

Администрирование сетевых подсистем

Настройка безопасного удалённого доступа по SSH (Лабораторная работа №11)

Заур Мустафаев

10 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель и задачи работы

Получение практических навыков настройки безопасного удалённого доступа к серверу по SSH.

Выполнение лабораторной работы

Запрет удалённого входа root по SSH

```
[zmustafaev@client.zmustafaev.net ~]$ ssh root@server.zmustafaev.net
The authenticity of host 'server.zmustafaev.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxmw0XTU.
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.zmustafaev.net' (ED25519) to the list of known host
s.
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
Permission denied, please try again.
root@server.zmustafaev.net's password:
root@server.zmustafaev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,
password).
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 1: Попытка входа под root

Ограничение доступа по списку пользователей

```
sshd_config [----] 18 L:[ 31+16 47/133] *(1250/3678b) 0010 0x00A
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes

AllowUsers vagrant

# 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
```

Настройка дополнительного порта SSH

```
sshd_config  [-M--]  0 L:[ 5+21 26/134] *(900 /3698b) 0010 0x00A

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# 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
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
```

Подключение к серверу через новый порт

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net  
zmustafaev@server.zmustafaev.net's password:  
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Nov 10 12:05:16 2025 from 192.168.1.30  
[zmustafaev@server.zmustafaev.net ~]$ sudo -i  
[sudo] password for zmustafaev:  
[root@server.zmustafaev.net ~]#  
logout  
[zmustafaev@server.zmustafaev.net ~]$  
logout  
Connection to server.zmustafaev.net closed.  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net -p2022  
zmustafaev@server.zmustafaev.net's password:  
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Nov 10 12:09:22 2025 from 192.168.1.30  
[zmustafaev@server.zmustafaev.net ~]$ sudo -i  
[sudo] password for zmustafaev:  
[root@server.zmustafaev.net ~]#  
logout  
[zmustafaev@server.zmustafaev.net ~]$  
logout  
Connection to server.zmustafaev.net closed.  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 4: Подключение через порт 2022

Аутентификация по SSH-ключу

```
|
|      . . . o |
|      oo.+.* = .|
|      SB *.=oB |
|      o *.=oo+.|
|      *.Bo.o o|
|      @=. o*|
|      .o+o .E*|
```

```
+-----[SHA256]-----+
```

```
[zmustafaev@client.zmustafaev.net ~]$ ssh-copy-id zmustafaev@server.zmustafaev.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out an
y 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
zmustafaev@server.zmustafaev.net's password:
```

Number of key(s) added: 1

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

```
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net -p2022
Web console: https://server.zmustafaev.net:9090/ or https://192.168.1.1:9090/
```

Last login: Mon Nov 10 12:09:41 2025 from 192.168.1.30

```
[zmustafaev@server.zmustafaev.net ~]$ █
```

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ lsof | grep TCP  
[zmustafaev@client.zmustafaev.net ~]$ ssh -fNL 8080:localhost:80 zmustafaev@server.zmu  
stafaev.net  
[zmustafaev@client.zmustafaev.net ~]$ lsof | grep TCP  
ssh      15084          zmustafaev    3u    IPv4          90271  
0t0      TCP client.zmustafaev.net:57304->mail.zmustafaev.net:ssh (ESTABLISHED)  
ssh      15084          zmustafaev    4u    IPv6          90281  
0t0      TCP localhost:webcache (LISTEN)  
ssh      15084          zmustafaev    5u    IPv4          90282  
0t0      TCP localhost:webcache (LISTEN)  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 6: Создание SSH-туннеля

Запуск команд на сервере без интерактивного входа

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ ssh zmustafaev@server.zmustafaev.net MAIL=~/.Mail  
dir mail  
s-nail version v14.9.24. Type '?' for help  
/home/zmustafaev/Maildir: 3 messages 1 unread  
   1 zmustafaev          2025-10-29 15:09   18/668   "test1           "  
   2 zmustafaev@client.zm 2025-11-04 09:00   21/855   "LMTP test       "  
▶U  3 zmustafaev          2025-11-04 09:22   22/840   "test3           "  
q  
Held 3 messages in /home/zmustafaev/Maildir  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 7: Пример выполнения команд

Попытка удалённого запуска графических приложений

```
[zmustafaev@client.zmustafaev.net ~]$  
[zmustafaev@client.zmustafaev.net ~]$ ssh -YC zmustafaev@server.zmustafaev.net firefox  
Warning: No xauth data; using fake authentication data for X11 forwarding.  
X11 forwarding request failed on channel 0  
Error: no DISPLAY environment variable specified  
[zmustafaev@client.zmustafaev.net ~]$ ssh -YC zmustafaev@server.zmustafaev.net firefox  
Warning: No xauth data; using fake authentication data for X11 forwarding.  
X11 forwarding request failed on channel 0  
Error: no DISPLAY environment variable specified  
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 8: Попытка запуска графического приложения

Вывод

В ходе работы были освоены:

- настройка доступа по SSH и обеспечение безопасности;
- ограничение входа root и контроль списка пользователей;
- работа с альтернативными портами и SELinux;
- ключевая аутентификация и SSH-туннели;
- автоматизация конфигурации.

Удалённый доступ стал безопасным, гибким и удобным в эксплуатации.