

Лабораторная работа №11

Настройка безопасного удалённого доступа по протоколу SSH

Демидова Е. А.

4 декабря 2023

Российский университет дружбы народов, Москва, Россия

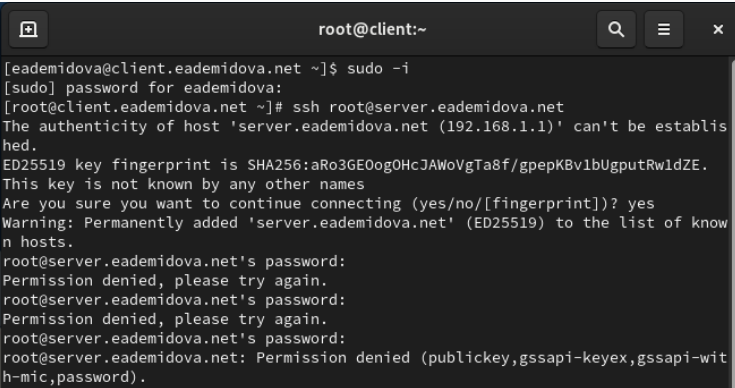
Вводная часть

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

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 и запустите графическое приложение на сервере.
7. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server.

Выполнение лабораторной работы

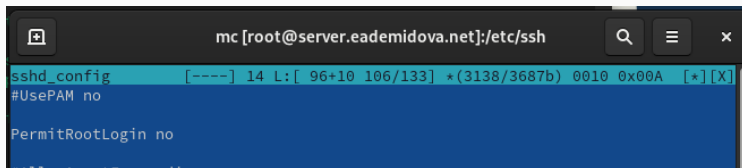
Запрет удалённого доступа по SSH для пользователя root



```
root@client:~  
[eademidova@client.eademidova.net ~]$ sudo -i  
[sudo] password for eademidova:  
[root@client.eademidova.net ~]# ssh root@server.eademidova.net  
The authenticity of host 'server.eademidova.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:aRo3GE0og0HcJAWoVgTa8f/gpepKBv1bUgputRw1dZE.  
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.eademidova.net' (ED25519) to the list of known hosts.  
root@server.eademidova.net's password:  
Permission denied, please try again.  
root@server.eademidova.net's password:  
Permission denied, please try again.  
root@server.eademidova.net's password:  
root@server.eademidova.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

Рис. 1: Попытка установить SSH-соединение

Запрет удалённого доступа по SSH для пользователя root



```
mc [root@server.eademidova.net]:/etc/ssh
sshd_config [----] 14 L:[ 96+10 106/133] *(3138/3687b) 0010 0x00A [*][X]
#UsePAM no
PermitRootLogin no
```

Рис. 2: Запрет входа на сервер пользователю root

Запрет удалённого доступа по SSH для пользователя root

```
h-mic,password).
[root@client.eademidova.net ~]# ssh root@server.eademidova.net
root@server.eademidova.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Dec  9 08:01:33 UTC 2023 from 192.168.1.30 on ssh:notty
There were 7 failed login attempts since the last successful login.
[root@server ~]# ^C
[root@server ~]# exit
logout
Connection to server.eademidova.net closed.
[root@client.eademidova.net ~]# ssh root@server.eademidova.net
root@server.eademidova.net's password:
Permission denied, please try again.
root@server.eademidova.net's password:
Permission denied, please try again.
root@server.eademidova.net's password:
root@server.eademidova.net: Permission denied (publickey,gssapi-keyex,gssapi-wit
h-mic,password).
[root@client.eademidova.net ~]#
```

Рис. 3: Повторная попытка SSH-соединение

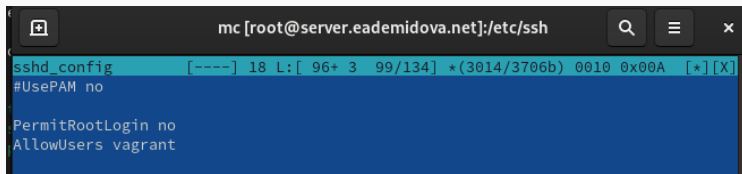
Ограничение списка пользователей для удалённого доступа по SSH

