

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 11

Настройка безопасного удалённого доступа по протоколу SSH

дисциплина: Администрирование Сетевых Подсистем

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

МОСКВА

2022 г.

Цель работы:

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

Выполнение работы:

1. Запрет удалённого доступа по SSH для пользователя root

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

```
sudo -i  
passwd root
```

```
[kreachna@server.kreachna.net ~]$ sudo -i  
[sudo] password for kreachna:  
[root@server.kreachna.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.
```

2. На сервере в дополнительном терминале запустите мониторинг системных событий:

```
sudo -i  
journalctl -x -f
```

```
[kreachna@server.kreachna.net ~]$ sudo -i  
[sudo] password for kreachna:  
[root@server.kreachna.net ~]# journalctl -x -f
```

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

```
ssh root@server.kreachna.net
```

```
[kreachna@client.kreachna.net ~]$ ssh root@server.kreachna.net  
The authenticity of host 'server.kreachna.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSayzizIaAix/x7vXlm2m4.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [server.kreachna.net]:2022  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.kreachna.net' (ED25519) to the list of known hosts.  
root@server.kreachna.net's password:  
Permission denied, please try again.  
root@server.kreachna.net's password:  
Permission denied, please try again.  
root@server.kreachna.net's password:  
root@server.kreachna.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

4. На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root, установив:

```
PermitRootLogin no
```

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

5. После сохранения изменений в файле конфигурации перезапустите sshd:

```
systemctl restart sshd
```

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

6. Повторите попытку получения доступа с клиента к серверу посредством SSH соединения через пользователя root:

```
ssh root@server
```

```
[kreachna@client.kreachna.net ~]$ ssh root@server
The authenticity of host 'server (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSayzizIaAix/x7vXlm2m4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.kreachna.net]:2022
  ~/.ssh/known_hosts:4: server.kreachna.net
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server' (ED25519) to the list of known hosts.
root@server's password:
Permission denied, please try again.
root@server's password:
Permission denied, please try again.
root@server's password:
root@server: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

2. Ограничение списка пользователей для удалённого доступа по SSH

1. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя kreachna:

```
ssh kreachna@server.kreachna.net
```

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

Last login: Fri Dec 16 12:50:27 2022
```

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

```
AllowUsers vagrant
```

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

3. После сохранения изменений в файле конфигурации перезапустите sshd:

```
systemctl restart sshd
```

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

4. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user:

```
ssh kreachna@server.kreachna.net
```

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

5. В файле /etc/ssh/sshd_config конфигурации sshd внесите следующее изменение:

```
AllowUsers vagrant user
```

```
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs server
AllowUsers vagrant kreachna
```

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

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

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

Last failed login: Fri Dec 16 13:13:02 UTC 2022 from 192.168.1.1 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Fri Dec 16 13:04:01 2022 from 192.168.1.30
```

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
```

```
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
```

2. После сохранения изменений в файле конфигурации перезапустите sshd:

```
systemctl restart sshd
```

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

3. Посмотрите расширенный статус работы sshd:

```
systemctl status -l sshd
```

```
[root@server.kreachna.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 Fri 2022-12-16 13:18:14 UTC; 16s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 7231 (sshd)
    Tasks: 1 (limit: 5748)
   Memory: 1.7M
      CPU: 12ms
   CGroup: /system.slice/ssh.service
           └─7231 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 16 13:18:14 server.kreachna.net systemd[1]: Starting OpenSSH server daemon...
Dec 16 13:18:14 server.kreachna.net sshd[7231]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Dec 16 13:18:14 server.kreachna.net sshd[7231]: error: Bind to port 2022 on :: failed: Permission denied.
Dec 16 13:18:14 server.kreachna.net sshd[7231]: Server listening on 0.0.0.0 port 22.
Dec 16 13:18:14 server.kreachna.net sshd[7231]: Server listening on :: port 22.
Dec 16 13:18:14 server.kreachna.net systemd[1]: Started OpenSSH server daemon.

The job identifier is 3001.
Dec 16 13:18:24 server.kreachna.net setroubleshoot[7232]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux messages run: sealert -l 33a68f0d-0660-40e9-89ec-ff92473d9385
Dec 16 13:18:24 server.kreachna.net setroubleshoot[7232]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.

***** Plugin bind_ports (92.2 confidence) suggests *****

If you want to allow /usr/sbin/sshd to bind to network port 2022

Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 2022
   where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.

***** Plugin catchall_boolean (7.83 confidence) suggests *****

If you want to allow nis to enabled
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.

