Отчёт по лабораторной работе №11

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

# 2 Выполнение лабораторной работы

## 2.1 Запрет удалённого доступа по SSH для пользователя root

Затем запустим виртуальную машину server. Откроем терминал и перейдем в режим суперпользователя.

В дополнительном терминале запустим мониторинг системных событий с помощью команды journalctl -x -f. С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя root(рис. fig. 1):

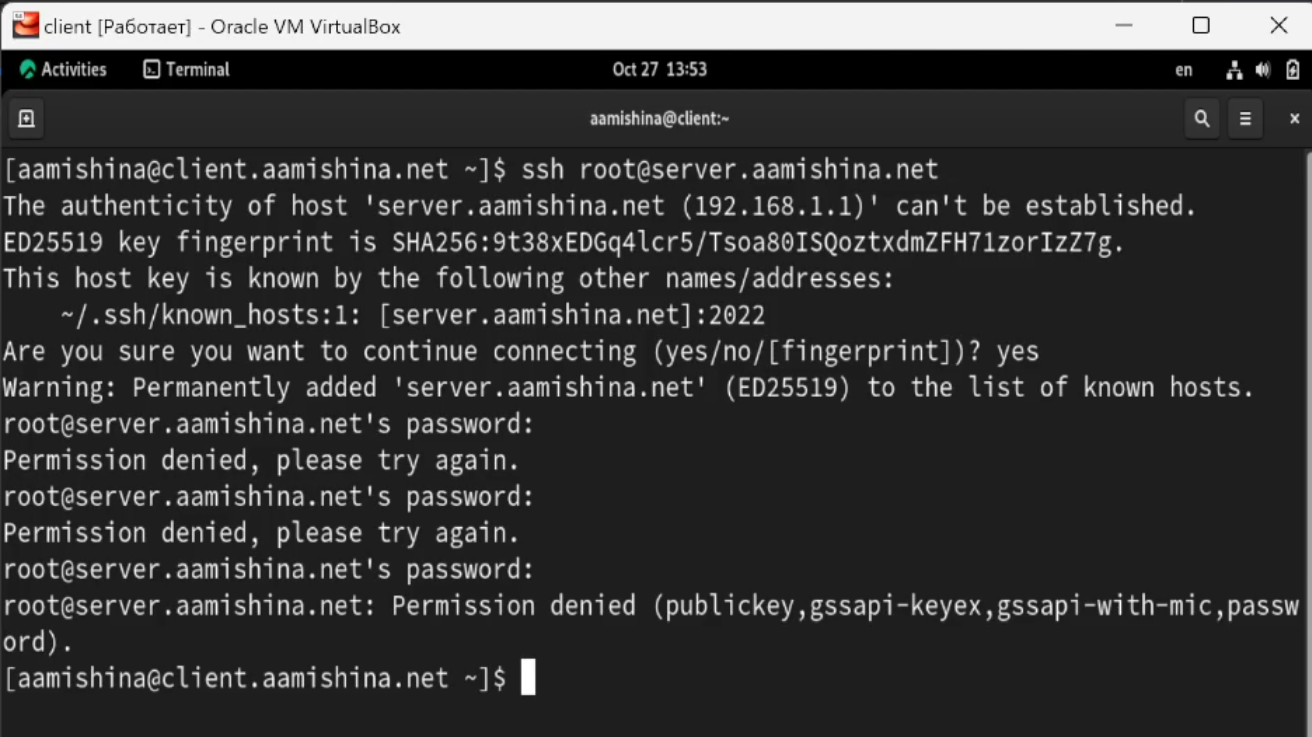


Рис. 1: Попытка установить SSH-соединение

При попытке соединения, так как мы делаем это первый раз, добавлям сервер в список известных хостов. Затем требуется ввести пароль от пользователя root, но соединение отклоняется.

На сервере откроем файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретим вход на сервер пользователю root, установив(рис. fig. 2):

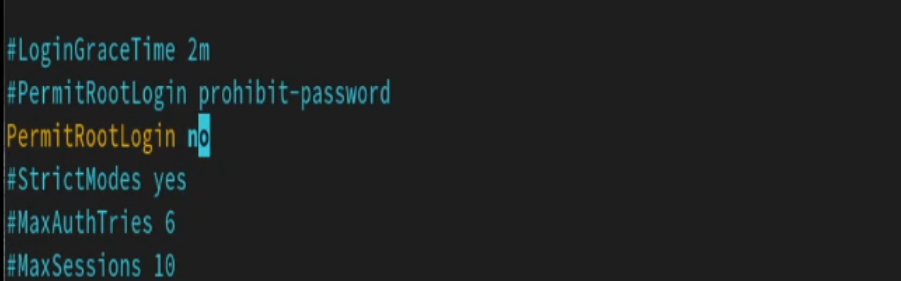


Рис. 2: Файл /etc/ssh/sshd\_config. Запрет входа на сервер пользователю root

После сохранения изменений в файле конфигурации перезапустим sshd с помощью команды systemctl restart sshd. Повторяем попытку получения доступа через root, вновь получаем отказ в доступе.

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя aamishina (рис. fig. 3):

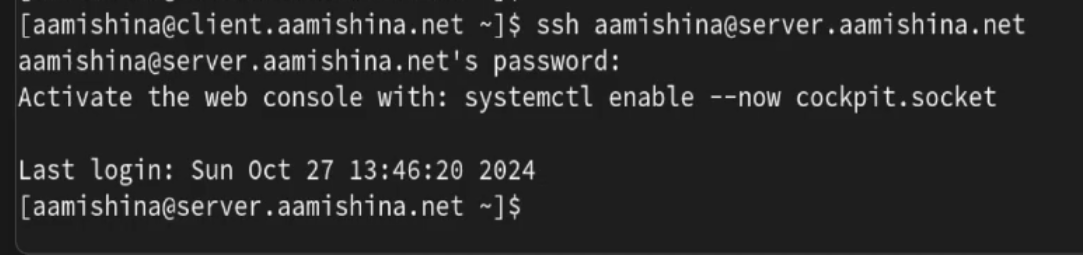


Рис. 3: Попытка установить SSH-соединение с клиента

Соединениие проходит удачно.