```
toget
[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net
The authenticity of host 'server.eademidova.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:aRo3GE0og0HcJAWoVgTa8f/gpepKBv1bUgputRwldZE.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.eademidova.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.eademidova.net' (ED25519) to the list of known hosts.
eademidova@server.eademidova.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec  9 08:09:41 2023 from 192.168.1.30
[eademidova@server.eademidova.net ~]$
```

Рис. 4: Попытка установить SSH-соединение с клиента

Ограничение списка пользователей для удалённого доступа по SSH

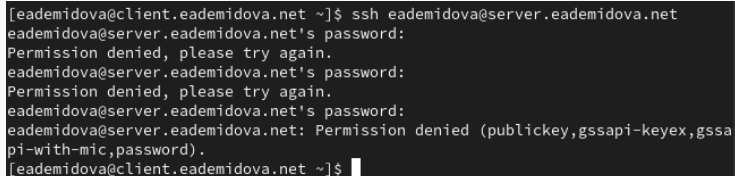


```
mc [root@server.eademidova.net]:/etc/ssh
sshd_config [-----] 18 L: [ 96+ 3 99/134] *(3014/3706b) 0010 0x00A [*] [X]
#UsePAM no

PermitRootLogin no
AllowUsers vagrant
```

Рис. 5: Изменение разрешенных пользователей для sshd

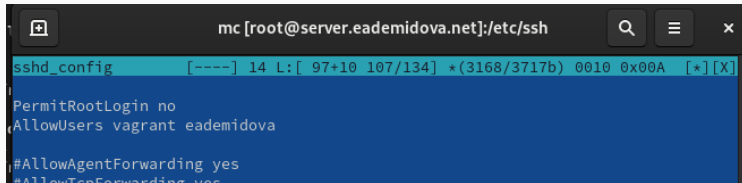
Ограничение списка пользователей для удалённого доступа по SSH

A terminal window with a dark background and light gray text. The text shows a user at a client machine attempting to SSH into a server. The first two attempts use a password and are denied. The third attempt uses a public key and is also denied. The prompt returns to the client machine.

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

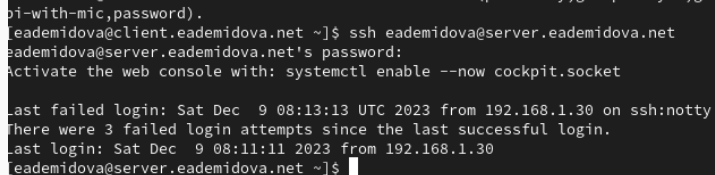
Рис. 6: Определение службы аутентификации пользователей

Ограничение списка пользователей для удалённого доступа по SSH



```
mc [root@server.eademidova.net]:/etc/ssh
sshd_config [-----] 14 L: [ 97+10 107/134] *(3168/3717b) 0010 0x00A [*] [X]
PermitRootLogin no
AllowUsers vagrant eademidova
#AllowAgentForwarding yes
#AllowTcpForwarding yes
```

Рис. 7: Изменение разрешенных пользователей для sshd

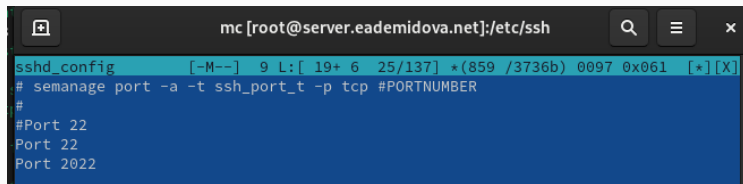


A terminal window showing an SSH session. The user 'eademidova' logs in from 'client.eademidova.net' to 'server.eademidova.net'. The terminal displays the password prompt, a message to activate the web console, and login history including failed attempts.