Do
setsebool -P nis_enabled 1
```

4. Исправьте на сервере метки SELinux к порту 2022:

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

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

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

```
[root@server.kreachna.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-12-16 13:21:20 UTC; 20s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 7292 (sshd)
    Tasks: 1 (limit: 5748)
   Memory: 1.7M
      CPU: 15ms
   CGroup: /system.slice/sshd.service
           └─7292 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 16 13:21:19 server.kreachna.net systemd[1]: Starting OpenSSH server daemon...
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on 0.0.0.0 port 2022.
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on :: port 2022.
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on 0.0.0.0 port 22.
Dec 16 13:21:20 server.kreachna.net sshd[7292]: Server listening on :: port 22.
Dec 16 13:21:20 server.kreachna.net systemd[1]: Started OpenSSH server daemon.
```

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

ssh [kreachna@server.kreachna.net](ssh:kreachna@server.kreachna.net)

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

Last login: Fri Dec 16 13:15:19 2022 from 192.168.1.1
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
```

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

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

ssh -p2022 [user@server.user.net](ssh:user@server.user.net)

```
[root@server.kreachna.net ~]# ssh -p2022 kreachna@server.kreachna.net
The authenticity of host '[server.kreachna.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSAYzizIaAix/x7vXlm2m4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.kreachna.net]:2022' (ED25519) to the list of known hosts.
kreachna@server.kreachna.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Dec 16 13:23:37 2022 from 192.168.1.1
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
```

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

4. Настройка удалённого доступа по SSH по ключу

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

PubkeyAuthentication yes

```
#MaxSessions 10

#PubkeyAuthentication yes
PubkeyAuthentication yes
```

2. После сохранения изменений в файле конфигурации перезапустите sshd.

3. На клиенте сформируйте SSH-ключ, введя в терминале под пользователем kreachna:

`ssh-keygen`

```
[kreachna@client.kreachna.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kreachna/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kreachna/.ssh/id_rsa
Your public key has been saved in /home/kreachna/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:AX8Q6cDj+GsCZeJKsU/0CMsoXHYTuILZPVqHuJnNpvI kreachna@client.kreachna.net
The key's randomart image is:
+---[RSA 3072]-----+
|    . . . oo      |
|    . . +o..     |
|.o o .+.+.o .    |
|o++=0oo .o       |
|+.X%++. S        |
|o*Bo+..          |
|o.o+ .           |
|o ... o          |
| oE o            |
+-----[SHA256]-----+
```

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

```
[kreachna@client.kreachna.net ~]$ cd /home/kreachna/.ssh/
[kreachna@client.kreachna.net .ssh]$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

5. Скопируйте открытый ключ на сервер, введя на клиенте:

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

```
[kreachna@client.kreachna.net ~]$ ssh-copy-id kreachna@server.kreachna.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
kreachna@server.kreachna.net's password:
\
Number of key(s) added: 1

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

6. Попробуйте получить доступ с клиента к серверу посредством SSH-соединения:

`ssh kreachna@server.kreachna.net`

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

Last login: Fri Dec 16 13:25:01 2022 from 192.168.1.1
```

5. Организация туннелей SSH, перенаправление TCP-портов

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

`lsof | grep TCP`

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

2. Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине:

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

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

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

lsof | grep TCP

```
[kreachna@client.kreachna.net ~]$ lsof | grep TCP
ssh                kreachna    3u      IPv4        48582      0t0      TCP client.kreachna.
net:32966->server.kreachna.net:ssh (ESTABLISHED)
ssh                kreachna    4u      IPv6        48602      0t0      TCP localhost:webcac
he (LISTEN)
ssh                kreachna    5u      IPv4        48603      0t0      TCP localhost:webcac
he (LISTEN)
```

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

6. Запуск консольных приложений через SSH

1. На клиенте откройте терминал под пользователем user (вместо user используйте ваш логин).
2. Посмотрите с клиента имя узла сервера:

ssh kreachna@server.kreachna.net hostname

```
[kreachna@client.kreachna.net ~]$ ssh kreachna@server.kreachna.net hostname
server.kreachna.net
```

3. Посмотрите с клиента список файлов на сервере:

ssh kreachna@server.kreachna.net ls -Al

```
[kreachna@client.kreachna.net ~]$ ssh kreachna@server.kreachna.net ls -Al
total 48
-rw-----. 1 kreachna kreachna 310 Dec 16 13:35 .bash_history
-rw-r--r--. 1 kreachna kreachna 18 May 16 2022 .bash_logout
-rw-r--r--. 1 kreachna kreachna 141 May 16 2022 .bash_profile
-rw-r--r--. 1 kreachna kreachna 519 Nov 12 16:46 .bashrc
drwxr-xr-x. 9 kreachna kreachna 4096 Nov 12 16:47 .cache
drwx-----. 9 kreachna kreachna 4096 Dec 2 10:30 .config
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Desktop
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Documents
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Downloads
drwx-----. 4 kreachna kreachna 32 Nov 12 16:46 .local
drwx-----. 5 kreachna kreachna 4096 Dec 10 13:53 Maildir
drwxr-xr-x. 4 kreachna kreachna 39 Nov 12 13:19 .mozilla
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Music
drwxr-xr-x. 2 kreachna kreachna 4096 Nov 26 13:16 Pictures
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Public
drwx-----. 2 kreachna kreachna 71 Dec 16 13:42 .ssh
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Templates
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-clipboard.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-display-svgx-x11.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-draganddrop.pid
-rw-r-----. 1 kreachna kreachna 5 Dec 16 12:50 .vboxclient-seamless.pid
drwxr-xr-x. 2 kreachna kreachna 6 Nov 12 16:46 Videos
-rw-----. 1 kreachna kreachna 0 Dec 16 12:50 .xsession-errors
-rw-----. 1 kreachna kreachna 0 Dec 10 12:17 .xsession-errors.old
```

4. Посмотрите с клиента почту на сервере:

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