На сервере откроем файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавим строку(fig. 4):

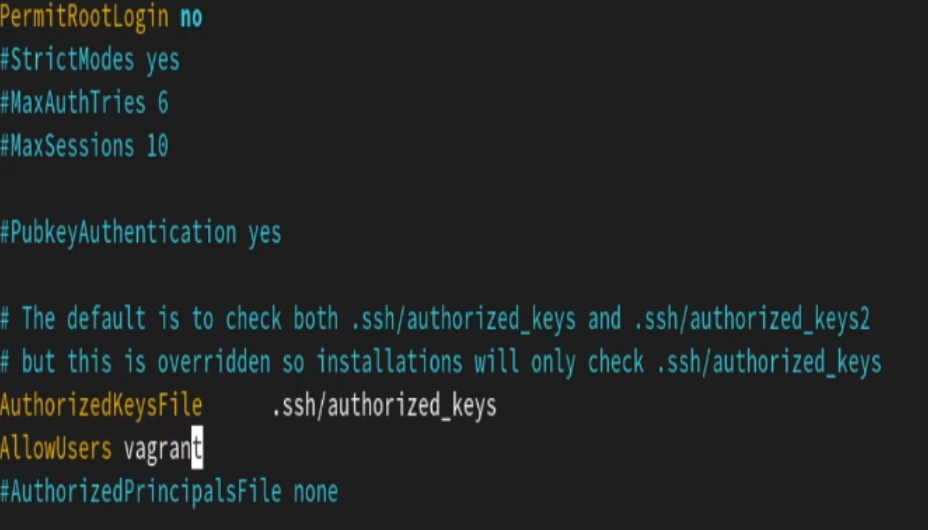


Рис. 4: Файл /etc/ssh/sshd\_config. Изменение разрешенных пользователей для sshd

После сохранения изменений в файле конфигурации перезапустим sshd.

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя aamishina(рис. fig. 5):

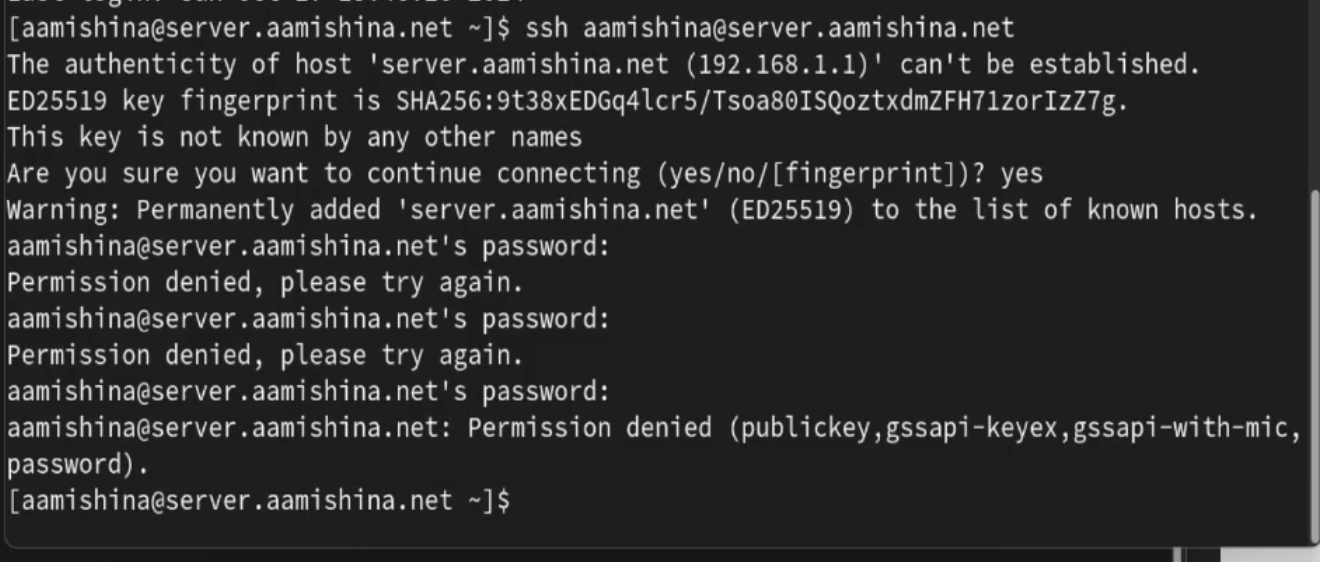


Рис. 5: Определение службы аутентификации пользователей

В этот раз соединение не устанавливается, так как в списке разрешенных пользователей нет нашего.

В файле /etc/ssh/sshd\_config конфигурации sshd внесем следующее изменение(fig. 6):

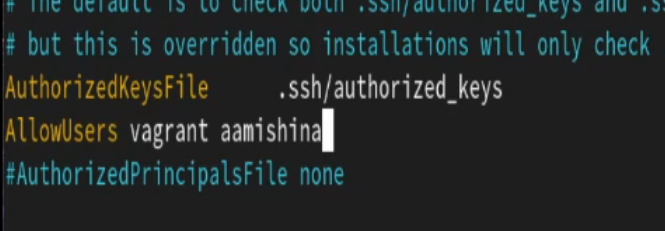


Рис. 6: Файл /etc/ssh/sshd\_config. Изменение разрешенных пользователей для sshd

Снова попытаемся установить соединение с клиента к серверу(fig. 7):

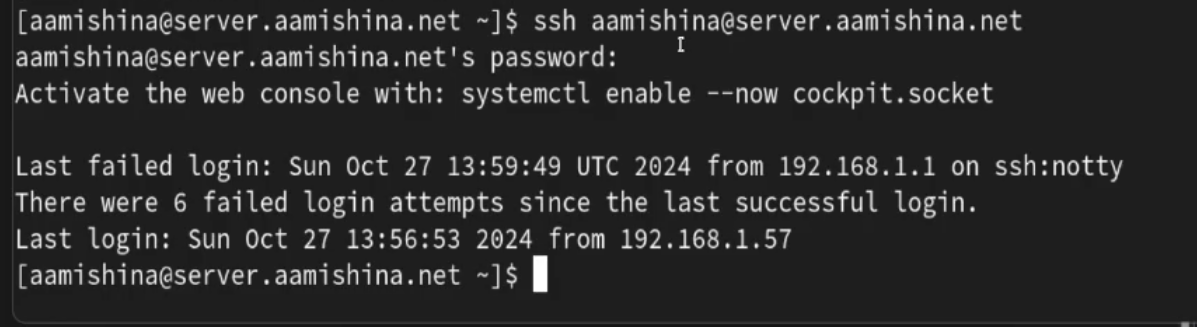


Рис. 7: Временный запуск SMTP-сервера

В этот раз доступ получен.