```
pi-with-mic,password).  
[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net  
eademidova@server.eademidova.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last failed login: Sat Dec 9 08:13:13 UTC 2023 from 192.168.1.30 on ssh:notty  
There were 3 failed login attempts since the last successful login.  
Last login: Sat Dec 9 08:11:11 2023 from 192.168.1.30  
[eademidova@server.eademidova.net ~]$
```

Рис. 8: Временный запуск SMTP-сервера

Настройка дополнительных портов для удалённого доступа по SSH



The screenshot shows a terminal window with a dark background. The title bar at the top reads "mc [root@server.eademidova.net]:/etc/ssh". The terminal content shows the configuration of the `sshd_config` file. The first line is highlighted in light blue and contains the command: `# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER`. Below this, there are three lines of configuration: `#`, `#Port 22`, `Port 22`, and `Port 2022`.

```
mc [root@server.eademidova.net]:/etc/ssh
sshd_config [-M--] 9 L:[ 19+ 6 25/137] *(859 /3736b) 0097 0x061 [*][X]
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
Port 22
Port 2022
```

Рис. 9: Добавление портов в файл конфигураций

Настройка дополнительных портов для удалённого доступа по SSH

```
Support: https://access.redhat.com/support
root@server:/etc/ssh

[root@server.eademidova.net ssh]# mc

[root@server.eademidova.net ssh]# systemctl restart sshd
[root@server.eademidova.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: ena>
   Active: active (running) since Sat 2023-12-09 08:16:56 UTC; 13s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 7726 (sshd)
     Tasks: 1 (limit: 5724)
    Memory: 1.4M
       CPU: 10ms
    CGroup: /system.slice/sshd.service
            └─7726 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 09 08:16:56 server.eademidova.net systemd[1]: Starting OpenSSH server daemon>
Dec 09 08:16:56 server.eademidova.net sshd[7726]: main: sshd: ssh-rsa algorithm>
Dec 09 08:16:56 server.eademidova.net sshd[7726]: error: Bind to port 2022 on 0>
Dec 09 08:16:56 server.eademidova.net sshd[7726]: error: Bind to port 2022 on :>
Dec 09 08:16:56 server.eademidova.net sshd[7726]: Server listening on 0.0.0.0 p>
Dec 09 08:16:56 server.eademidova.net sshd[7726]: Server listening on :: port 2>
Dec 09 08:16:56 server.eademidova.net systemd[1]: Started OpenSSH server daemon>
lines 1-19/19 (END)
```

Рис. 10: Расширенный статус работы sshd

Настройка дополнительных портов для удалённого доступа по SSH

```
The job identifier is 3466.
Dec 09 08:16:57 server.eademidova.net systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service.
Subject: A start job for unit dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

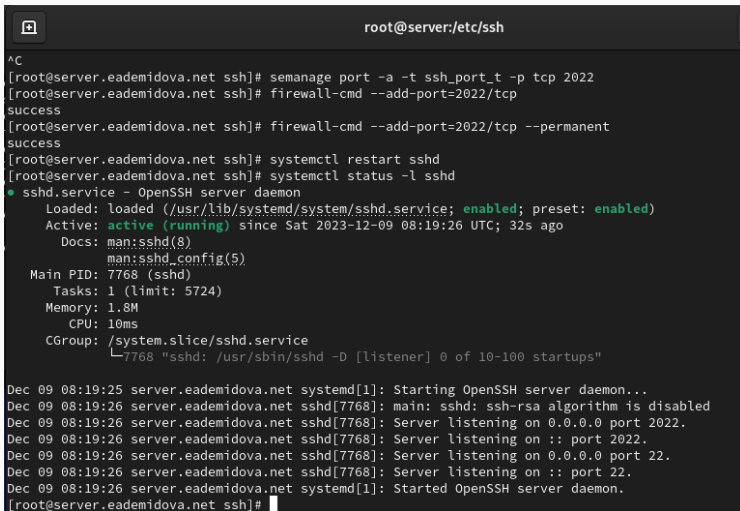
A start job for unit dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@1.service has finished successfully.

