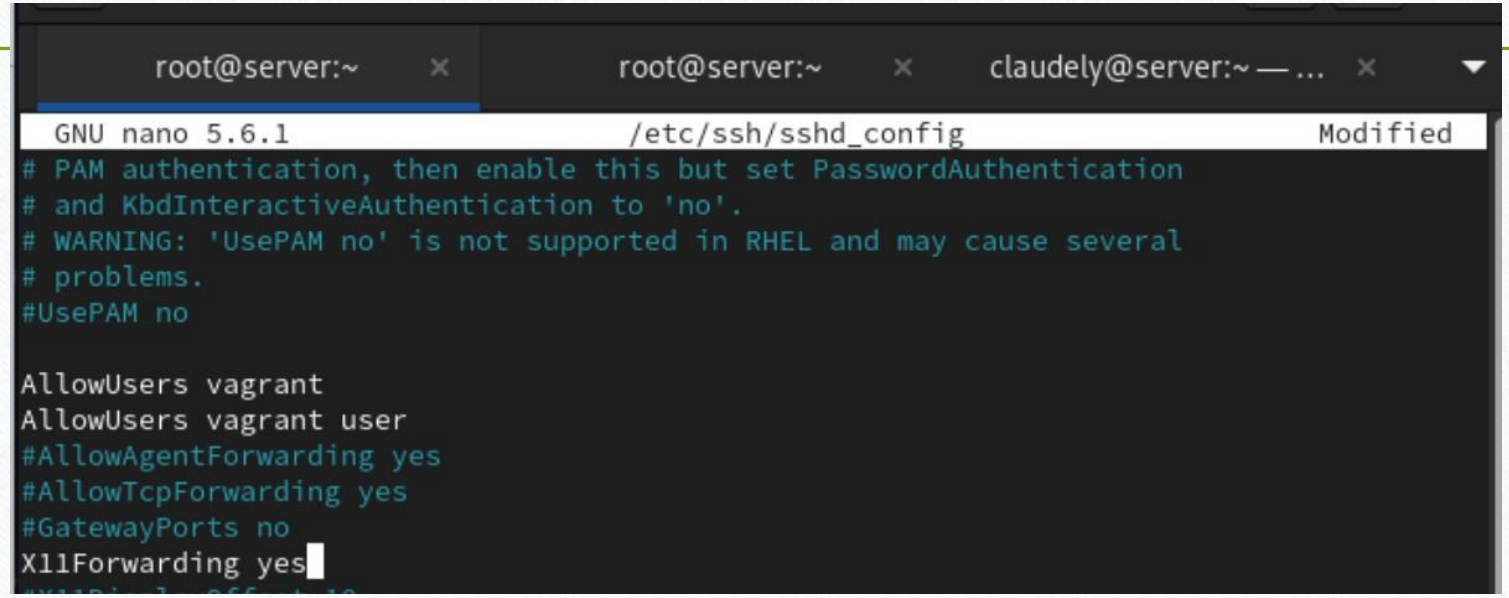


Рис. 7.1. Разрешение отображать на сервере в конфигурационном файле /etc/ssh/sshd_config на локальном клиентском компьютере графические интерфейсы X11.

Запуск графических приложений через SSH (X11Forwarding)

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 7.2. Перезапуск sshd.

