

# Настройка безопасного удалённого доступа по протоколу SSH

---

Абд эль хай мохамад

15-12-2023

РУДН, Москва, Российская Федерация

# Введение

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

# Задачи

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root.
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя.
3. Настройте удалённый доступ к серверу по SSH через порт 2022.
4. Настройте удалённый доступ к серверу по SSH по ключу.
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080.
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере.
7. Используя удалённое SSH-соединение, запустите с клиента графическое приложение на сервере.

# Запрет удалённого доступа по SSH для пользователя root

С клиента я попытался получить доступ к серверу через SSH-соединение через пользователя root:  
`ssh root@server.maabeldelhay.net`

Я не смог получить доступ к серверу как пользователь root.

На сервере я открыл файл конфигурации `sshd` `/etc/ssh/sshd_config`, чтобы отредактировать настройку и запретить пользователю root вход на сервер, установив:  
«PermitRootLogin нет»

После сохранения изменений в файле конфигурации я перезапустил `sshd`:  
`systemctl перезапустить sshd`

Я снова попытался получить доступ клиента к серверу через SSH-соединения через пользователя root:  
`ssh root@server.maabeldelhay.net`  
У меня не было доступа к серверу.

```
root@server:~  
Dec 12 19:17:36 server.maabeldelhay.net named[872]: timed out resolving 'cdn77.org/DS/IN': 192.168.1.1#53  
Dec 12 19:17:36 server.maabeldelhay.net named[872]: timed out resolving 'cdn77.org/DS/IN': 192.168.1.1#53  
Dec 12 19:17:36 server.maabeldelhay.net named[872]: network unreachable resolving 'sec2.rcode0.net/AAAA/IN': 2001:67c:1bc::100#53  
Dec 12 19:17:36 server.maabeldelhay.net named[872]: network unreachable resolving 'sec2.rcode0.net/AAAA/IN': 2001:67c:10b8::100#53  
Dec 12 19:17:36 server.maabeldelhay.net named[872]: network unreachable resolving 'sec2.rcode0.net/A/IN': 2001:67c:10b8::100#53  
Dec 12 19:17:58 server.maabeldelhay.net sshd[5896]: main: sshd: ssh-rsa algorithm is disabled  
Dec 12 19:18:07 server.maabeldelhay.net unix_chkpwd[5898]: password check failed for user (root)  
Dec 12 19:18:07 server.maabeldelhay.net sshd[5896]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.118 user=root  
Dec 12 19:18:10 server.maabeldelhay.net sshd[5896]: Failed password for root from 192.168.1.118 port 47088 ssh2  
Dec 12 19:18:15 server.maabeldelhay.net unix_chkpwd[5901]: password check failed for user (root)  
Dec 12 19:18:17 server.maabeldelhay.net sshd[5896]: Failed password for root from 192.168.1.118 port 47088 ssh2  
Dec 12 19:18:24 server.maabeldelhay.net unix_chkpwd[5902]: password check failed for user (root)  
Dec 12 19:18:26 server.maabeldelhay.net sshd[5896]: Failed password for root from 192.168.1.118 port 47088 ssh2  
Dec 12 19:18:26 server.maabeldelhay.net sshd[5896]: Connection closed by authenticating user root 192.168.1.118 port 47088 [preauth]  
Dec 12 19:18:26 server.maabeldelhay.net sshd[5896]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.118 user=root
```

# Настройка удалённого доступа по SSH по ключу

На сервере в файле конфигурации `/etc/ssh/sshd_config` я изменил параметр, чтобы разрешить аутентификацию по ключу:

`PubkeyAuthentication yes`

После сохранения изменений в файле конфигурации я перезапустил `sshd`.

На клиенте я начал генерировать ключ SSH, введя в терминал под пользователем `maabeldelhay`:

`ssh-keygen`

Закрытый ключ был записан в файл `~/.ssh/id_rsa`, а открытый ключ — в файл `~/.ssh/id_rsa.pub`.