The job identifier is 3542.
Dec 09 08:16:59 server.eademidova.net setroubleshoot[7727]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux messages run: sealert -l 74c0e7ad-d686-4d3a-8d2b-7d7c3372df2c
Dec 09 08:16:59 server.eademidova.net setroubleshoot[7727]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.

***** Plugin bind_ports (92.2 configuration) suggests *****
```

Рис. 11: Мониторинг системных сообщений

Настройка дополнительных портов для удалённого доступа по SSH

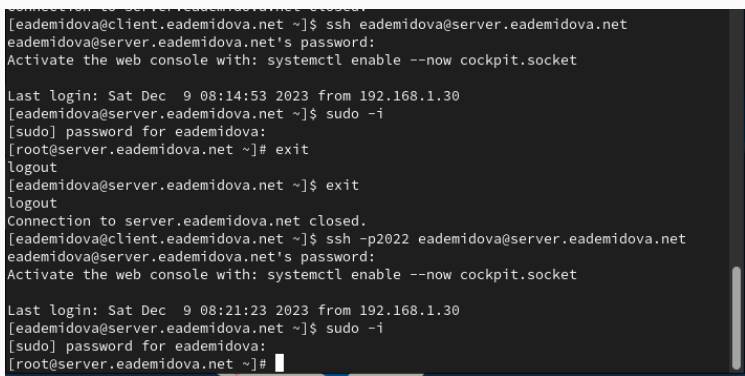
A terminal window titled 'root@server:/etc/ssh' with a '+' icon in the top-left corner. The terminal shows a series of commands and their outputs. The commands are: 'semanage port -a -t ssh_port_t -p tcp 2022', 'firewall-cmd --add-port=2022/tcp', 'firewall-cmd --add-port=2022/tcp --permanent', 'systemctl restart sshd', and 'systemctl status -l sshd'. The status output for 'sshd.service' shows it is 'loaded' and 'active (running)' since Saturday, 2023-12-09 at 08:19:26 UTC, 32 seconds ago. It also lists documentation files, main PID (7768), tasks (1), memory (1.8M), CPU (10ms), and CGroup. Below the status, there are several log messages from 'systemd[1]' and 'sshd[7768]' indicating the start of the OpenSSH server daemon and its listening ports (0.0.0.0:2022, :::2022, 0.0.0.0:22, and :::22).

