

Лабораторная работа №11

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Российский университет дружбы народов, Москва, Россия

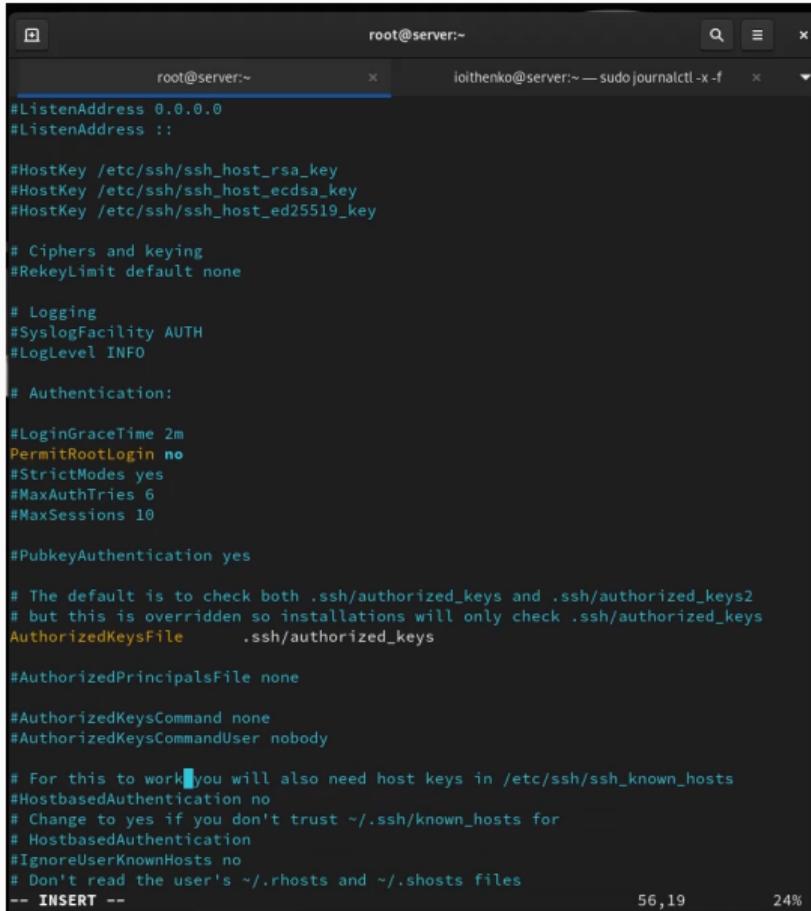
Цель работы

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

Выполнение лабораторной работы

```
[ioithenko@client.ioithenko.net ~]$ ssh root@server.ioithenko.net
The authenticity of host 'server.ioithenko.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:Thye46E17svni0fMP0tToWzEFseVN0KvqNQRg3jfWCY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [server.ioithenko.net]:22
    ~/.ssh/known_hosts:4: server
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.ioithenko.net' (ED25519) to the list of known hosts.
root@server.ioithenko.net's password:
Permission denied, please try again.
root@server.ioithenko.net's password:
Permission denied, please try again.
root@server.ioithenko.net's password:
root@server.ioithenko.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

Рис. 1: Попытка установить SSH-соединение



```
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work, you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
-- INSERT --
```

Рис. 2: Запрет входа на сервер пользователю root

```
[ioithenko@client.ioithenko.net ~]$ ssh root@server
The authenticity of host 'server (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:Thye46E17svni0fMP0tToWzEFseVN0KvqNQRg3jfWCY.
This host key is known by the following other names/addresses:
    ~/ssh/known_hosts:1: [server.ioithenko.net]:22
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
).
```

Рис. 3: Повторная попытка SSH-соединение

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

Last login: Thu Nov 14 18:54:41 2024
[ioithenko@server.ioithenko.net ~]$ █
```

