

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 11

дисциплина: Администрирование сетевых подсистем

Настройка безопасного удалённого доступа по протоколу SSH

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

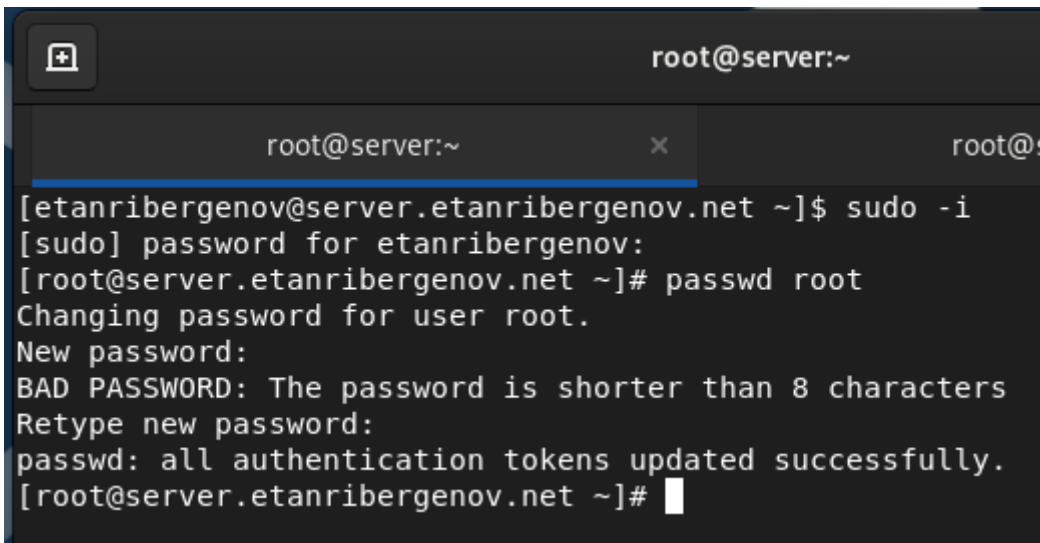
Цель работы

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

Ход работы

1. Запрет удалённого доступа по SSH для пользователя root

1. На сервере задайте пароль для пользователя root, если этого не было сделано ранее
`passwd root`



```
root@server:~  
[etanribergenov@server.etanribergenov.net ~]$ sudo -i  
[sudo] password for etanribergenov:  
[root@server.etanribergenov.net ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@server.etanribergenov.net ~]#
```

Рис. 1. Смена пароля

2. На сервере в дополнительном терминале запустите мониторинг системных событий

```
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]# journalctl -x -f
Apr 08 16:03:34 server.etanribergenov.net systemd[1]: Starting Hostname Service.
..
Subject: A start job for unit systemd-hostnamed.service has begun execution
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit systemd-hostnamed.service has begun execution.

The job identifier is 2691.
Apr 08 16:03:35 server.etanribergenov.net systemd[1]: Started Hostname Service.
Subject: A start job for unit systemd-hostnamed.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit systemd-hostnamed.service has finished successfully.

The job identifier is 2691.
Apr 08 16:03:54 server.etanribergenov.net passwd[5964]: pam_unix(passwd:chauthtok): password changed for root
Apr 08 16:03:54 server.etanribergenov.net passwd[5964]: gkr-pam: couldn't update
```

Рис. 2. Запуск мониторинга системных событий

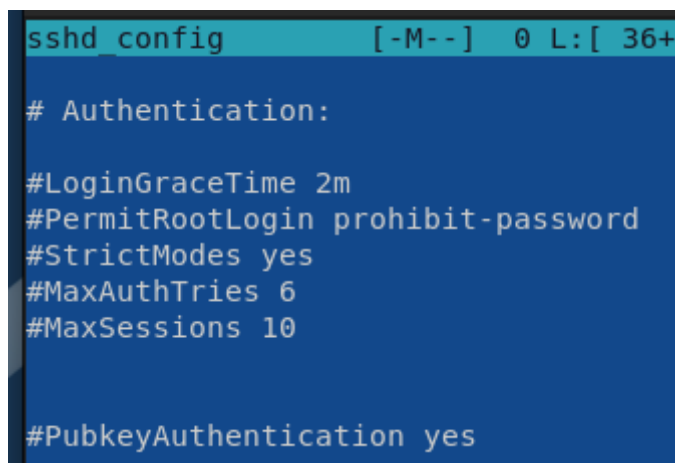
3. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root