```
root@server:/etc/ssh
^C
[root@server.eademidova.net ssh]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.eademidova.net ssh]# firewall-cmd --add-port=2022/tcp
success
[root@server.eademidova.net ssh]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.eademidova.net ssh]# systemctl restart sshd
[root@server.eademidova.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2023-12-09 08:19:26 UTC; 32s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 7768 (sshd)
    Tasks: 1 (limit: 5724)
   Memory: 1.8M
      CPU: 10ms
   CGroup: /system.slice/sshd.service
           └─7768 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 09 08:19:25 server.eademidova.net systemd[1]: Starting OpenSSH server daemon...
Dec 09 08:19:26 server.eademidova.net sshd[7768]: main: sshd: ssh-rsa algorithm is disabled
Dec 09 08:19:26 server.eademidova.net sshd[7768]: Server listening on 0.0.0.0 port 2022.
Dec 09 08:19:26 server.eademidova.net sshd[7768]: Server listening on :: port 2022.
Dec 09 08:19:26 server.eademidova.net sshd[7768]: Server listening on 0.0.0.0 port 22.
Dec 09 08:19:26 server.eademidova.net sshd[7768]: Server listening on :: port 22.
Dec 09 08:19:26 server.eademidova.net systemd[1]: Started OpenSSH server daemon.
[root@server.eademidova.net ssh]#
```

Рис. 12: Просмотр расширенного статуса работы sshd после настройки работы по порту 2022

Настройка дополнительных портов для удалённого доступа по SSH

A terminal window showing the process of establishing an SSH connection and configuring it. The user is on a client machine and connects to a server named 'server.eademidova.net'. The connection is successful, and the user is prompted to enter their password. After logging in, the user runs 'sudo -i' to become the root user. The root user then runs 'exit' to return to the regular user. The user then runs 'exit' again to close the SSH session. The connection is closed. The user then runs 'ssh -p2022 eademidova@server.eademidova.net' to establish a new SSH connection on port 2022. The connection is successful, and the user is prompted to enter their password. After logging in, the user runs 'sudo -i' to become the root user. The root user then runs 'exit' to return to the regular user. The user then runs 'exit' again to close the SSH session. The connection is closed.

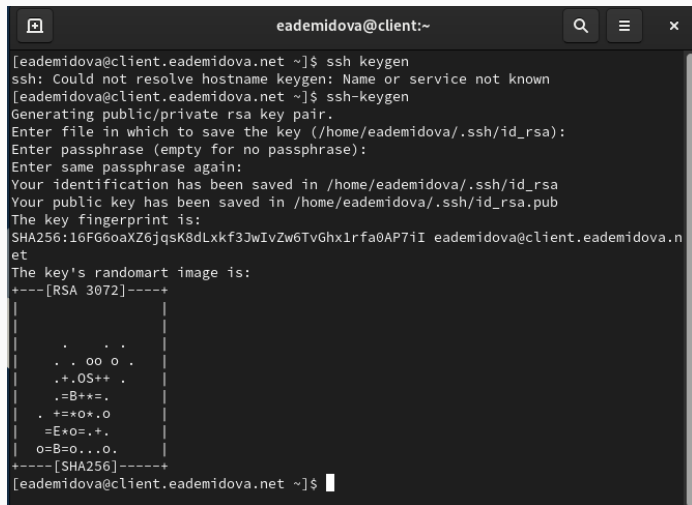
```
connection to server.eademidova.net closed.  
[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net  
eademidova@server.eademidova.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Dec  9 08:14:53 2023 from 192.168.1.30  
[eademidova@server.eademidova.net ~]$ sudo -i  
[sudo] password for eademidova:  
[root@server.eademidova.net ~]# exit  
logout  
[eademidova@server.eademidova.net ~]$ exit  
logout  
Connection to server.eademidova.net closed.  
[eademidova@client.eademidova.net ~]$ ssh -p2022 eademidova@server.eademidova.net  
eademidova@server.eademidova.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Dec  9 08:21:23 2023 from 192.168.1.30  
[eademidova@server.eademidova.net ~]$ sudo -i  
[sudo] password for eademidova:  
[root@server.eademidova.net ~]#
```

Рис. 13: Установка SSH-соединение с клиента

На сервере в конфигурационном файле `/etc/ssh/sshd_config` зададим параметр, разрешающий аутентификацию по ключу, написав:

```
PubkeyAuthentication yes
```

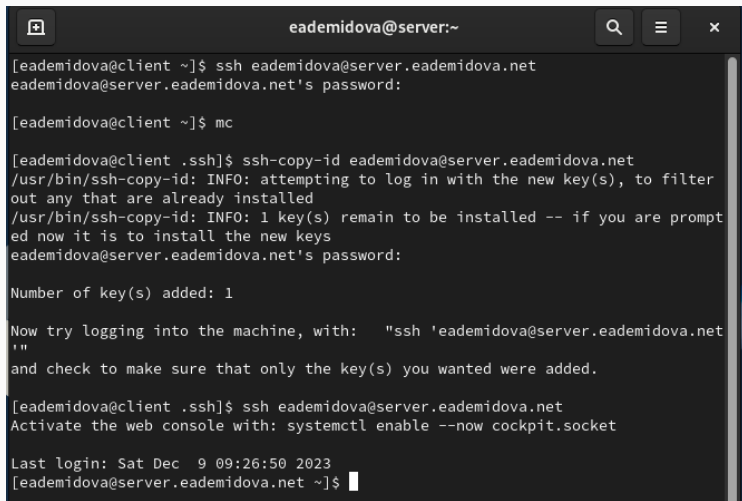
Настройка удалённого доступа по SSH по ключу

A terminal window titled 'eademidova@client:~' with standard window controls (search, menu, close). The terminal shows the execution of 'ssh keygen', which fails with a hostname error. Then 'ssh-keygen' is run successfully, prompting for a file path (defaulting to /home/eademidova/.ssh/id_rsa), a passphrase (left empty), and confirmation of the passphrase. It then displays the key's fingerprint (SHA256:16FG6oaXZ6jqsK8dLxkf3JwIvZw6TvGhx1rfa0AP7iI) and a randomart image for the RSA 3072 key. The terminal ends with the prompt '[eademidova@client.eademidova.net ~]\$' and a cursor.