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдем строку Port и ниже этой строки добавим(fig. 8):

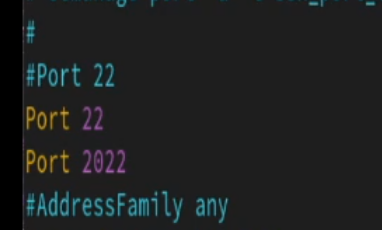


Рис. 8: Файл /etc/ssh/sshd\_configю. Добавление портов в файл конфигураций

Эта запись сообщает процессу sshd о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.

После сохранения изменений в файле конфигурации перезапустим sshd.

Посмотрим расширенный статус работы sshd(fig. 9):

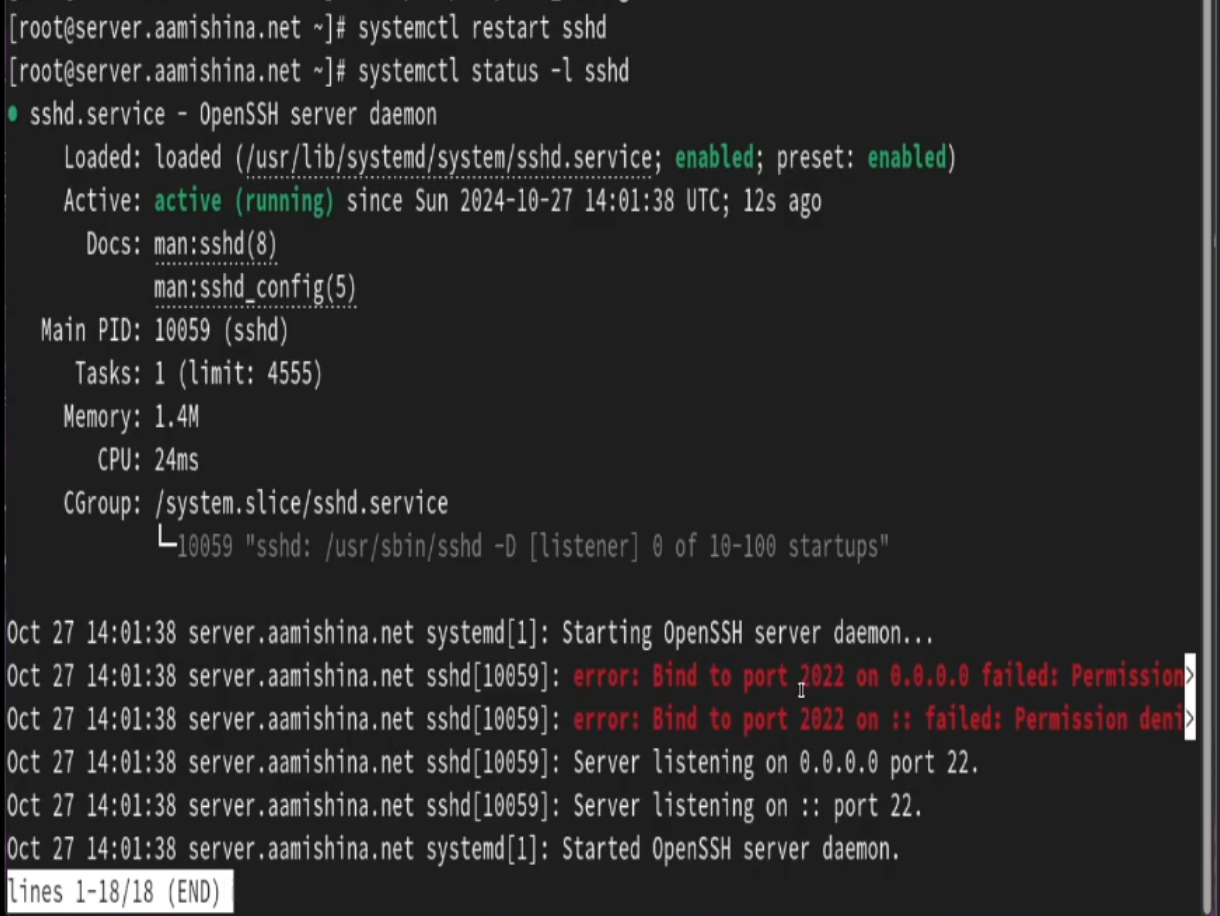


Рис. 9: Расширенный статус работы sshd

Система сообщает об отказе в работе sshd через порт 2022. Дополнительно посмотрим сообщения в терминале с мониторингом системных событий(рис. fig. 10):

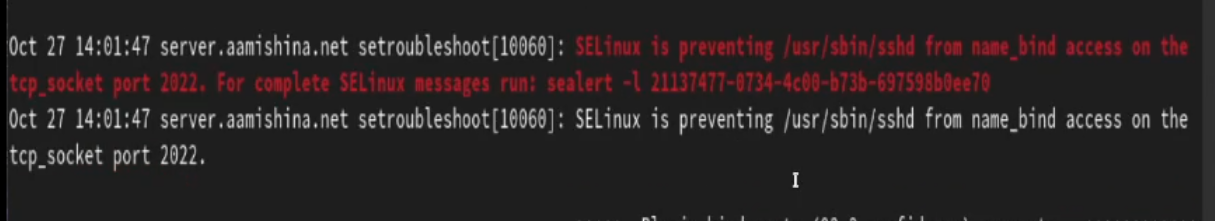


Рис. 10: Мониторинг системных сообщений

Можно увидеть, что отказ происходит из-за запрета SELinux на работу с этим портом.

Исправим на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана откроем порт 2022 протокола. Вновь перезапустим sshd и посмотрите расширенный статус его работы. Статус показывает, что процесс sshd теперь прослушивает два порта(fig. 11)