`ssh root@server.etanribergenov.net`

```
etanribergenov@client:~
[etanribergenov@client.etanribergenov.net ~]$ ssh root@server.etanribergenov.net
The authenticity of host 'server.etanribergenov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.etanribergenov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yesyes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.etanribergenov.net' (ED25519) to the list of known hosts.
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
root@server.etanribergenov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 3. Попытка получения доступа к серверу посредством SSH-соединения через root

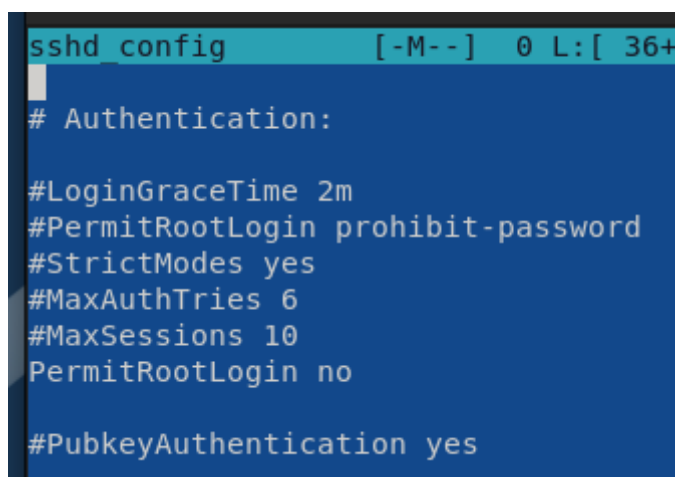
Получить доступ не удалось. Проверил конфиг. файл sshd – там для параметра разрешения входа для root установлено по умолчанию значение «запретить ввод пароля».

A terminal window showing the contents of the /etc/ssh/sshd_config file. The title bar reads 'sshd_config [-M--] 0 L:[36+'. The visible configuration includes: '# Authentication:', '#LoginGraceTime 2m', '#PermitRootLogin prohibit-password', '#StrictModes yes', '#MaxAuthTries 6', '#MaxSessions 10', and '#PubkeyAuthentication yes'.

```
sshd_config [-M--] 0 L:[ 36+
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
```

Рис. 4. Конф. файл sshd_config

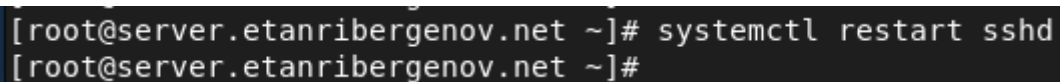
4. На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root, установив
PermitRootLogin no

A terminal window showing the sshd_config file after modification. The title bar is the same. The configuration is identical to the previous screenshot, but the line '#PermitRootLogin prohibit-password' has been replaced with 'PermitRootLogin no'.

```
sshd_config [-M--] 0 L:[ 36+
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
PermitRootLogin no
#PubkeyAuthentication yes
```

Рис. 5. Конф. файл sshd_config: изменение значения параметра

5. После сохранения изменений в файле конфигурации перезапустите sshd:

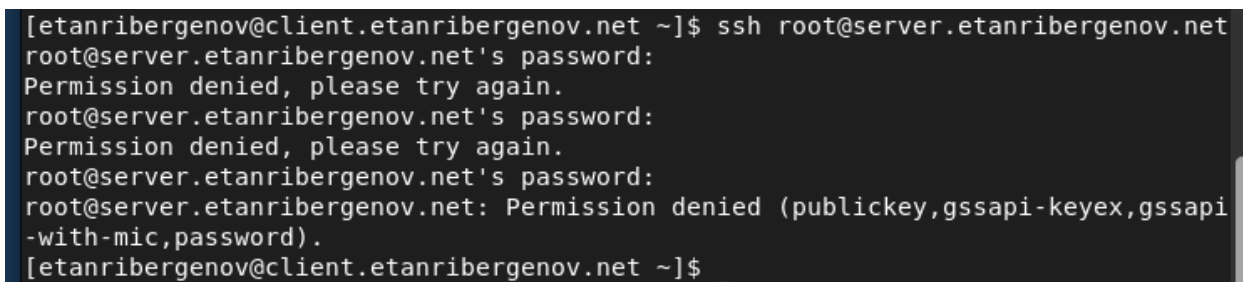
A terminal window showing the command to restart the sshd service using systemctl.

```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 6. Перезапуск sshd

- Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root

```
ssh root@server
```



```
[etanribergenov@client.etanribergenov.net ~]$ ssh root@server.etanribergenov.net
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
root@server.etanribergenov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[eetanribergenov@client.etanribergenov.net ~]$
```

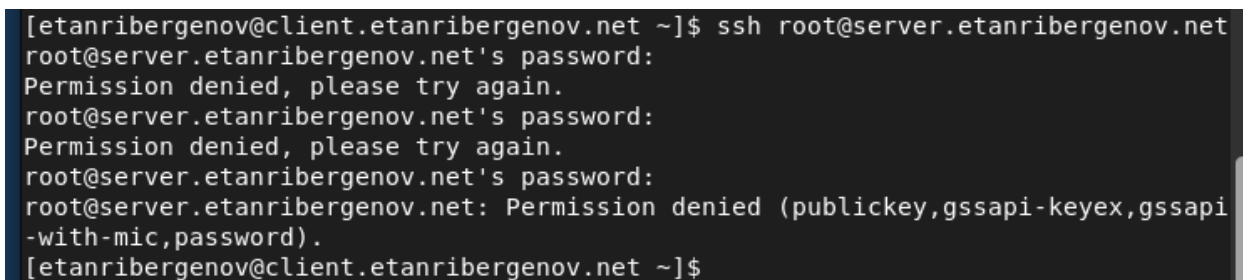
Рис. 7. Повторная попытка получения доступа к серверу

Собственно, ничего не изменилось – в доступе всё также отказано.