```
[eademidova@client.eademidova.net ~]$ ssh keygen
ssh: Could not resolve hostname keygen: Name or service not known
[eademidova@client.eademidova.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/eademidova/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/eademidova/.ssh/id_rsa
Your public key has been saved in /home/eademidova/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:16FG6oaXZ6jqsK8dLxkf3JwIvZw6TvGhx1rfa0AP7iI eademidova@client.eademidova.net
The key's randomart image is:
+---[RSA 3072]-----+
|
|  .      .
| . . oo o .
| .+.OS++ .
| . =B+*=.
| . +=*o*.o
| =E*o=.+.
| o=B=o...o.
|
+----[SHA256]-----+
[eademidova@client.eademidova.net ~]$
```

Рис. 14: Формирования SSH-ключа на клиенте

Настройка удалённого доступа по SSH по ключу



A terminal window titled 'eademidova@server:~' with search, menu, and close icons in the title bar. The terminal shows a sequence of commands and their outputs:

```
[eademidova@client ~]$ ssh eademidova@server.eademidova.net
eademidova@server.eademidova.net's password:

[eademidova@client ~]$ mc

[eademidova@client .ssh]$ ssh-copy-id eademidova@server.eademidova.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
eademidova@server.eademidova.net's password:

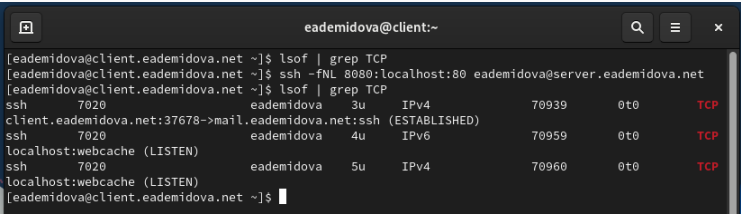
Number of key(s) added: 1

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

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

Last login: Sat Dec  9 09:26:50 2023
[eademidova@server.eademidova.net ~]$
```

Рис. 15: Установка SSH-соединения с сервером с клиента