Внесение изменений в настройки внутреннего окружения виртуальной машины

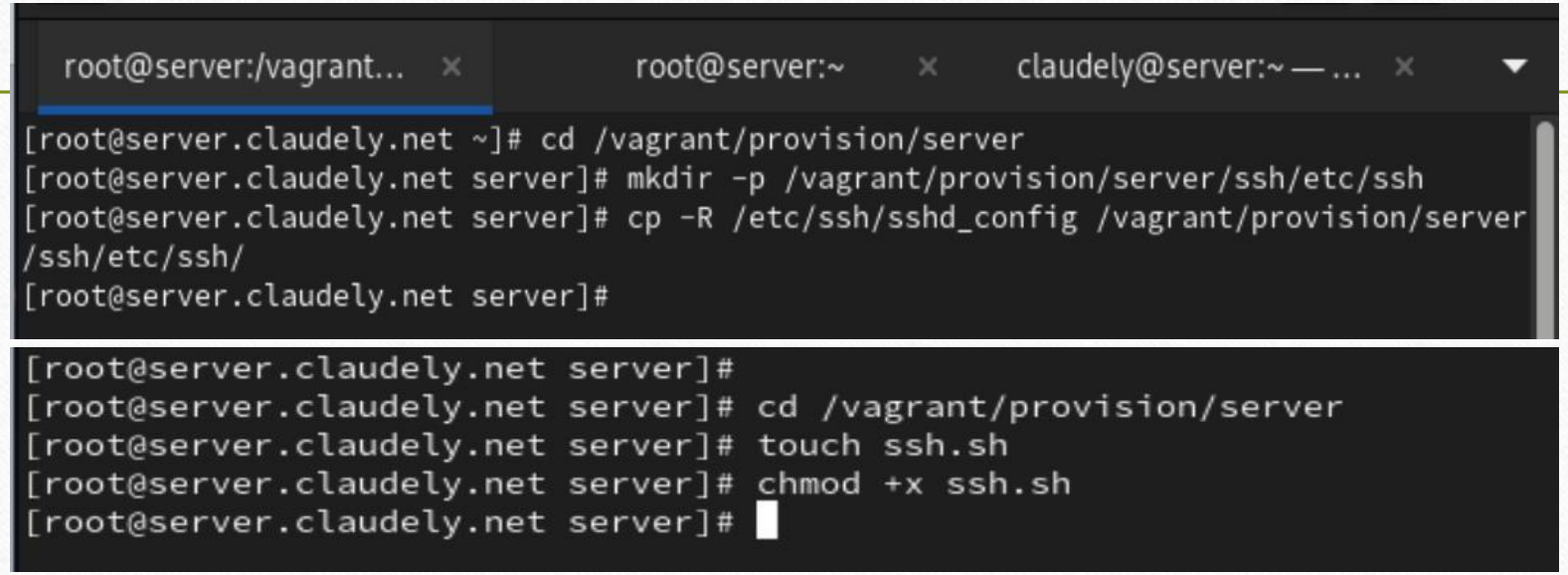


Рис. 8.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога ssh, в который поместили в соответствующие подкаталоги конфигурационный файл sshd_config. Создание в каталоге /vagrant/provision/server исполняемого файла ssh.sh.

Внесение изменений в настройки внутреннего окружения виртуальной машины

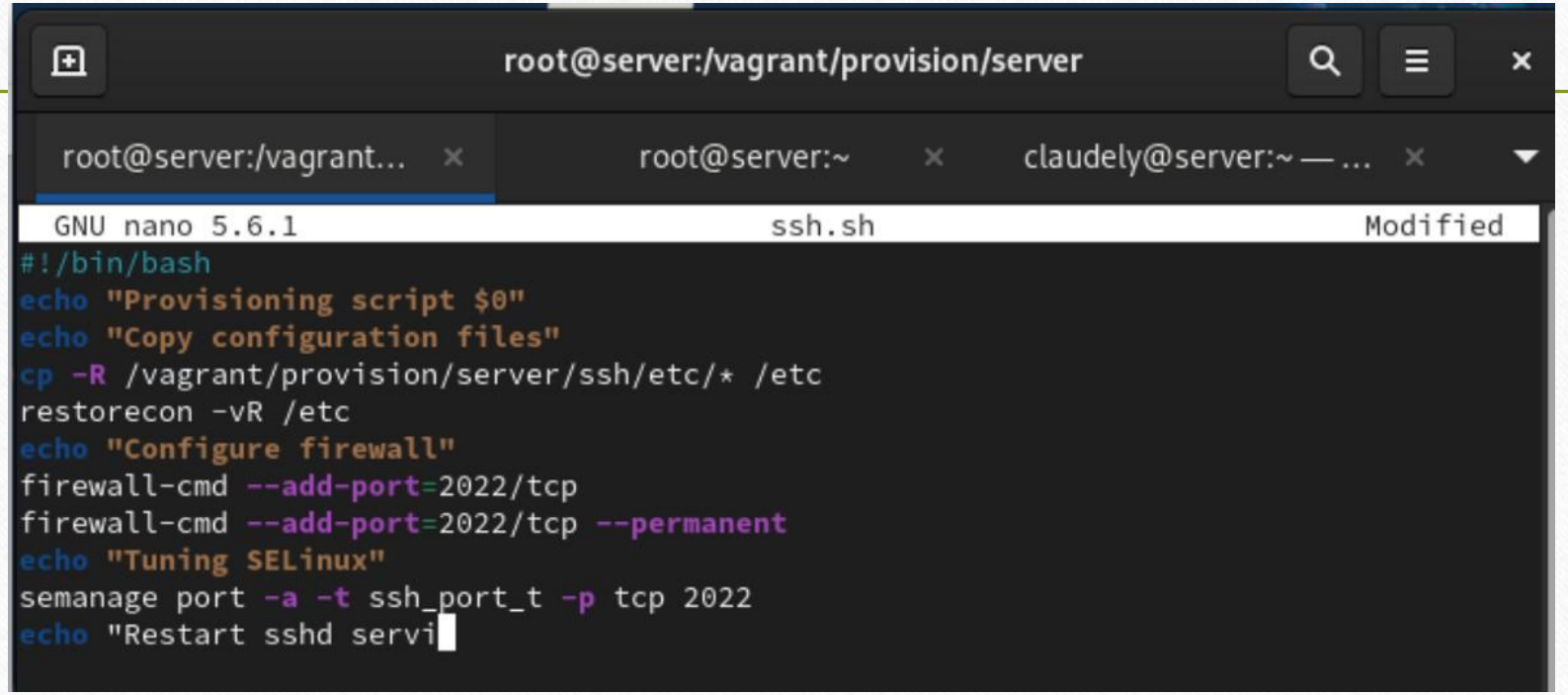


Рис. 8.2. Открытие файла на редактирование и написание в нём скрипта.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/firewall.sh"
server.vm.provision "server mail",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/mail.sh"
        server.vm.provision "server ssh",
                        type: "shell",
                        preserve_order: true,
                        path: "provision/server/ssh.sh"

    server.vm.provider :virtualbox do |v|
```

Рис. 8.3. Редактирование конфигурационного файла Vagrantfile.

Вывод

В ходе выполнения лабораторной работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Спасибо за внимание!