```
[kreachna@client.kreachna.net ~]$ ssh kreachna@server.kreachna.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/kreachna/Maildir: 3 messages
• 1 kreachna 2022-12-09 11:34 18/646 "example1"
  2 kreachna@client.krea 2022-12-10 12:34 21/814 "LMTP test"
  3 kreachna 2022-12-10 13:52 22/832 "Checking the correcti"
```


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`

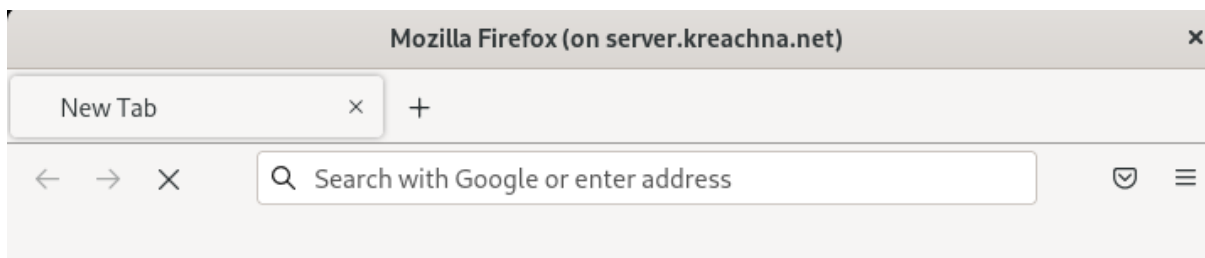
```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
```

2. После сохранения изменения в конфигурационном файле перезапустите `sshd`.

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

3. Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например `firefox` (вместо `user` используйте ваш логин):

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



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`:

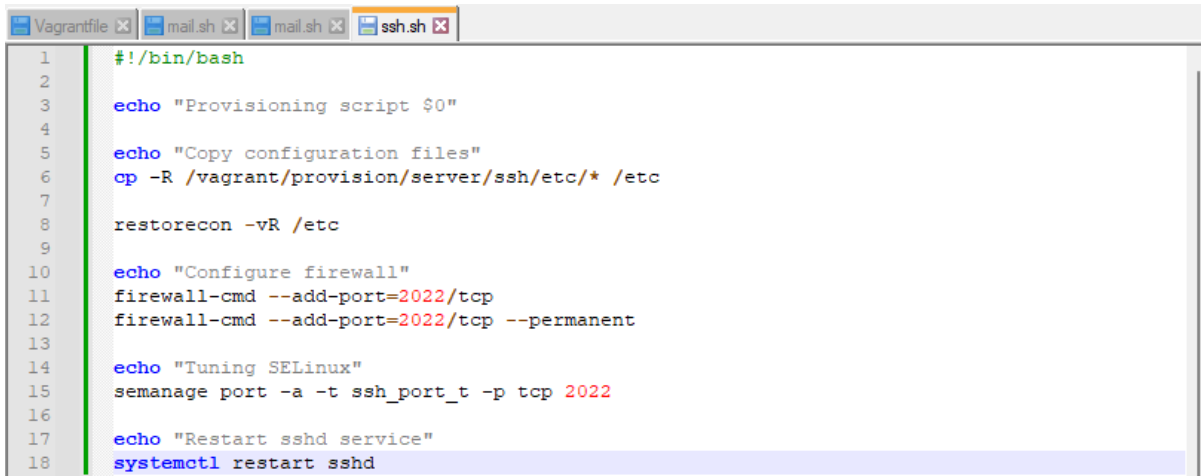
```
[root@server.kreachna.net ~]# cd /vagrant/provision/server
[root@server.kreachna.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.kreachna.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
```

2. В каталоге `/vagrant/provision/server` создайте исполняемый файл `ssh.sh`:

```
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

```
[root@server.kreachna.net server]# cd /vagrant/provision/server
[root@server.kreachna.net server]# touch ssh.sh
[root@server.kreachna.net server]# chmod +x ssh.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт:



```
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/ssh/etc/* /etc
7
8  restorecon -vR /etc
9
10 echo "Configure firewall"
11 firewall-cmd --add-port=2022/tcp
12 firewall-cmd --add-port=2022/tcp --permanent
13
14 echo "Tuning SELinux"
15 semanage port -a -t ssh_port_t -p tcp 2022
16
17 echo "Restart sshd service"
18 systemctl restart sshd
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

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

Ответ на контрольные вопросы:

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?
`/etc/ssh/sshd_config: PermitRootlogin no`
`/etc/ssh/sshd_config: AllowUsers alice`
2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?
Добавить новый порт в в файле конфигурации, исправить метки безопасности и открыть порт в настройках межсетевого экрана. Организация через разные порты дает гарантию возможности открыть сеансы ssh даже при ошибке конфигурации.
3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

fN

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

```
ssh -fNL 5555:localhost:80 server2.example.com
```

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

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

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

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

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

Вывод:

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