Рис. 4: Попытка установить SSH-соединение с клиента

```
Nov 14 19:20:52 server.ioithenko.net sshd[7151]: pam_unix(sshd:session): session opened for user ioithenko(uid=1001) by ioithenko(uid=0)
Nov 14 19:20:52 server.ioithenko.net systemd[1]: Starting Hostname Service...
Subject: A start job for unit systemd-hostnamed.service has begun execution
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

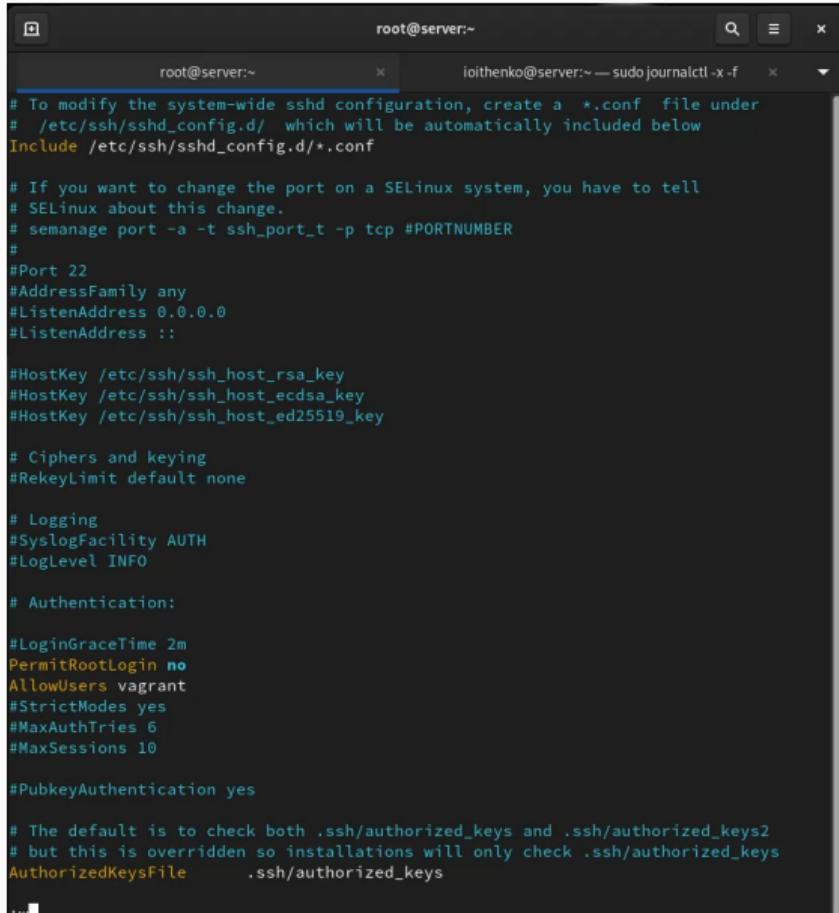
A start job for unit systemd-hostnamed.service has begun execution.

The job identifier is 2827.
Nov 14 19:20:52 server.ioithenko.net systemd[1]: Started Hostname Service.
Subject: A start job for unit systemd-hostnamed.service has finished successfully
y
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

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

The job identifier is 2827.
```

Рис. 5: Мониторинг



The screenshot shows a terminal window with two tabs. The active tab is titled 'root@server:~' and displays the configuration file for the SSH daemon (sshd). The configuration file contains various parameters such as port number, host keys, ciphers, logging, authentication methods, and user permissions. The configuration file is located at /etc/ssh/sshd_config.d/*.

```
# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
```

Рис. 6: Изменение разрешенных пользователей для sshd

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

Рис. 7: Определение службы аутентификации пользователей

The screenshot shows a terminal window with two tabs. The active tab is titled 'root@server:~' and displays the contents of the /etc/ssh/sshd_config file. The configuration file includes comments about sshd options and specifies a port of 22, host keys, ciphers, logging, authentication, and root login settings. The second tab, titled 'ioithenko@server:~ — sudo journalctl -x -f', is visible in the background. The terminal interface has a dark theme with light-colored text.

