

Администрирование сетевых подсистем

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

Суннатилло Махмудов

24 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Приобрести практические навыки настройки безопасного удалённого доступа к серверу с помощью SSH.

1. Запретить вход root по SSH и ограничить список пользователей.
2. Настроить работу SSH на нескольких портах с SELinux и firewalld.
3. Включить аутентификацию по ключу.
4. Настроить туннели и переадресацию портов.
5. Запускать консольные и X11-приложения по SSH.
6. Автоматизировать конфигурацию.

Теоретическая часть

- Клиент–серверный протокол защищённого удалённого доступа.
- Аутентификация: пароль, ключ, комбинированные методы.
- Шифрование трафика, целостность данных, сжатие.
- Переадресация портов: -L (локальная), -R (обратная), -D (SOCKS).

Процесс выполнения

Запрет удалённого входа root

```
[smahmudov@client.smahmudov.net ~]$ ssh root@smahmudov.net
The authenticity of host 'smahmudov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.smahmudov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'smahmudov.net' (ED25519) to the list of known hosts.
root@smahmudov.net's password:
Permission denied, please try again.
root@smahmudov.net's password:
Permission denied, please try again.
root@smahmudov.net's password:
root@smahmudov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[smahmudov@client.smahmudov.net ~]$
```

Рис. 1: Попытки входа root и изменение параметра

Запрет удалённого входа root

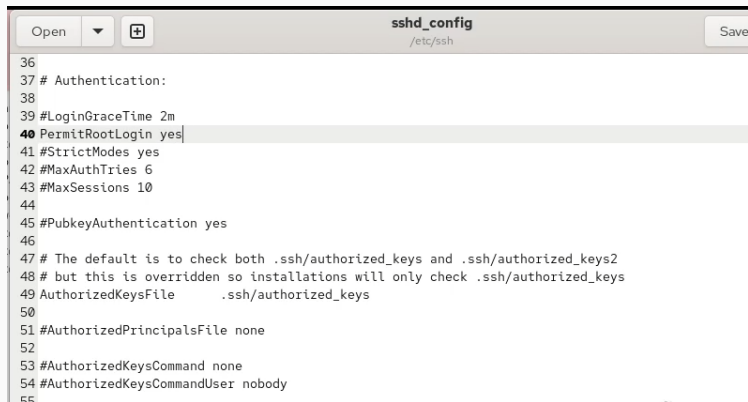


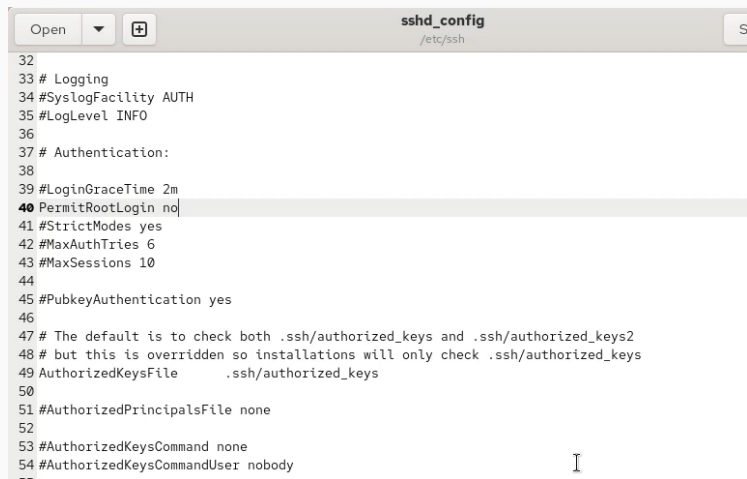
Рис. 2: Изменение параметра на yes (для проверки)

Запрет удалённого входа root

```
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ ssh root@smahmudov.net  
root@smahmudov.net's password:  
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/  
  
Last failed login: Sat Oct 18 06:39:23 UTC 2025 from 192.168.1.30 on ssh:notty  
There were 3 failed login attempts since the last successful login.  
Last login: Sat Oct 18 06:38:13 2025  
root@server:~#  
root@server:~#  
logout  
Connection to smahmudov.net closed.  
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$
```

Рис. 3: Успешный вход при временном разрешении

Запрет удалённого входа root



```
32
33 # Logging
34 #SyslogFacility AUTH
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40 PermitRootLogin no
41 #StrictModes yes
42 #MaxAuthTries 6
43 #MaxSessions 10
44
45 #PubkeyAuthentication yes
46
47 # The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
48 # but this is overridden so installations will only check .ssh/authorized_keys
49 AuthorizedKeysFile      .ssh/authorized_keys
50
51 #AuthorizedPrincipalsFile none
52
53 #AuthorizedKeysCommand none
54 #AuthorizedKeysCommandUser nobody
55
```