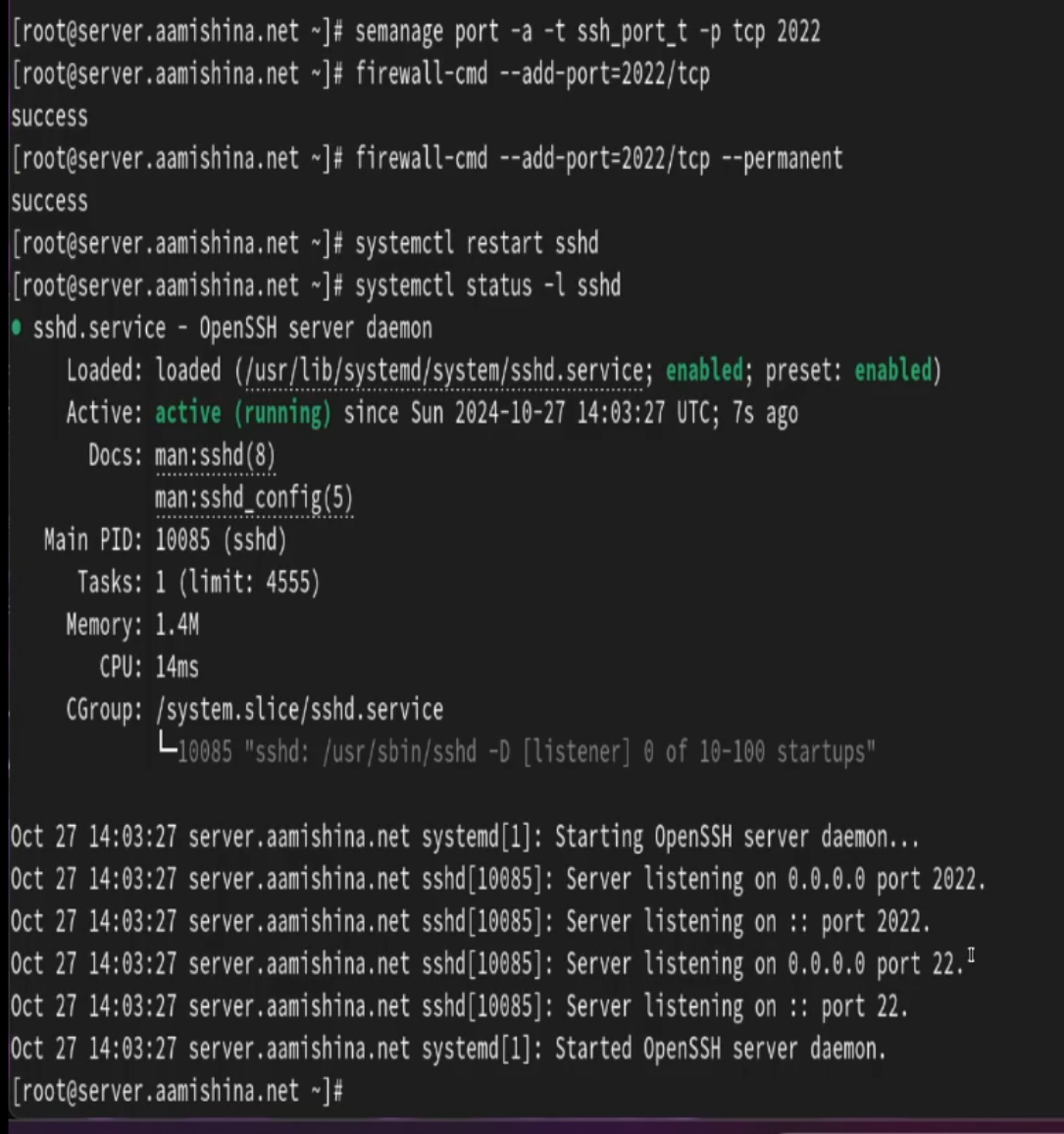


Рис. 11: Просмотр расширенного статуса работы sshd после настройки работы по порту 2022

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя aamishina обычным способом и указав порт 2022(рис. fig. 12):

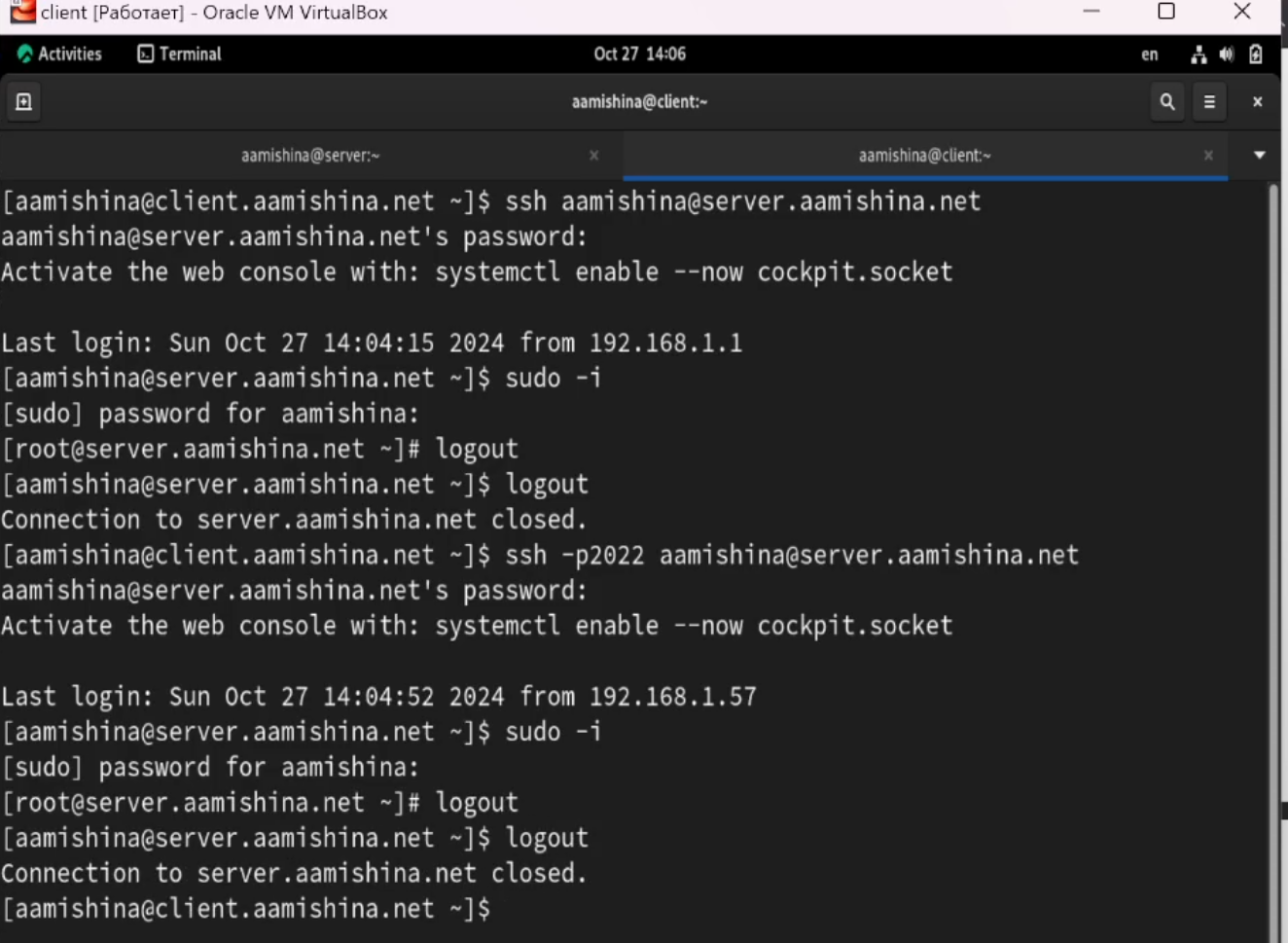


Рис. 12: Установка SSH-соединение с клиента

## 2.4 Настройка удалённого доступа по SSH по ключу

Создадим пару из открытого и закрытого ключей для входа на сервер.