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant ioithenko
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

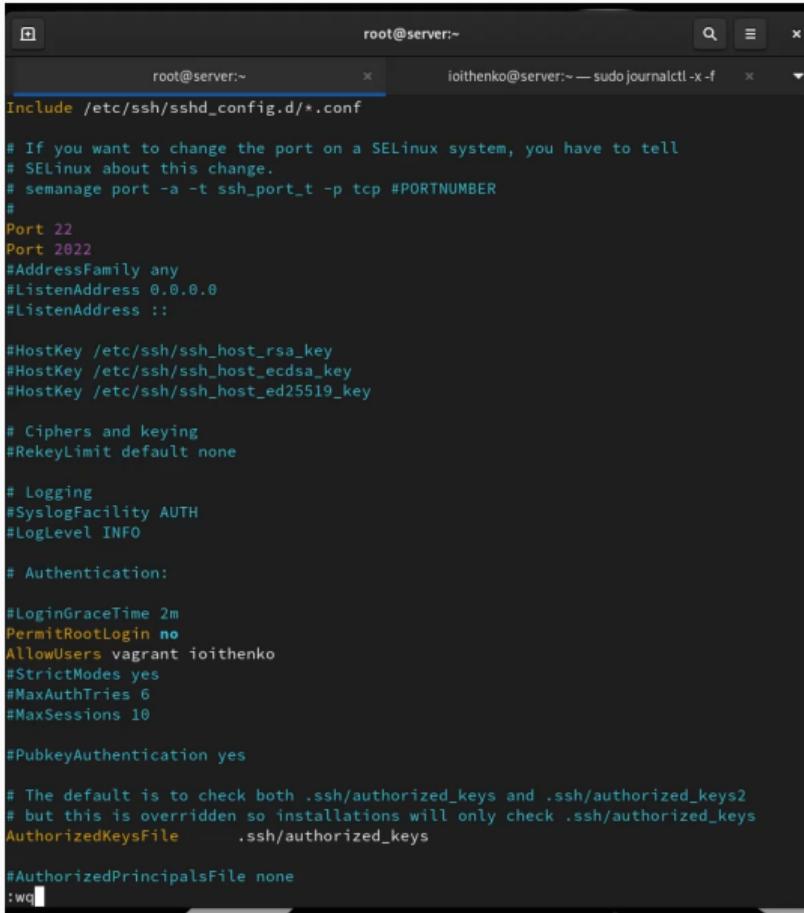
#PubkeyAuthentication yes
:|
```

Рис. 8: Изменение разрешенных пользователей для sshd

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

Last failed login: Thu Nov 14 19:23:14 UTC 2024 from 192.168.1.1 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Thu Nov 14 19:20:52 2024 from 192.168.1.30
[ioithenko@server.ioithenko.net ~]$
```

Рис. 9: Временный запуск SMTP-сервера



```
root@server:~          root@server:~          ioithenko@server:~ — sudo journalctl -x -f
Include /etc/ssh/sshd_config.d/* .conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant ioithenko
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none
:wq
```

Рис. 10: Добавление портов в файл конфигураций

```
[root@server.ioithenko.net ~]# vi /etc/ssh/sshd_config
[root@server.ioithenko.net ~]# systemctl restart sshd
[root@server.ioithenko.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
    Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
      Active: active (running) since Thu 2024-11-14 19:24:57 UTC; 19s ago
        Docs: man:sshd(8)
               man:sshd_config(5)
    Main PID: 7284 (sshd)
       Tasks: 1 (limit: 4555)
      Memory: 1.4M
         CPU: 15ms
        CGroup: /system.slice/sshd.service
                   └─7284 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 14 19:24:57 server.ioithenko.net systemd[1]: Starting OpenSSH server daemon...
Nov 14 19:24:57 server.ioithenko.net sshd[7284]: error: Bind to port 2222 on 0.0.0.0 failed: Address already in use
Nov 14 19:24:57 server.ioithenko.net sshd[7284]: error: Bind to port 2222 on :: failed: Address already in use
Nov 14 19:24:57 server.ioithenko.net sshd[7284]: Server listening on 0.0.0.0 port 22.
Nov 14 19:24:57 server.ioithenko.net sshd[7284]: Server listening on :: port 22.
Nov 14 19:24:57 server.ioithenko.net systemd[1]: Started OpenSSH server daemon.
lines 1-18/18 (END)
```