2. Ограничение списка пользователей для удалённого доступа по SSH

- С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя etanribergenov

```
ssh etanribergenov@server.etanribergenov.net
```



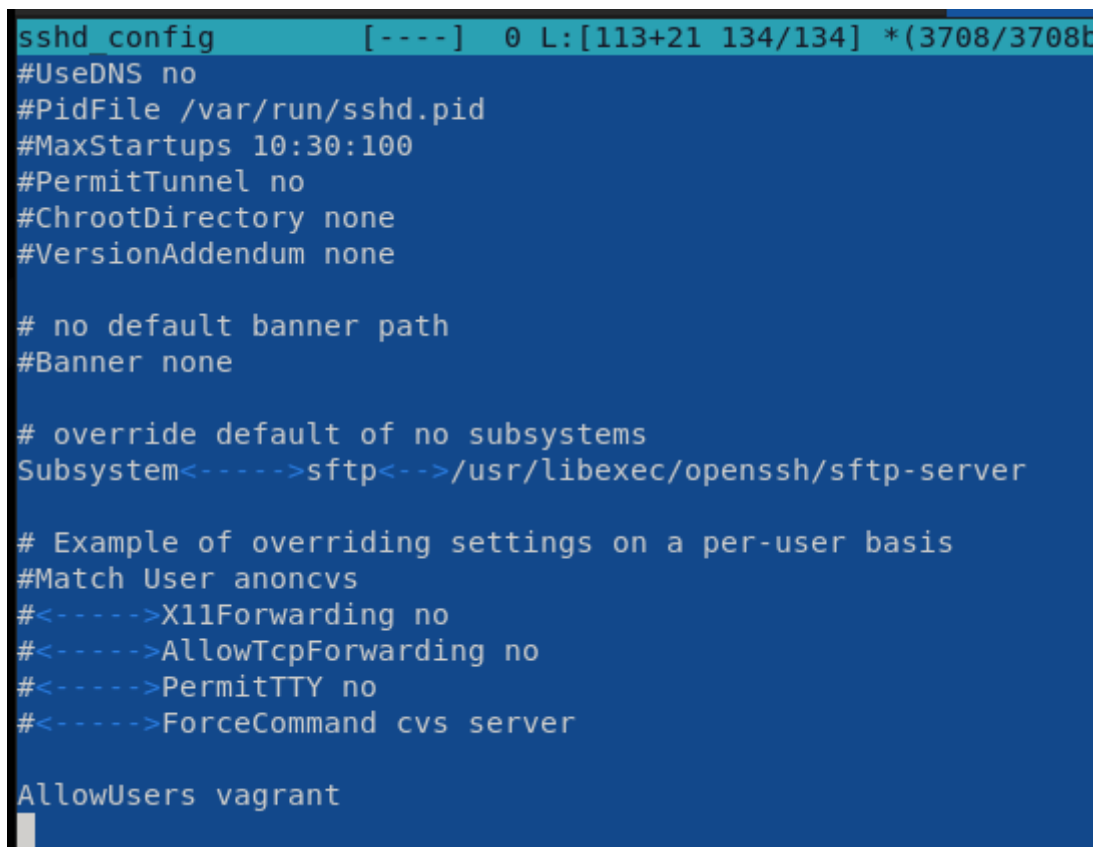
```
[etanribergenov@client.etanribergenov.net ~]$ ssh root@server.etanribergenov.net
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
Permission denied, please try again.
root@server.etanribergenov.net's password:
root@server.etanribergenov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[eetanribergenov@client.etanribergenov.net ~]$
```

Рис. 8. Попытка получения доступа к серверу посредством SSH-соединения

Ничего нового в конф. файл sshd добавлено не было – следовательно, и ничего нового не произошло.

2. На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd на редактирование и добавьте строку

AllowUsers vagrant



```
sshd_config [----] 0 L:[113+21 134/134] *(3708/3708b
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

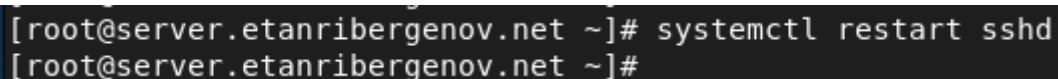
# override default of no subsystems
Subsystem<----->sftp<-->/usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#<----->X11Forwarding no
#<----->AllowTcpForwarding no
#<----->PermitTTY no
#<----->ForceCommand cvs server

AllowUsers vagrant
```

Рис. 9. Разрешение на доступ пользователю vagrant

3. После сохранения изменений в файле конфигурации перезапустите sshd



```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 10. Перезапуск sshd

- Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя etanribergenov

```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
etanribergenov@server.etanribergenov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 11. Попытка получения доступа к серверу клиентом через SSH

- В файле /etc/ssh/sshd_config конфигурации sshd внесите следующее изменение
AllowUsers vagrant etanribergenov

```
sshd_config  [-M--]  0 L:[114+21 135/135] *(3732/37
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem<----->sftp<-->/usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#<----->X11Forwarding no
#<----->AllowTcpForwarding no
#<----->PermitTTY no
#<----->ForceCommand cvs server

AllowUsers vagrant etanribergenov
```

Рис. 12. Разрешение на доступ пользователю etanribergenov

6. После сохранения изменений в файле конфигурации перезапустите sshd и вновь попытайтесь получить доступ с клиента к серверу посредством SSH-соединения через пользователя etanribergenov.

```
[root@server.etanribergenov.net ~]# systemctl restart sshd  
[root@server.etanribergenov.net ~]#
```

Рис. 13. Перезапуск sshd

```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net  
etanribergenov@server.etanribergenov.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last failed login: Sat Apr 8 17:30:36 UTC 2023 from 192.168.1.30 on ssh:notty  
There were 3 failed login attempts since the last successful login.  
Last login: Sat Apr 8 15:52:30 2023  
[etanribergenov@server.etanribergenov.net ~]$
```