Скопировал открытый ключ на сервер, введя на клиенте:

`ssh-copy-id maabeldelhay@server.maabeldelhay.net`

В конце концов я попытался получить доступ к серверу с клиента через SSH-соединение:

`ssh maabeldelhay@server.maabeldelhay.net`

теперь я смог пройти аутентификацию без ввода пароля для учетной записи удаленного пользователя.

```
[maabeldelhay@client.maabeldelhay.net ~]$ ssh-copy-id maabeldelhay@server.maabeldelhay.net
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
maabeldelhay@server.maabeldelhay.net's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'maabeldelhay@server.maabeldelhay.net'"
and check to make sure that only the key(s) you wanted were added.

[maabeldelhay@client.maabeldelhay.net ~]$ ssh maabeldelhay@server.maabeldelhay.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Dec 12 20:16:46 2023
[maabeldelhay@server.maabeldelhay.net ~]$
```

# Выполнение задачи

сначала я проверил, работают ли какие-либо службы на клиенте по протоколу TCP:

```
lsof | grep TCP
```

по-видимому, не было никаких служб, работающих с TCP.

Я перенаправил порт 80 на server.maabedelhay.net на порт 8080 на локальном компьютере.

```
ssh -fNL 8080:localhost:80
```

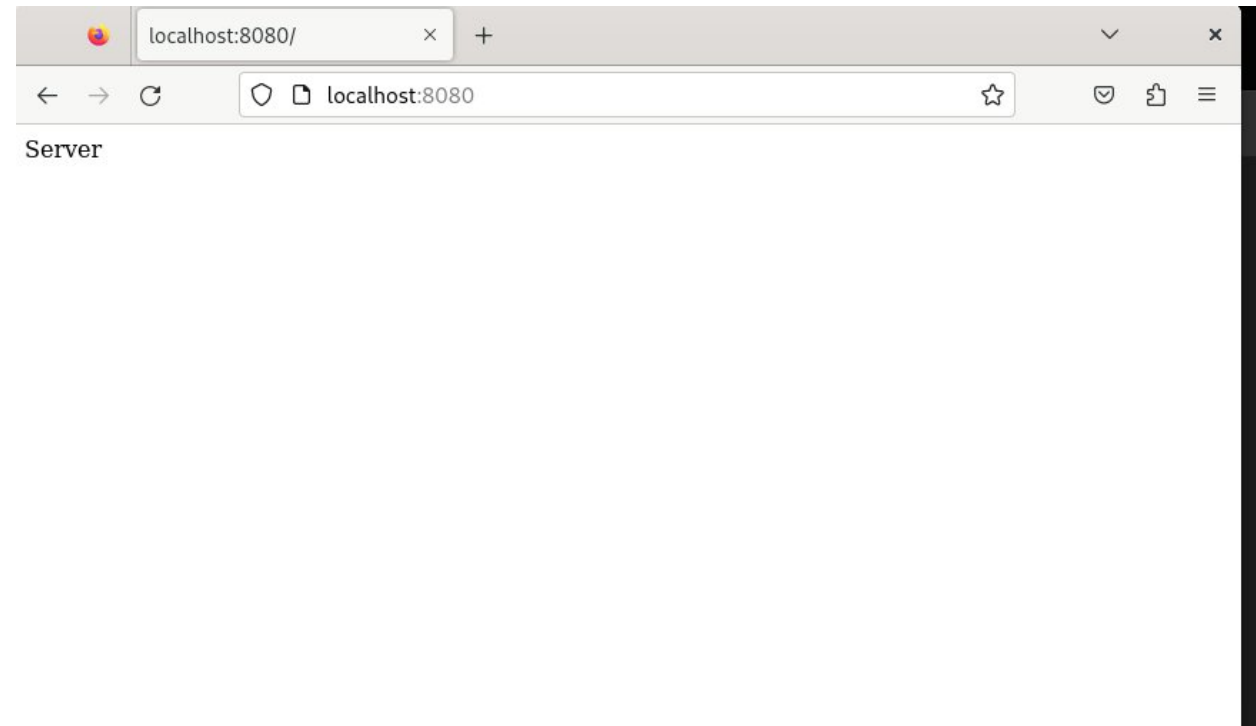
```
maabedelhay@server.maabedelhay.net
```