Рис. 11: Расширенный статус работы sshd

```
Nov 14 19:25:08 server.ioithenko.net setroubleshoot[7285]: SELinux is preventing /u  
sr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELin  
ux messages run: sealert -l 4ece7059-0df4-4c75-a736-ce844cc7b10f  
Nov 14 19:25:08 server.ioithenko.net setroubleshoot[7285]: SELinux is preventing /u  
sr/sbin/sshd from name_bind access on the tcp_socket port 2022.  
  
***** Plugin bind_ports  
(92.2 confidence) suggests *****  
  
If you want to allow /us  
r/sbin/sshd to bind to network port 2022  
Then you need to modify  
the port type.  
Do  
# semanage port -a -t PO  
RT_TYPE -p tcp 2022  
where PORT_TYPE is o  
ne of the following: ssh_port_t, vnc_port_t, xserver_port_t.  
  
***** Plugin catchall_b  
oolean (7.83 confidence) suggests *****  
  
If you want to allow nis  
to enabled  
Then you must tell SELin  
ux about this by enabling the 'nis_enabled' boolean.
```

Рис. 12: Мониторинг системных сообщений

```
[root@server.ioithenko.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.ioithenko.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.ioithenko.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.ioithenko.net ~]# systemctl restart sshd
[root@server.ioithenko.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
      Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
      Active: active (running) since Thu 2024-11-14 19:27:30 UTC; 9s ago
        Docs: man:sshd(8)
               man:sshd_config(5)
    Main PID: 7309 (sshd)
       Tasks: 1 (limit: 4555)
      Memory: 1.6M
         CPU: 22ms
        CGroup: /system.slice/sshd.service
                   └─7309 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 14 19:27:30 server.ioithenko.net systemd[1]: Starting OpenSSH server daemon...
Nov 14 19:27:30 server.ioithenko.net sshd[7309]: Server listening on 0.0.0.0 port >
Nov 14 19:27:30 server.ioithenko.net sshd[7309]: Server listening on :: port 2022.
Nov 14 19:27:30 server.ioithenko.net sshd[7309]: Server listening on 0.0.0.0 port >
Nov 14 19:27:30 server.ioithenko.net sshd[7309]: Server listening on :: port 22.
Nov 14 19:27:30 server.ioithenko.net systemd[1]: Started OpenSSH server daemon.
```

Рис. 13: Просмотр расширенного статуса работы sshd после настройки работы по порту 2022

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

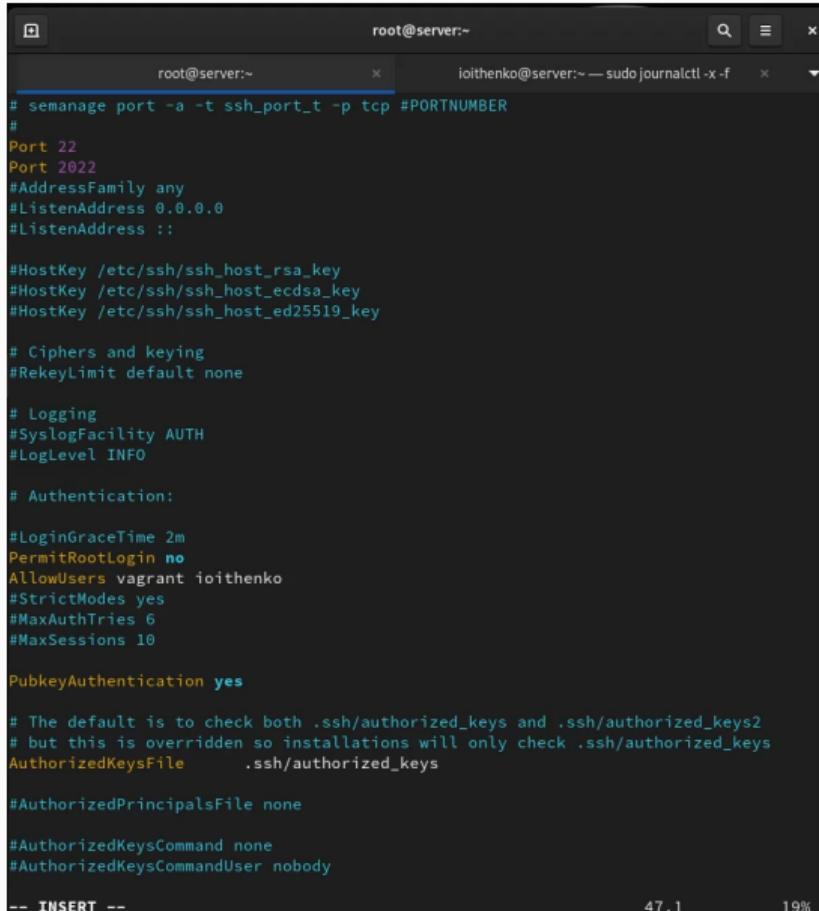
Last login: Thu Nov 14 19:24:00 2024 from 192.168.1.1
[ioithenko@server.ioithenko.net ~]$ sudo -i
[sudo] password for ioithenko:
[root@server.ioithenko.net ~]# logout
[ioithenko@server.ioithenko.net ~]$ logout
Connection to server.ioithenko.net closed.
```

Рис. 14: Установка SSH-соединение с клиента

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

Last login: Thu Nov 14 19:28:28 2024 from 192.168.1.1
[ioithenko@server.ioithenko.net ~]$ sudo -i
[sudo] password for ioithenko:
[root@server.ioithenko.net ~]# logout
[ioithenko@server.ioithenko.net ~]$ logout
Connection to server.ioithenko.net closed.
[ioithenko@client.ioithenko.net ~]$
```