Рис. 14. Попытка получения доступа с клиента к серверу через SSH

3. Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации sshd /etc/ssh/sshd_config найдите строку Port и ниже этой строки добавьте

Port 22

Port 2022

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.


```
sshd_config [-M--]
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Рис. 15. Организация соединения sshd через два разных порта

2. После сохранения изменений в файле конфигурации перезапустите sshd

```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 16. Перезапуск sshd

3. Посмотрите расширенный статус работы sshd

`systemctl status -l sshd`

```
[root@server.etanribergenov.net ~]#
[root@server.etanribergenov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-04-08 17:38:39 UTC; 17s ago
     Docs: man:ssh(8)
           man:ssh_config(5)
   Main PID: 7272 (sshd)
    Tasks: 1 (limit: 5789)
   Memory: 1.7M
      CPU: 61ms
   CGroup: /system.slice/ssh.service
           └─7272 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 08 17:38:39 server.etanribergenov.net systemd[1]: Starting OpenSSH server daemon:
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: error: Bind to port 2022: Address
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: error: Bind to port 2022: Address
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: Server listening on 0.0.0.0 port
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: Server listening on :: port
Apr 08 17:38:39 server.etanribergenov.net systemd[1]: Started OpenSSH server daemon:
ESCOC
```

Рис. 17. Просмотр расширенного статуса работы sshd (1)

```
t systemd[1]: Starting OpenSSH server daemon...
t sshd[7272]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
t sshd[7272]: error: Bind to port 2022 on :: failed: Permission denied.
t sshd[7272]: Server listening on 0.0.0.0 port 22.
t sshd[7272]: Server listening on :: port 22.
t systemd[1]: Started OpenSSH server daemon.
~
```

Рис. 18. Просмотр расширенного статуса работы sshd (2)

```
A start job for unit sshd.service has begun execution.

The job identifier is 3998.
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: error: Bind to port 2022 on :: failed: Permission denied.
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: Server listening on 0.0.0.0 port 22.
Apr 08 17:38:39 server.etanribergenov.net sshd[7272]: Server listening on :: port 22.
Apr 08 17:38:39 server.etanribergenov.net systemd[1]: Started OpenSSH server daemon.

Subject: A start job for unit sshd.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit sshd.service has finished successfully.

The job identifier is 3998.
Apr 08 17:38:39 server.etanribergenov.net systemd[1]: Started dbus-:1.1-org.fedoraproject.Setroubleshootd@2.service.

Subject: A start job for unit dbus-:1.1-org.fedoraproject.Setroubleshootd@2.service has finished successfully
```

Рис. 19. Мониторинг системных сообщений

Видно, что подключение через порт 2022 не удалось — отказано в доступе.

4. Исправьте на сервере метки SELinux к порту 2022

```
semanage port -a -t ssh_port_t -p tcp 2022
```

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

Рис. 20. Исправление на сервере меток SELinux к порту 2022

5. В настройках межсетевого экрана откройте порт 2022 протокола TCP

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

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

```
[root@server.etanribergenov.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.etanribergenov.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.etanribergenov.net ~]#
```

Рис. 21. Открытие порта 2022 протокола TCP в настройке firewall

6. Вновь перезапустите sshd и посмотрите расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта.

```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 22. Перезапуск sshd

```
[root@server.etanribergenov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-04-08 17:53:25 UTC; 18s ago
     Docs: man:ssh(8)
           man:ssh_config(5)
  Main PID: 7427 (sshd)
    Tasks: 1 (limit: 5789)
   Memory: 2.2M
      CPU: 55ms
   CGroup: /system.slice/ssh.service
           └─7427 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 08 17:53:25 server.etanribergenov.net systemd[1]: Starting OpenSSH server daemon:
Apr 08 17:53:25 server.etanribergenov.net sshd[7427]: Server listening on 0.0.0.0 port 22.
Apr 08 17:53:25 server.etanribergenov.net sshd[7427]: Server listening on :: port 22.
Apr 08 17:53:25 server.etanribergenov.net sshd[7427]: Server listening on 0.0.0.0 port 2022.
Apr 08 17:53:25 server.etanribergenov.net sshd[7427]: Server listening on :: port 2022.
Apr 08 17:53:25 server.etanribergenov.net systemd[1]: Started OpenSSH server daemon:
#55686
```

Рис. 23. Просмотр расширенного статуса sshd (1)

```
t systemd[1]: Starting OpenSSH server daemon...
t sshd[7427]: Server listening on 0.0.0.0 port 2022.
t sshd[7427]: Server listening on :: port 2022.
t sshd[7427]: Server listening on 0.0.0.0 port 22.
t sshd[7427]: Server listening on :: port 22.
t systemd[1]: Started OpenSSH server daemon.
~
```

Рис. 24. Просмотр расширенного статуса sshd (2)

7. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя etanribergenov

После открытия оболочки пользователя введите `sudo -i` для получения доступа root

```
[etanribergenov@server.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net
The authenticity of host 'server.etanribergenov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.etanribergenov.net' (ED25519) to the list of known hosts.
etanribergenov@server.etanribergenov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Apr  8 17:32:37 2023 from 192.168.1.30
[etanribergenov@server.etanribergenov.net ~]$
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]#
```

Рис. 25. Получение доступа через SSH к серверу и к root

8. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через своего пользователя, указав порт 2022:

```
ssh -p2022 etanribergenov@server.etanribergenov.net
```

После открытия оболочки пользователя введите `sudo -i` для получения доступа root

```
[etanribergenov@client.etanribergenov.net ~]$ ssh -p2022 etanribergenov@server.e
tanribergenov.net
etanribergenov@server.etanribergenov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Apr  8 17:58:06 2023 from 192.168.1.1
[etanribergenov@server.etanribergenov.net ~]$
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]#
```

Рис. 26. Получение доступа посредством SSH к серверу и к root через порт 2022

4. Настройка удалённого доступа по SSH по ключу

В этом упражнении создаётся пара из открытого и закрытого ключей для входа на сервер.

1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` задайте параметр, разрешающий аутентификацию по ключу

`PubkeyAuthentication yes`

```
sshd config [----]
PermitRootLogin no
PubkeyAuthentication yes
```

Рис. 27. Настройка разрешения аутентификации по ключу

2. После сохранения изменений в файле конфигурации перезапустите sshd

```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 28. Перезапуск sshd

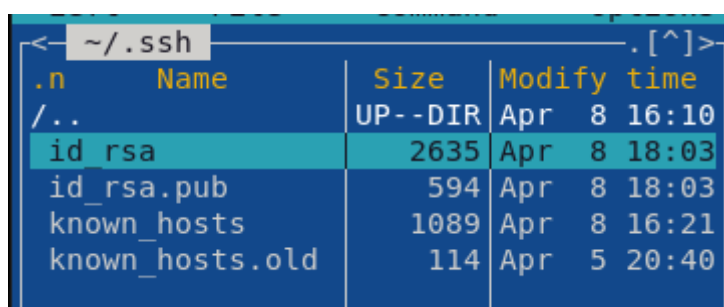
3. На клиенте сформируйте SSH-ключ, введя в терминале под своим пользователем `ssh-keygen`

Нажимал Enter для принятия каталога по умолчанию и при запросе фразы для использования установки без пароля.

```
[etanribergenov@client.etanribergenov.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/etanribergenov/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/etanribergenov/.ssh/id_rsa
Your public key has been saved in /home/etanribergenov/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:X6EEu0oKHwNFeMRx6/iJGgSqgg4ATFpJ0hwWspYRvZI etanribergenov@client.etanrib
ergenov.net
The key's randomart image is:
+---[RSA 3072]-----+
|.0*00....|
|B+==....|
|B=0 = ..|
|+E = 0. .|
|o * ... S|
|o+ ..0 .|
|+ o.. o .|
|o. o.|
|=.o.|
+----[SHA256]-----+
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 29. Генерация ssh-ключа

4. Закрытый ключ теперь будет записан в файл ~/.ssh/id_rsa, а открытый ключ записывается в файл ~/.ssh/id_rsa.pub. ~/.ssh/id_rsa.pub



Name	Size	Modify	time
UP--DIR		Apr 8	16:10
id_rsa	2635	Apr 8	18:03
id_rsa.pub	594	Apr 8	18:03
known_hosts	1089	Apr 8	16:21
known_hosts.old	114	Apr 5	20:40

Рис. 30. Проверка создания ключей

5. Скопируйте открытый ключ на сервер, введя на клиенте

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

При запросе введите пароль пользователя на удалённом сервере.

```
[etanribergenov@client.etanribergenov.net ~]$ ssh-copy-id etanribergenov@server.
etanribergenov.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 prompt
ed now it is to install the new keys
etanribergenov@server.etanribergenov.net's password:

Number of key(s) added: 1

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

Рис. 31. Копирование открытого ключа на сервер с клиента

```
/home/etanribergenov/.ssh/authorized_keys 594/594 100%
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDEHb0Q82A6L3y3W4xWjZotmAAVwjo/JeYhLG7uc/4N
RLy4dSbR7keIxfhEhYAdfBs/oRgzu0UumEVUkTwqr5c07x5gAclajA5z4PjMF0kA+BreucXKrsqnddb7
vrHe8YqUgQjT7tjPylihNCZQ1PlzpyDvbbvZid67kdRUPk0EQjcST1oLAUeP8dk5xINK3aS4m8j+2Coy
zGmMwiZS0FhZEE/jIwAJLNyUj80xH+3d93yYJreENNiSYG0xcdj33NgZJPmFoqUbJlB0Q0+RM07qCh3c
0KH+h3woDVj5sJAMUM0fz0j7qf6/3E8CUBog6hPsVolDC4PMTZ4hEaQ/+IdXsTBGuprqKbqGp0J32R0b
TMBW7h0KsFNqfU0wyuUw3NLyx6K5ZnXAajDYUWrohNLIRmrNpShi0reFMe0XnAlcBiZaNBGQvqLxeEGi
n6ym5tu/rlJrqzsfXTt4cD4LAtK6e7rQ2o9CJ0mI2agB8PCdhv0HrwalnH2MmMRbrJ1LXnU= etanrib
ergenov@client.etanribergenov.net
```

Рис. 32. Проверка наличия открытого ключа на сервере

6. Попробуйте получить доступ с клиента к серверу посредством SSH-соединения
- Теперь вы должны пройти аутентификацию без ввода пароля для учётной записи удалённого пользователя.