На сервере в конфигурационном файле /etc/ssh/sshd\_config зададим параметр, разрешающий аутентификацию по ключу, написав:

PubkeyAuthentication yes

После сохранения изменений в файле конфигурации перезапустим sshd.

На клиенте сформируем SSH-ключ, введя в терминале(fig. 13):

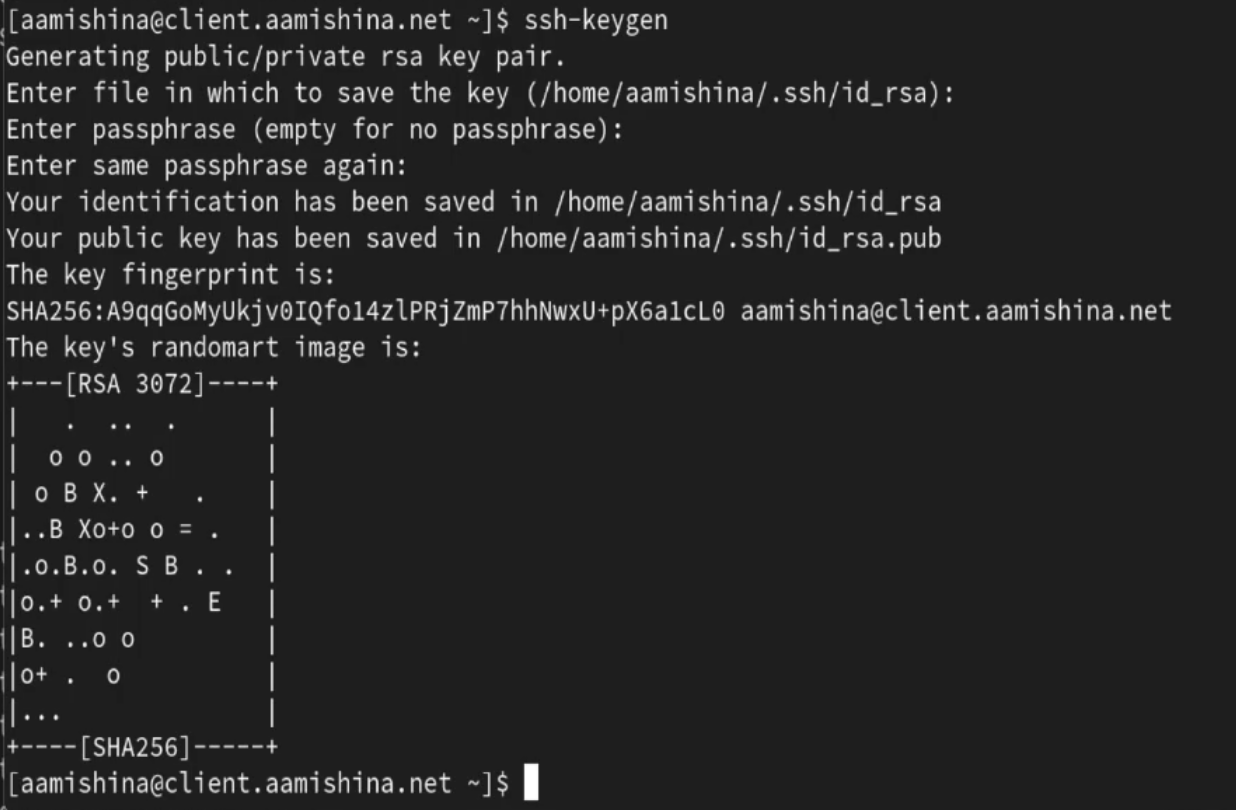


Рис. 13: Формирования SSH-ключа на клиенте

Закрытый ключ теперь будет записан в файл ~/.ssh/id\_rsa, а открытый ключ записывается в файл ~/.ssh/id\_rsa.pub.

Скопируем открытый ключ на сервер, введя на клиенте:

ssh-copy-id user@server.user.net

Попробуем получить доступ с клиента к серверу посредством SSH-соединения(fig. 14):