Рис. 15: Установка SSH-соединение с клиентом с указанием порта 2022



The screenshot shows a terminal window with two tabs. The left tab is titled 'root@server:~' and contains the command:

```
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
```

The right tab is titled 'ioithenko@server:~ — sudo journalctl -x -f' and shows the output of a journalctl command.

The configuration file content is as follows:

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

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant ioithenko
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

-- INSERT --

Рис. 16: Установка SSH-соединение с клиента

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ioithenko/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ioithenko/.ssh/id_rsa
Your public key has been saved in /home/ioithenko/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:0FBjDbnQdlHMiwZTxExqikvHWwpG+1Gb91LfifipRqk ioithenko@client.ioithenko.net
The key's randomart image is:
----[RSA 3072]----+
| .o+=.=. o0+|
| .+++.o o .o=|
| .o.o. .+ .|
| ... + + o |
| S * * + o |
| o B.=.o=|
| +.+....+|
| E . . . |
| ...o |
----[SHA256]----+
[ioithenko@client.ioithenko.net ~]$ ssh-copy-id ioithenko@server.ioithenko.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
ioithenko@server.ioithenko.net's password:

Number of key(s) added: 1

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

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

Last login: Thu Nov 14 19:30:00 2024 from 192.168.1.30
[ioithenko@server.ioithenko.net ~]$ logout
Connection to server.ioithenko.net closed.
[ioithenko@client.ioithenko.net ~]$
```

Рис. 17: Создание и копирование открытого ключа, установка SSH-соединения с сервером с клиента