Снова на клиенте я проверил, работают ли какие-либо службы по протоколу TCP:

```
lsof | grep TCP
```

Он показывает, что служба, использующая протокол TCP, — это ssh, а также пользователь, использующий эту службу, и расположение файла.

На клиенте я запустил Firefox и в адресной строке ввел localhost:8080. На веб-странице было указано «Сервер», поскольку он настроен для этого.



# Выполнение задачи

## фигура 13

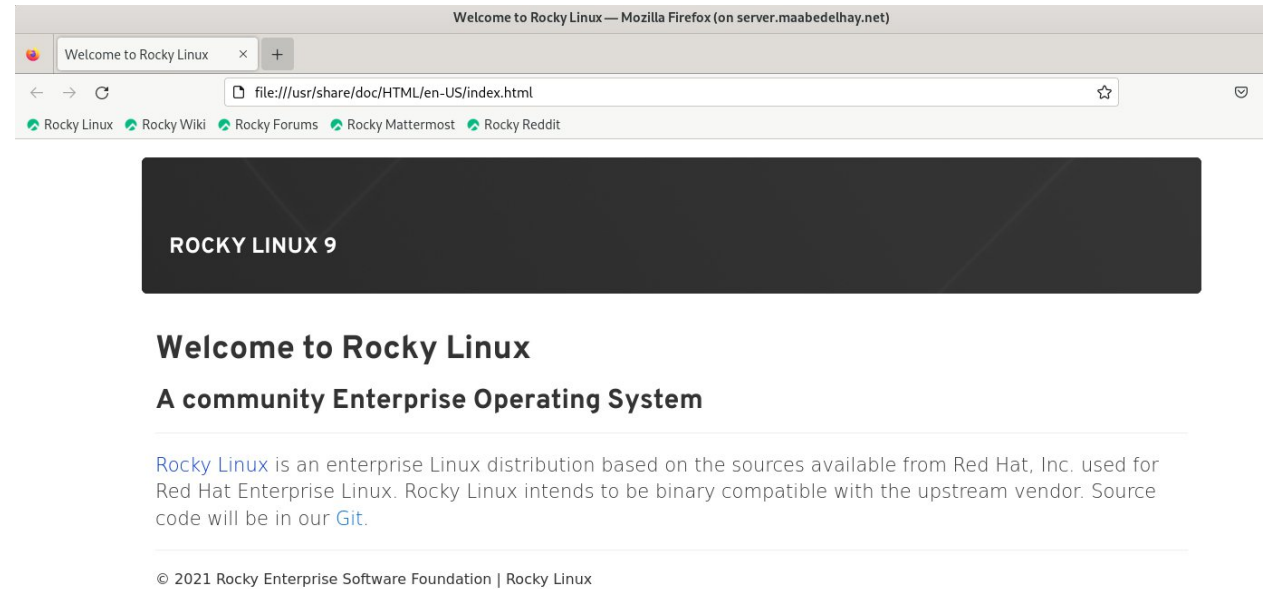
На сервере в файле конфигурации `/etc/ssh/sshd_config` я разрешил отображение графического интерфейса X11 на локальном клиентском компьютере:

X11Переадресация да

После сохранения изменений в файле конфигурации я перезапустил `sshd`.

Я подключился к серверу удаленно с клиента и запустил графическое приложение:

`ssh -YC maabedelhay@server.maabedelay.net firefox`



Получил практические навыки настройки удаленного доступа к серверу по SSH.



Спасибо За Внимание