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

Last login: Sat Apr  8 17:59:50 2023 from 192.168.1.30
[etanribergenov@server.etanribergenov.net ~]$
```

Рис. 33. Получение доступа к серверу с клиента без ввода пароля

5. Организация туннелей SSH, перенаправление TCP-портов

1. На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP

`lsof | grep TCP`

```
[etanribergenov@client.etanribergenov.net ~]$ lsof | grep TCP
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 34. Просмотр запущенных служб с протоколом TCP

2. Перенаправьте порт 80 на server.etanribergenov.net на порт 8080 на локальной машине

`ssh -fNL 8080:localhost:80 etanribergenov@server.etanribergenov.net`

```
[etanribergenov@client.etanribergenov.net ~]$ ssh -fNL 8080:localhost:80 etanribergenov@server.etanribergenov.net
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 35. Создание туннеля: перенаправление порта 80 на сервере на порт 8080 локальной машины (клиента)

3. Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP

```
[etanribergenov@client.etanribergenov.net ~]$ lsof | grep TCP
ssh      7337      etanribergenov    3u      IPv4      53077
   0t0      TCP client.etanribergenov.net:37270->server.etanribergenov.net:s
sh (ESTABLISHED)
ssh      7337      etanribergenov    4u      IPv6      53099
   0t0      TCP localhost:webcache (LISTEN)
ssh      7337      etanribergenov    5u      IPv4      53100
   0t0      TCP localhost:webcache (LISTEN)
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 36. Просмотр запущенных служб с протоколом TCP

Первая запись свидетельствует о подключении (туннель), две остальные – переброску порта.

4. На клиенте запустите браузер и в адресной строке введите localhost:8080. Убедитесь, что отобразится страница с приветствием «Welcome to the server.etanribergenov.net server».

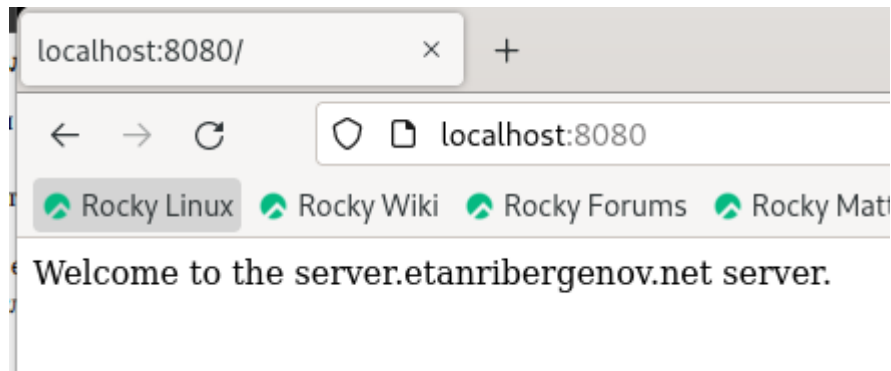


Рис. 37. Проверка работы туннеля

6. Запуск консольных приложений через SSH

1. На клиенте откройте терминал под своим пользователем
2. Посмотрите с клиента имя узла сервера

```
ssh etanribergenov@server.etanribergenov.net hostname
```

```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.n
et hostname
server.etanribergenov.net
[eetanribergenov@client.etanribergenov.net ~]$
```

Рис. 38. Просмотр с клиента имя узла сервера

3. Посмотрите с клиента список файлов на сервере

ssh etanribergenov@server.etanribergenov.net ls -Al

```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net
et ls -Al
total 44
-rw-----. 1 etanribergenov etanribergenov 771 Apr  8 18:29 .bash_history
-rw-r--r--. 1 etanribergenov etanribergenov  18 May 16 2022 .bash_logout
-rw-r--r--. 1 etanribergenov etanribergenov 141 May 16 2022 .bash_profile
-rw-r--r--. 1 etanribergenov etanribergenov 546 Apr  3 12:50 .bashrc
drwxr-xr-x. 10 etanribergenov etanribergenov 4096 Apr  6 12:01 .cache
drwx-----. 10 etanribergenov etanribergenov 4096 Apr  6 12:01 .config
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Desktop
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Documents
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Downloads
drwx-----.  4 etanribergenov etanribergenov   32 Apr  3 12:20 .local
drwx-----.  5 etanribergenov etanribergenov 4096 Apr  7 15:35 Maildir
drwxr-xr-x.  4 etanribergenov etanribergenov   39 Nov  1 09:32 .mozilla
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Music
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Pictures
drwxr-xr-x.  2 etanribergenov etanribergenov   6 Apr  3 12:20 Public
drwx-----.  2 etanribergenov etanribergenov   71 Apr  8 18:05 .ssh
```