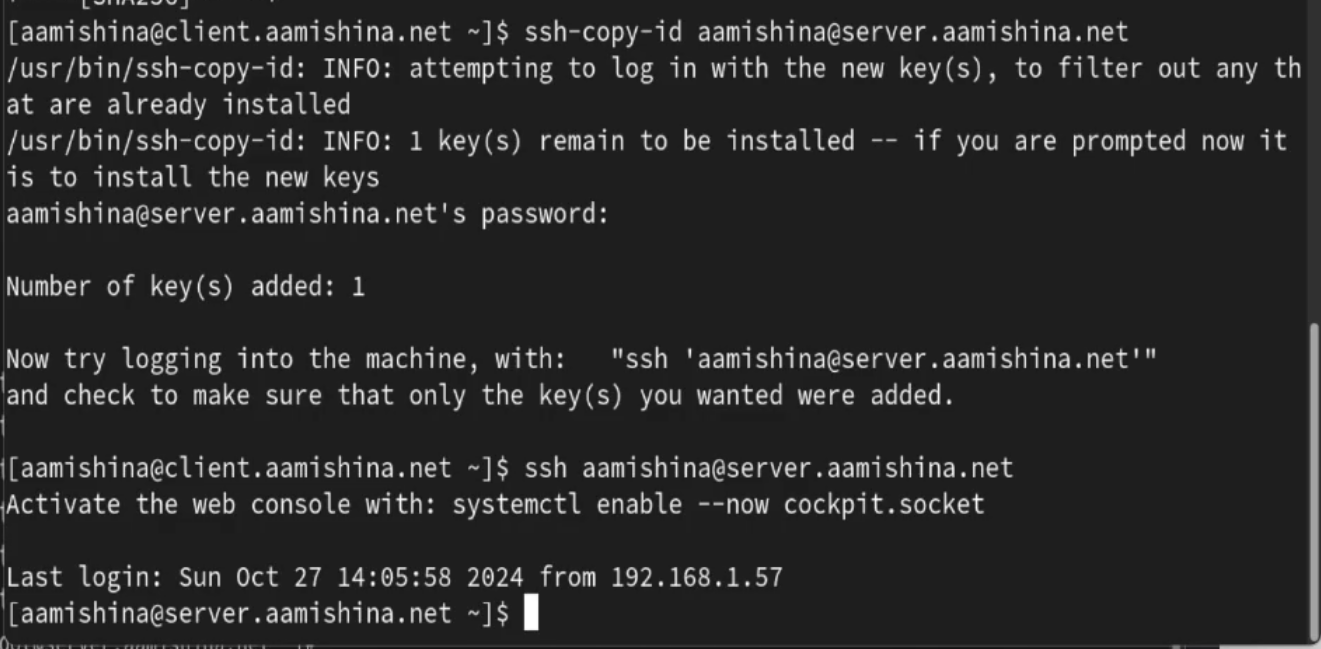


Рис. 14: Установка SSH-соединения с сервером с клиента

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP, на данный момент их нет. Перенаправим порт 80 на server.aamishina.net на порт 8080 на локальной машине и вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP(рис. fig. 15)

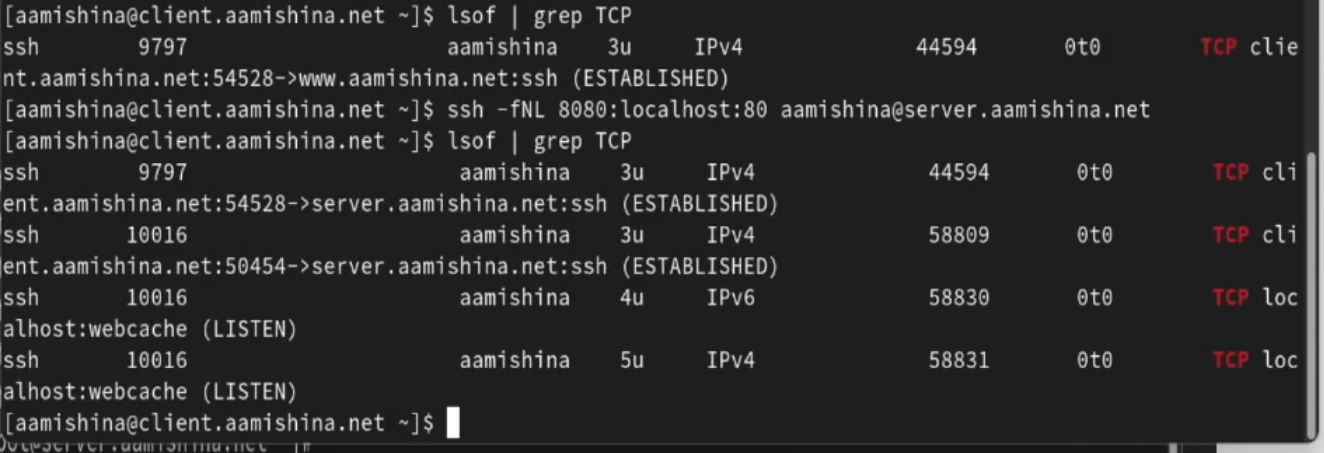


Рис. 15: Просмотр активных служб с протоколом TCP. Перенаправление порта 80 на server.aamishina.net на порт 8080

Появилось три новые службы, использующие TCP протокол – появился доступ к server.aamishina.net по ssh, а также к локальному хосту по IPv4 и IPv6.

На клиенте запустим браузер и в адресной строке введем localhost:8080. Отображается страница с приветствием «Welcome to the server.aamishina.net server»(fig. 16):

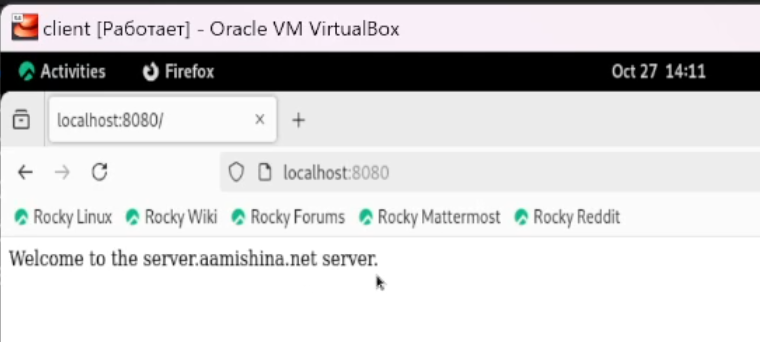


Рис. 16: Просмотр локального сервера в браузере на клиенте

## 2.6 Запуск консольных приложений через SSH

На клиенте откроем терминал под пользователем aamishina и посмотрим с клиента имя узла сервера, файлов на сервере (рис. fig. 17) и почту(рис. fig. 18):