```
[ioithenko@client.ioithenko.net ~]$ lsof | grep TCP
[ioithenko@client.ioithenko.net ~]$ ssh -fNL 8080:localhost:80 ioithenko@server
.ioithenko.net
[ioithenko@client.ioithenko.net ~]$ lsof | grep TCP
ssh      10166             ioithenko  3u      IPv4          6055
2      0t0      TCP  client.ioithenko.net:38514->ns.ioithenko.net:ssh (ESTABL
ISHED)
ssh      10166             ioithenko  4u      IPv6          6057
1      0t0      TCP  localhost:webcache (LISTEN)
ssh      10166             ioithenko  5u      IPv4          6057
2      0t0      TCP  localhost:webcache (LISTEN)
[ioithenko@client.ioithenko.net ~]$
```

Рис. 18: Просмотр активных служб с протоколом TCP

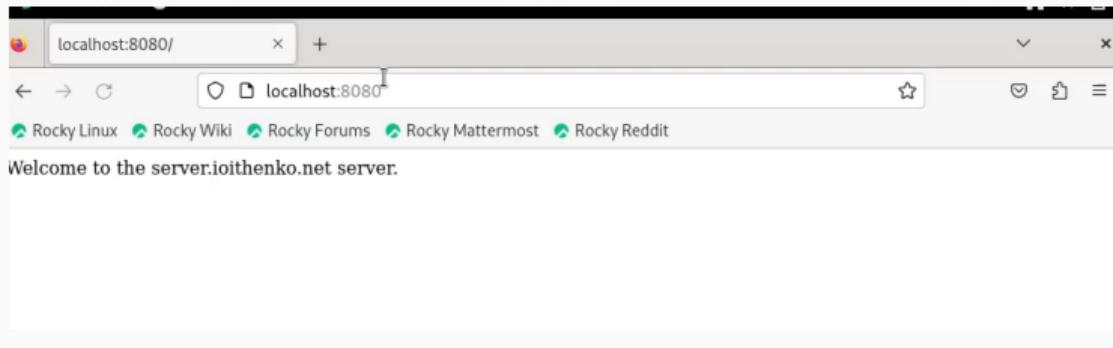


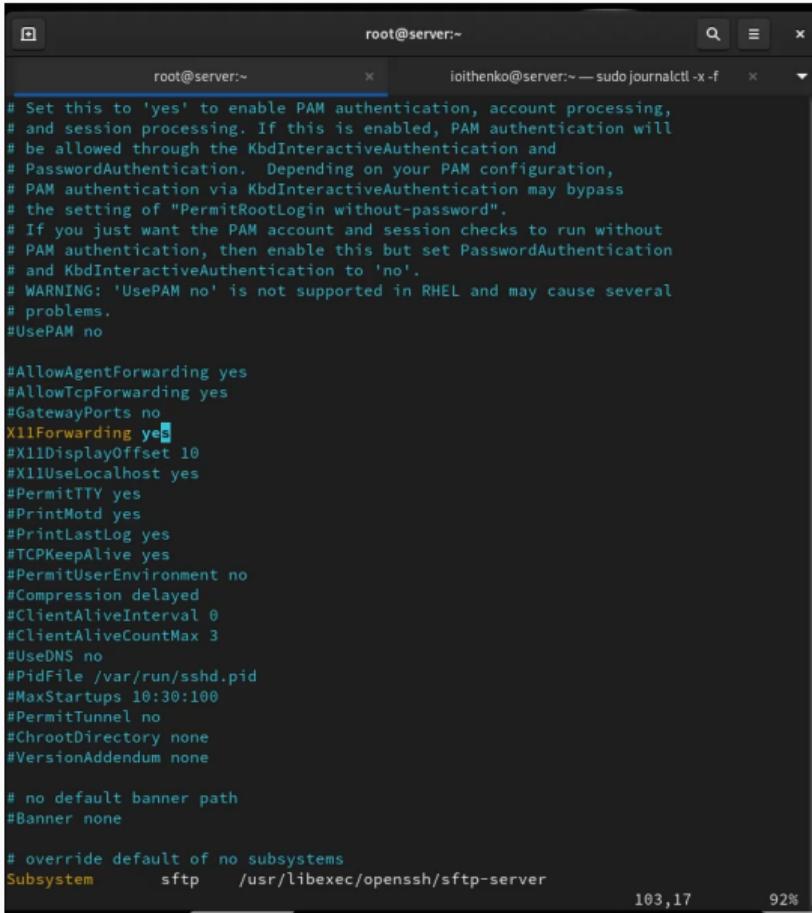
Рис. 19: Просмотр локального сервера в браузере на клиенте