```
eademidova@client:~  
[eademidova@client.eademidova.net ~]$ lsof | grep TCP  
[eademidova@client.eademidova.net ~]$ ssh -fNL 8080:localhost:80 eademidova@server.eademidova.net  
[eademidova@client.eademidova.net ~]$ lsof | grep TCP  
ssh          7020          eademidova    3u      IPv4          70939        0t0      TCP  
client.eademidova.net:37678->mail.eademidova.net:ssh (ESTABLISHED)  
ssh          7020          eademidova    4u      IPv6          70959        0t0      TCP  
localhost:webcache (LISTEN)  
ssh          7020          eademidova    5u      IPv4          70960        0t0      TCP  
localhost:webcache (LISTEN)  
[eademidova@client.eademidova.net ~]$
```

Рис. 16: Просмотр активных служб с протоколом TCP

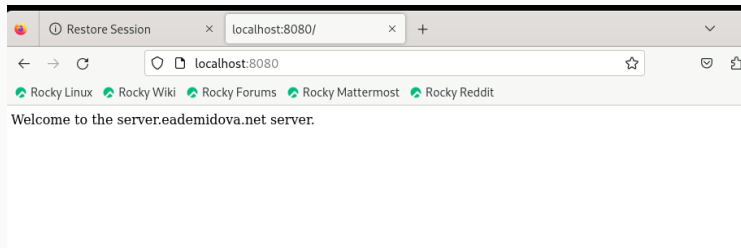
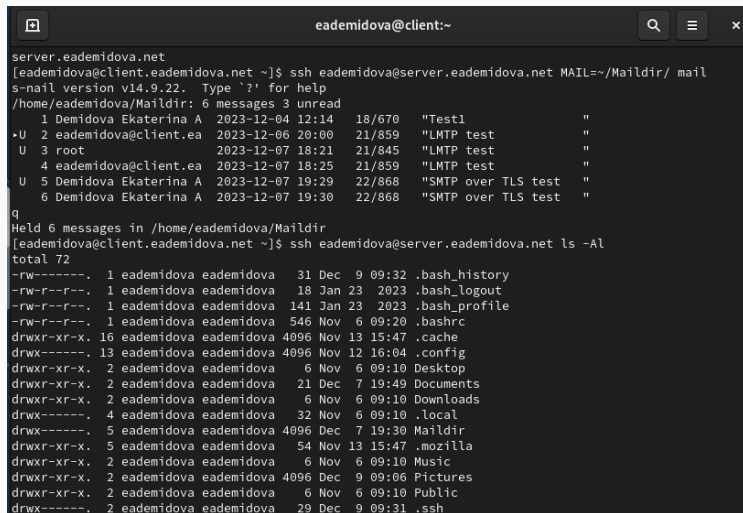


Рис. 17: Просмотр локального сервера в браузере на клиенте

Запуск консольных приложений через SSH



```
server.eademidova.net
[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22.  Type '?' for help
/home/eademidova/Maildir: 6 messages 3 unread
 1 Demidova Ekaterina A 2023-12-04 12:14 18/670 "Test1"
•U 2 eademidova@client.ea 2023-12-06 20:00 21/859 "LMTP test"
U 3 root 2023-12-07 18:21 21/845 "LMTP test"
 4 eademidova@client.ea 2023-12-07 18:25 21/859 "LMTP test"
U 5 Demidova Ekaterina A 2023-12-07 19:29 22/868 "SMTP over TLS test"
 6 Demidova Ekaterina A 2023-12-07 19:30 22/868 "SMTP over TLS test"
q
Held 6 messages in /home/eademidova/Maildir
[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net ls -Al
total 72
-rw-----, 1 eademidova eademidova 31 Dec 9 09:32 .bash_history
-rw-r--r--, 1 eademidova eademidova 18 Jan 23 2023 .bash_logout
-rw-r--r--, 1 eademidova eademidova 141 Jan 23 2023 .bash_profile
-rw-r--r--, 1 eademidova eademidova 546 Nov 6 09:20 .bashrc
drwxr-xr-x, 16 eademidova eademidova 4096 Nov 13 15:47 .cache
drwx-----, 13 eademidova eademidova 4096 Nov 12 16:04 .config
drwxr-xr-x, 2 eademidova eademidova 6 Nov 6 09:10 Desktop
drwxr-xr-x, 2 eademidova eademidova 21 Dec 7 19:49 Documents
drwxr-xr-x, 2 eademidova eademidova 6 Nov 6 09:10 Downloads
drwx-----, 4 eademidova eademidova 32 Nov 6 09:10 .local
drwx-----, 5 eademidova eademidova 4096 Dec 7 19:30 Maildir
drwxr-xr-x, 5 eademidova eademidova 54 Nov 13 15:47 .mozilla
drwxr-xr-x, 2 eademidova eademidova 6 Nov 6 09:10 Music
drwxr-xr-x, 2 eademidova eademidova 4096 Dec 9 09:06 Pictures
drwxr-xr-x, 2 eademidova eademidova 6 Nov 6 09:10 Public
drwx-----, 2 eademidova eademidova 29 Dec 9 09:31 .ssh
```

Рис. 18: Просмотр информации о сервере с клиента через ssh

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