Рис. 39. Просмотр с клиента списка файлов сервера

4. Посмотрите с клиента почту на сервере

ssh etanribergenov@server.etanribergenov.net MAIL=~/.Maildir/ mail

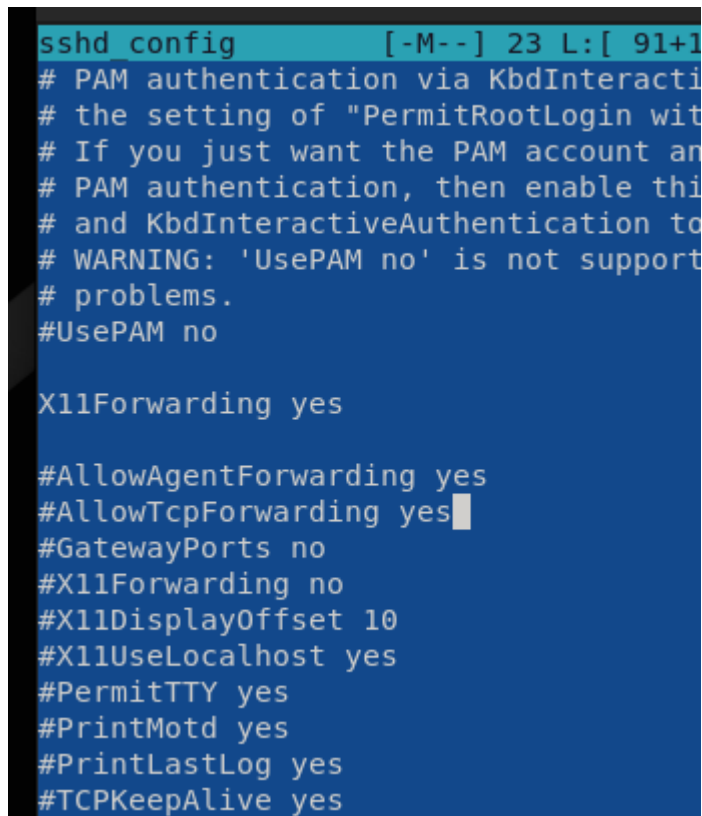
```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net
et MAIL=~/.Maildir/ mail
s-nail version v14.9.22.  Type '?' for help
/home/etanribergenov/Maildir: 2 messages
▶ 1 etanribergenov      2023-04-06 21:49    18/728    "test1          "
  2 etanribergenov@clien 2023-04-07 13:46    21/924    "LMTP test      "
q
Held 2 messages in /home/etanribergenov/Maildir
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 40. Просмотр с клиента имя почты сервера

7. Запуск графических приложений через SSH (X11Forwarding)

1. На сервере в конфигурационном файле /etc/ssh/sshd_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11

X11Forwarding yes



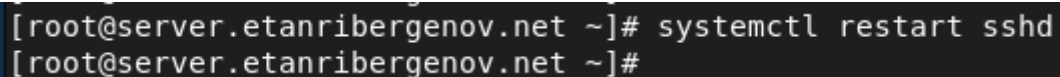
```
sshd_config [-M--] 23 L:[ 91+1
# PAM authentication via KbdInteracti
# the setting of "PermitRootLogin wit
# If you just want the PAM account an
# PAM authentication, then enable thi
# and KbdInteractiveAuthentication to
# WARNING: 'UsePAM no' is not support
# problems.
#UsePAM no

X11Forwarding yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
```

Рис. 41. Разрешение отображать на локальном клиентском узле графические интерфейсы X11

2. После сохранения изменения в конфигурационном файле перезапустите sshd



```
[root@server.etanribergenov.net ~]# systemctl restart sshd
[root@server.etanribergenov.net ~]#
```

Рис. 42. Перезапуск sshd

3. Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например, firefox

`ssh -YC etanribergenov@server.etanribergenov.net firefox`