```
[ioithenko@client.ioithenko.net ~]$ ssh ioithenko@server.ioithenko.net hostname
server.ioithenko.net
[ioithenko@client.ioithenko.net ~]$ ssh ioithenko@server.ioithenko.net ls -Al
total 68
-rw-----. 1 ioithenko ioithenko 1711 Nov 14 19:30 .bash_history
-rw-r--r--. 1 ioithenko ioithenko 18 Apr 30 2024 .bash_logout
-rw-r--r--. 1 ioithenko ioithenko 141 Apr 30 2024 .bash_profile
-rw-r--r--. 1 ioithenko ioithenko 519 Sep 5 17:46 .bashrc
drwx-----. 10 ioithenko ioithenko 4096 Oct 21 16:41 .cache
drwx-----. 10 ioithenko ioithenko 4096 Sep 19 16:23 .config
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Desktop
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Documents
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Downloads
drwx-----. 4 ioithenko ioithenko 32 Sep 5 18:48 .local
drwx-----. 5 ioithenko ioithenko 4096 Nov 1 19:39 Maildir
drwxr-xr-x. 4 ioithenko ioithenko 39 Sep 5 00:13 .mozilla
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Music
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Pictures
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Public
drwx-----. 2 ioithenko ioithenko 71 Nov 14 19:32 .ssh
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Templates
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-clipboard-tty1
-control.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-clipboard-tty1
-service.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-draganddrop-tt
y1-control.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-draganddrop-tt
y1-service.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-hostversion-tt
y1-control.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-seamless-tty1-
control.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-seamless-tty1-
service.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-vmsvga-session
-tty1-control.pid
-rw-r-----. 1 ioithenko ioithenko 5 Nov 14 18:54 .vboxclient-vmsvga-session
-tty1-service.pid
drwxr-xr-x. 2 ioithenko ioithenko 6 Sep 5 18:48 Videos
-rw-----. 1 ioithenko ioithenko 2153 Nov 1 16:48 .viminfo
-rw-----. 1 ioithenko ioithenko 0 Nov 14 18:54 .xsession-errors
-rw-----. 1 ioithenko ioithenko 0 Nov 1 18:32 .xsession-errors.old
[ioithenko@client.ioithenko.net ~]$
```

Рис. 20: Просмотр информации о сервере с клиента через ssh

```
[ioithenko@client.ioithenko.net ~]$ ssh ioithenko@server.ioithenko.net MAIL=~/Maildir/ mail
s-nail version v14.9.22. Type `?' for help
/home/ioithenko/Maildir: 5 messages 3 unread
  1 ioithenko      2024-10-30 15:03  18/641  "test1"
•U 2 ioithenko      2024-10-30 15:04  18/642  "test2"
  U 3 ioithenko      2024-10-30 15:11  18/642  "test1"
  U 4 ioithenko@client.ioi  2024-11-01 17:38  21/864  "LMTP test"
  5 ioithenko      2024-11-01 19:39  22/813  "TLS test"
```

Рис. 21: Просмотр почты сервера с клиента через ssh



```
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#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
```

Рис. 22: Просмотр информации о сервере с клиента через ssh

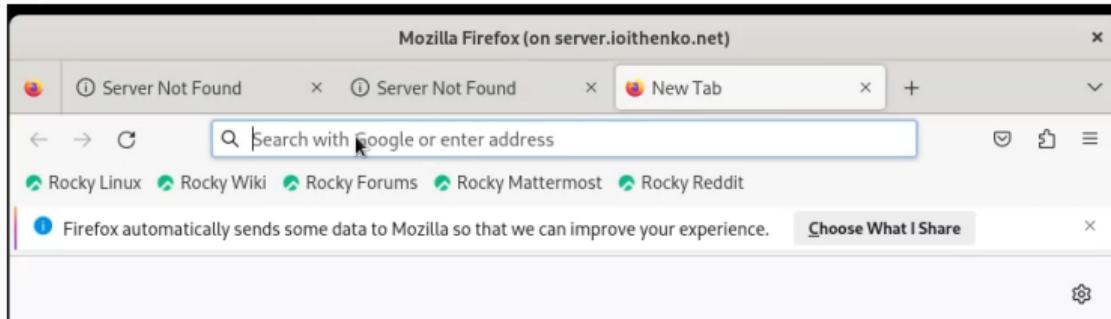


Рис. 23: Запуск графического приложения через ssh

Выводы

В ходе выполнения данной работы я приобрела практические навыки по настройке удалённого доступа к серверу с помощью SSH.