```
X11Forwarding yes
```

Запуск графических приложений через SSH (X11Forwarding)

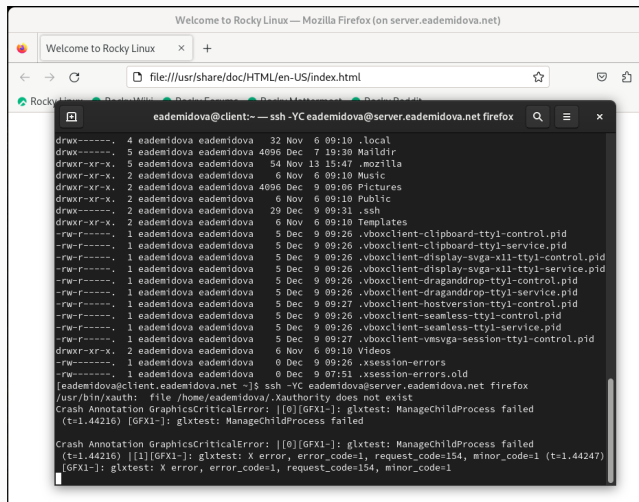
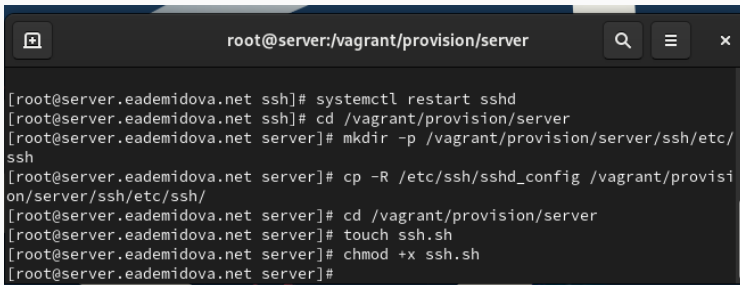


Рис. 19: Запуск графического приложения через ssh

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
root@server:/vagrant/provision/server

[root@server.eademidova.net ssh]# systemctl restart sshd
[root@server.eademidova.net ssh]# cd /vagrant/provision/server
[root@server.eademidova.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.eademidova.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.eademidova.net server]# cd /vagrant/provision/server
[root@server.eademidova.net server]# touch ssh.sh
[root@server.eademidova.net server]# chmod +x ssh.sh
[root@server.eademidova.net server]#
```

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

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
mc [root@server.eademidova.net]:/vagrant/provision/server
ssh.sh [-----] 22 L:[ 1+15 16/ 16] *(364 / 364b) <EOF> [*][X]
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc

restorecon -vR /etc

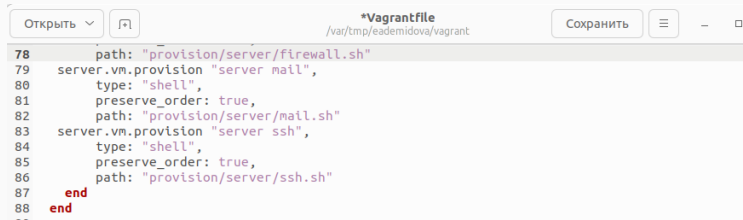
echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent

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

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

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

Внесение изменений в настройки внутреннего окружения виртуальной машины



The image shows a code editor window titled '*Vagrantfile' with the path '/var/tmp/eademidova/vagrant'. The editor contains a Vagrantfile configuration snippet. Line 78 is highlighted, showing 'path: "provision/server/firewall.sh"'. The configuration includes two 'server.vm.provision' blocks, one for 'server mail' and one for 'server ssh', both using shell scripts and preserving order. The 'server ssh' block is currently being edited, with 'end' being typed on line 87.

```
78     path: "provision/server/firewall.sh"
79   server.vm.provision "server mail",
80     type: "shell",
81     preserve_order: true,
82     path: "provision/server/mail.sh"
83   server.vm.provision "server ssh",
84     type: "shell",
85     preserve_order: true,
86     path: "provision/server/ssh.sh"
87   end
88 end
```

Рис. 22: Изменение конфигурационного файла Vagrant

Заключение

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