```
[etanribergenov@client.etanribergenov.net ~]$ ssh -YC etanribergenov@server.etanribergenov.net firefox
```

Рис. 43. Удалённый запуск браузера сервера на клиенте: команда

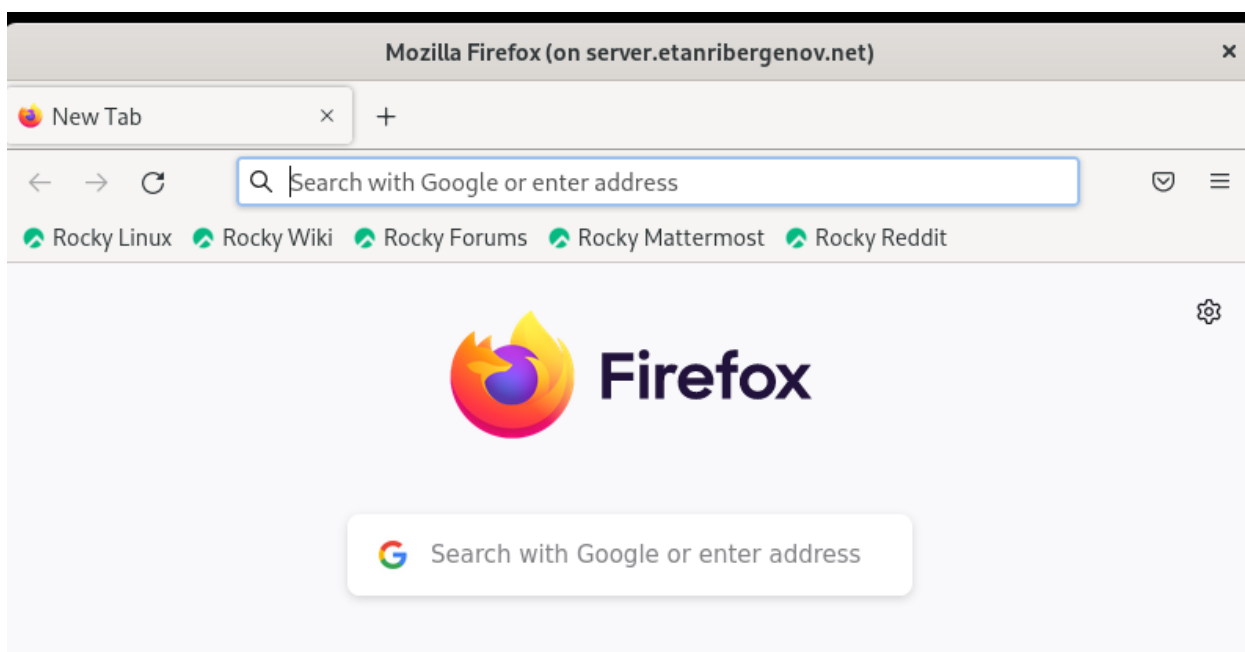


Рис. 44. Удалённый запуск браузера сервера на клиенте: результат

8. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `ssh`, в который поместите в соответствующие подкаталоги конфигурационный файл `sshd_config`

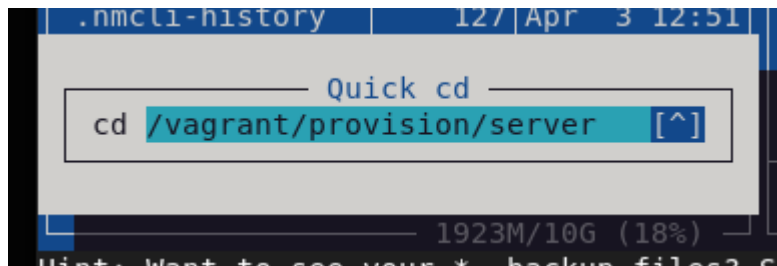


Рис. 45. Переход в каталог для внесения изменений в настройки сервера

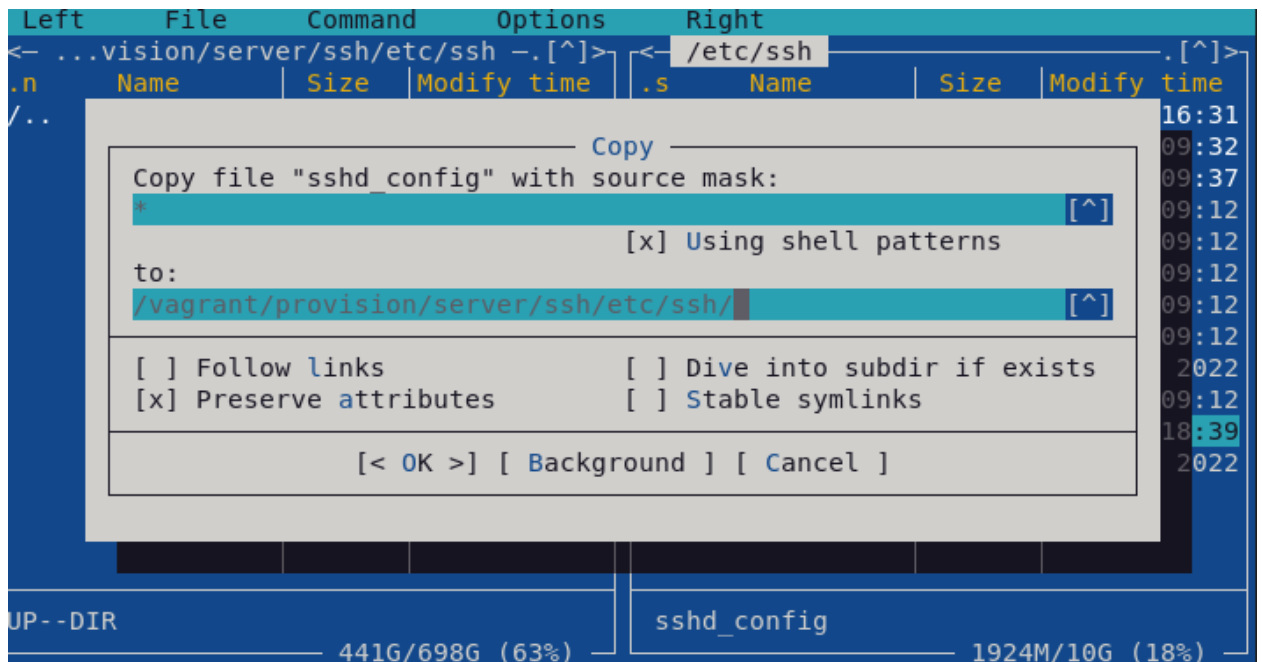


Рис. 46. Копирование конф. файла sshd

2. В каталоге /vagrant/provision/server создайте исполняемый файл ssh.sh, в котором пропишите скрипт, повторяющий произведённые в лаб. работе действия.

```
ssh.sh [----] 0 L:[ 1+12 13/ 18]
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc

restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent

echo "Tuning SELinux"
semanage port -a -t ssh_port_t -p tcp 2022

echo "Restart sshd service"
systemctl restart sshd
```

Рис. 47. Скрипт, повторяющий действия лабораторной работы

3. Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile необходимо добавить в конфигурации сервера запись.

```
Vagrantfile [----] 27 L:[ 62+10 72/
    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"
```

Рис. 48. Запись для скрипта в конф. файле Vagrantfile

Вывод

В результате выполнения лабораторной работы я приобрёл практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Ответы на контрольные вопросы

1. Параметру AllowUsers задать значение alice
2. В конф. файле параметру Port задать значение 22 и 2022. Для гарантии возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации
3. Параметры fNL
4. Команда `ssh -fNL 5555:localhost:80 server2.example.com`
5. Команда `semanage port -a -t ssh_port_t -p tcp 2022`
6. Команда `firewall-cmd --add-port=2022/tcp`