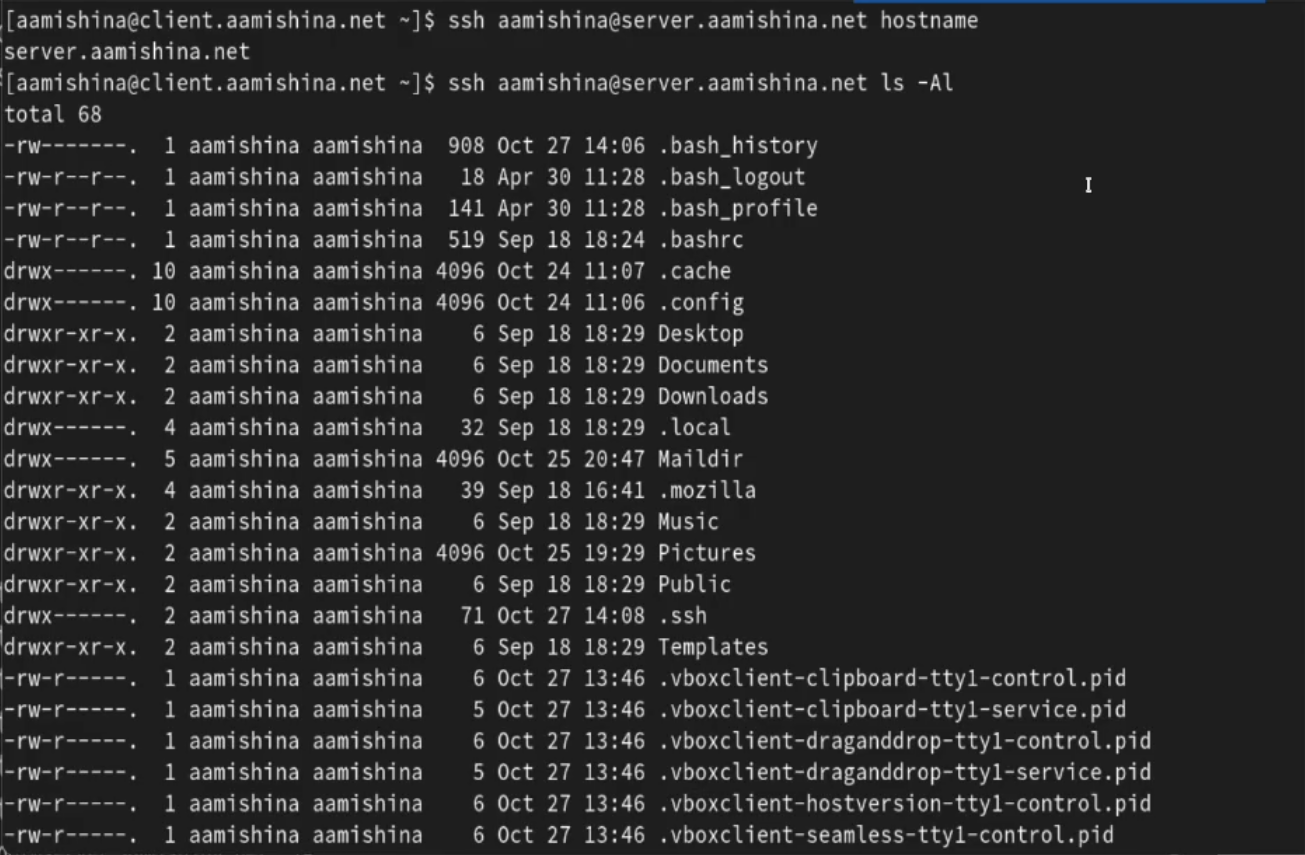


Рис. 17: Просмотр имени узла сервера и файлов на сервере через ssh

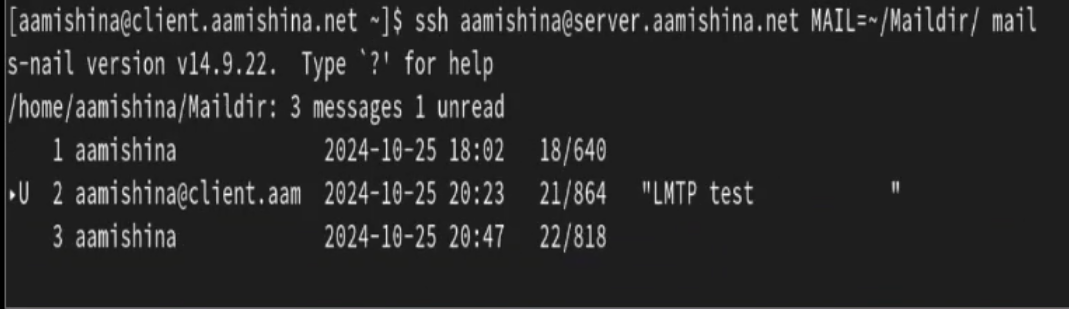


Рис. 18: Просмотр почты через ssh

## 2.7 Запуск графических приложений через SSH (X11Forwarding)

На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешим отображать на локальном клиентском компьютере графические интерфейсы X11, прописав:

X11Forwarding yes

После сохранения изменения в конфигурационном файле перезапустим sshd.

Попробуем с клиента удалённо подключиться к серверу и запустить графическое приложение firefox(рис. fig. 19):

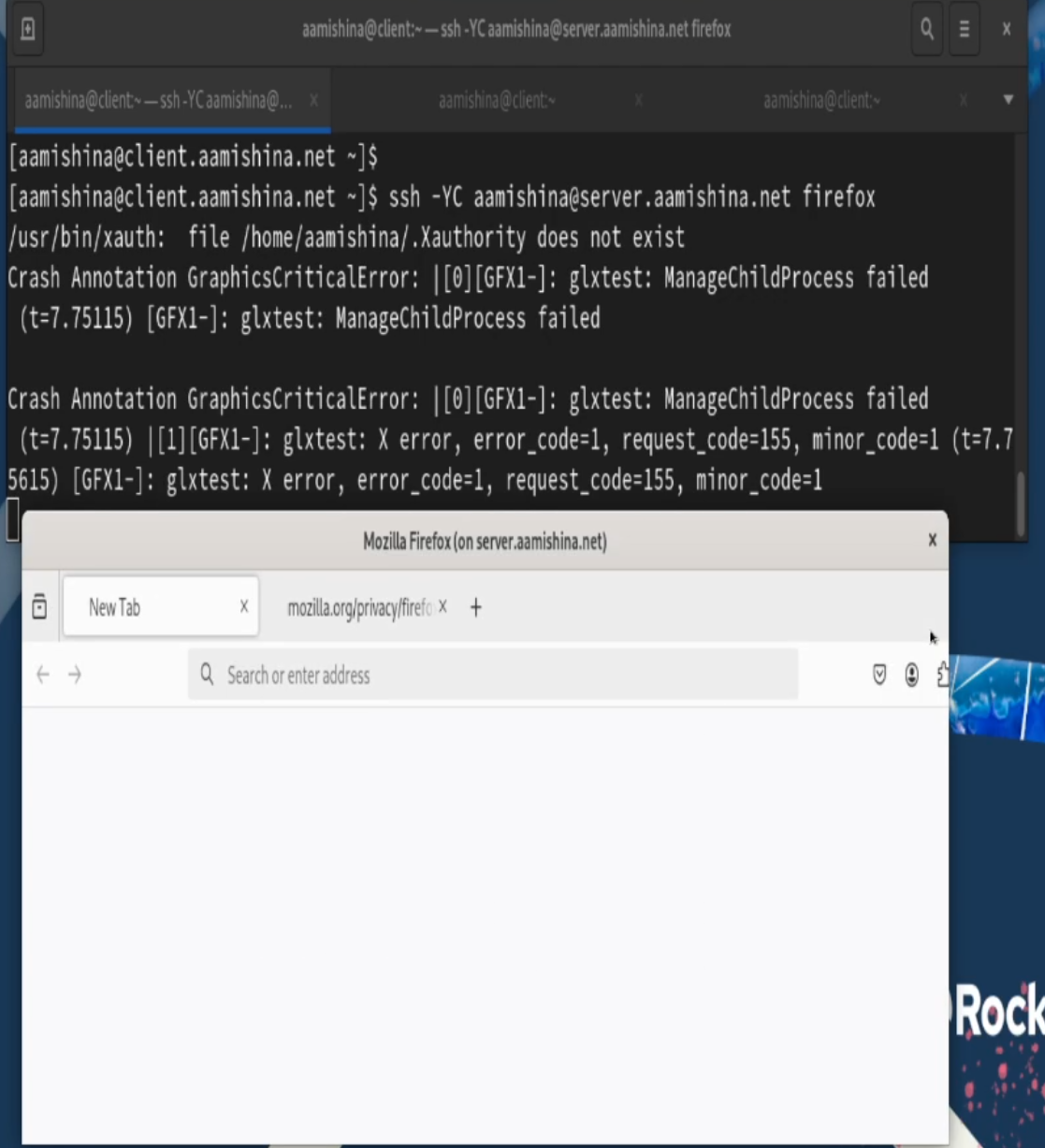


Рис. 19: Запуск графического приложения через ssh

## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог ssh, в который поместим в соответствующие подкаталоги конфигурационный файл sshd\_config и в каталоге /vagrant/provision/server создадим исполняемый файл ssh.sh(рис. fig. 20)

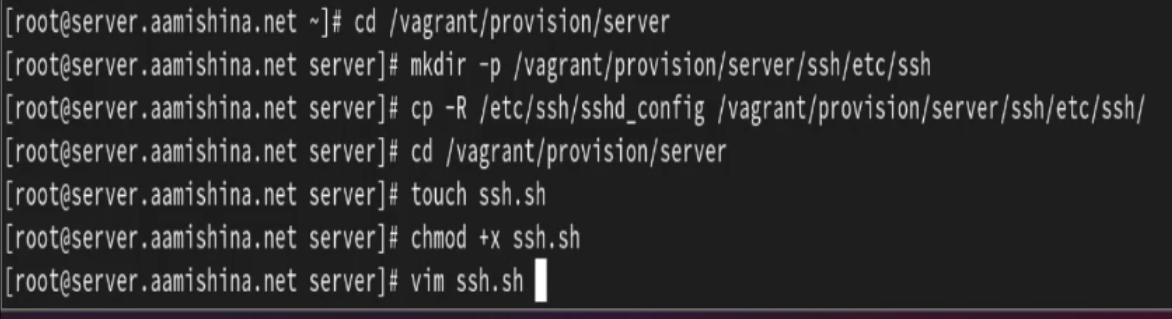


Рис. 20: Создание окружения для внесения изменений в настройки окружающей среды

Пропишем скрипт в /vagrant/provision/server/ssh.sh (fig. 21):

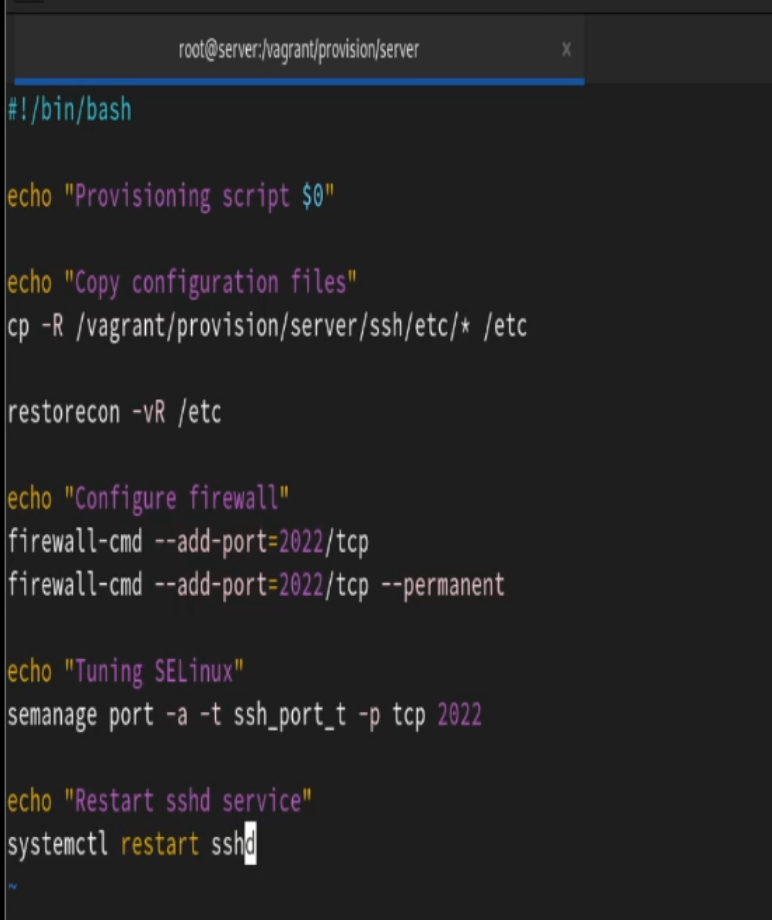


Рис. 21: Скрипт файла /vagrant/provision/server/ssh.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим следующую запись в разделе конфигурации для сервера(fig. 22):

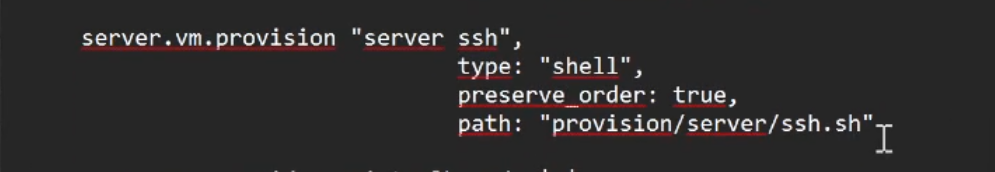


Рис. 22: Изменние конфигурационного файла Vagrant

# 3 Контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

В файле /etc/ssh/sshd\_config конфигурации прописать PermitRootLogin no и AllowUsers alice.

1. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

Для настройки удалённого доступа по SSH через несколько портов нужно отредактировать файл конфигурации SSH и добавить строку Port <порт>.

1. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

Для установки фонового соединения без команды используется параметр -N при использовании команды ssh: ssh -N <hostname>

1. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

ssh -fNL 80:localhost:55555 server2.example.com

1. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

semanage port -a -t ssh\_port\_t -p tcp 2022

1. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

firewall-cmd --add-port=2022/tcp --permanent

# 4 Выводы

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