Рис. 4: Возврат запрета и подтверждение отказа

Запрет удалённого входа root

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

Рис. 5: Итог — отказ во входе для root

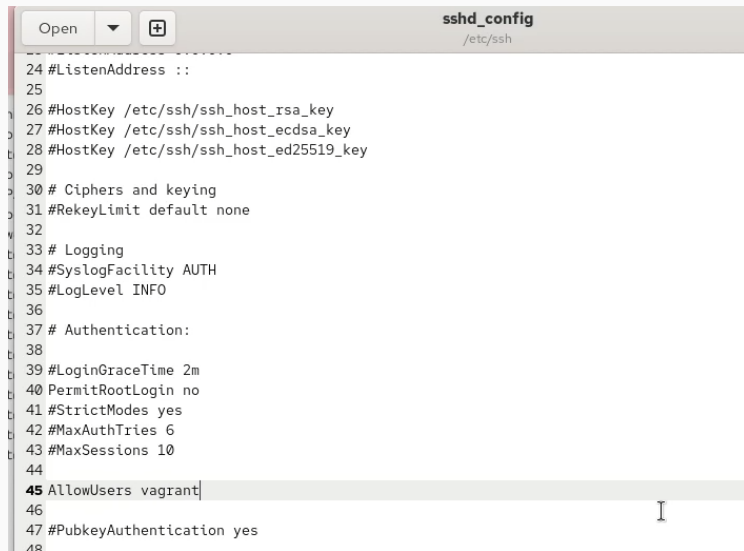
Ограничение списка пользователей (AllowUsers)

```
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net
The authenticity of host 'server.smahmudov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.smahmudov.net]:2022
  ~/.ssh/known_hosts:4: smahmudov.net
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.smahmudov.net' (ED25519) to the list of known hosts.
smahmudov@server.smahmudov.net's password:
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/

Last login: Sat Oct 18 06:36:09 2025
[smahmudov@server.smahmudov.net ~]$
```

Рис. 6: Успешный вход пользователя до ограничения

Ограничение списка пользователей (AllowUsers)



```
24 #ListenAddress ::
25
26 #HostKey /etc/ssh/ssh_host_rsa_key
27 #HostKey /etc/ssh/ssh_host_ecdsa_key
28 #HostKey /etc/ssh/ssh_host_ed25519_key
29
30 # Ciphers and keying
31 #RekeyLimit default none
32
33 # Logging
34 #SyslogFacility AUTH
35 #LogLevel INFO
36
37 # Authentication:
38
39 #LoginGraceTime 2m
40 PermitRootLogin no
41 #StrictModes yes
42 #MaxAuthTries 6
43 #MaxSessions 10
44
45 AllowUsers vagrant
46
47 #PubkeyAuthentication yes
48
```


Рис. 7. Добавление AllowUsers vagrant

Ограничение списка пользователей (AllowUsers)

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

Рис. 8: Отказ во входе для smahmudov

Ограничение списка пользователей (AllowUsers)



```
Open ▼ + sshd_config
/etc/ssh
37 # Authentication:
38
39 #LoginGraceTime 2m
40 PermitRootLogin no
41 #StrictModes yes
42 #MaxAuthTries 6
43 #MaxSessions 10
44
45 AllowUsers vagrant smahmudov
46
47 #PubkeyAuthentication yes
48
49 # The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
50 # but this is overridden so installations will only check .ssh/authorized_keys
51 AuthorizedKeysFile .ssh/authorized_keys
52
53 #AuthorizedPrincipalsFile none
54
55 #AuthorizedKeysCommand none
56 #AuthorizedKeysCommandUser nobody
57
```

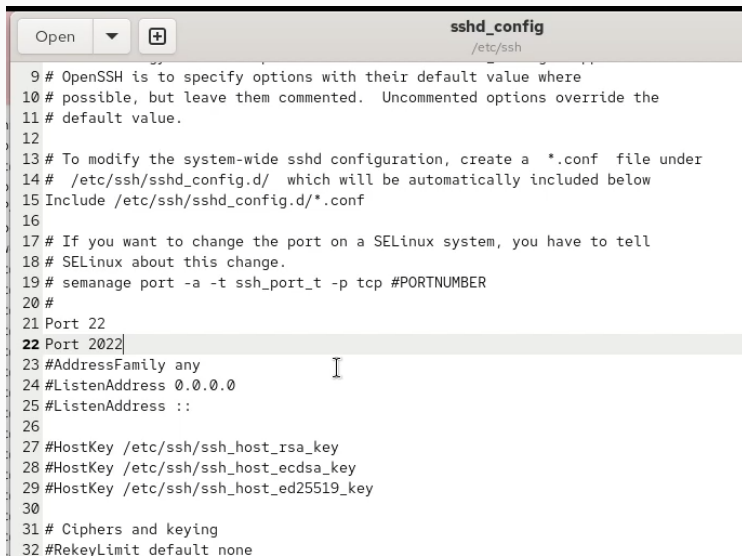
Рис. 9: Разрешение для vagrant и smahmudov

Ограничение списка пользователей (AllowUsers)

```
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net  
smahmudov@server.smahmudov.net's password:  
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/  
  
Last failed login: Sat Oct 18 06:44:18 UTC 2025 from 192.168.1.30 on ssh:notty  
There were 3 failed login attempts since the last successful login.  
Last login: Sat Oct 18 06:43:20 2025 from 192.168.1.30  
[smahmudov@server.smahmudov.net ~]$  
[smahmudov@server.smahmudov.net ~]$  
logout  
Connection to server.smahmudov.net closed.  
[smahmudov@client.smahmudov.net ~]$
```

Рис. 10: Повторный успешный вход

Параллельные порты SSH (22 и 2022)

A screenshot of a text editor window titled 'sshd_config' with the path '/etc/ssh' shown below the title. The editor contains the default SSH daemon configuration file. Line 22, 'Port 2022', is highlighted in a light gray background. A mouse cursor is positioned at the end of line 24, '#ListenAddress 0.0.0.0'.

```
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented. Uncommented options override the
11 # default value.
12
13 # To modify the system-wide sshd configuration, create a *.conf file under
14 # /etc/ssh/sshd_config.d/ which will be automatically included below
15 Include /etc/ssh/sshd_config.d/*.conf
16
17 # If you want to change the port on a SELinux system, you have to tell
18 # SELinux about this change.
19 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
20 #
21 Port 22
22 Port 2022
23 #AddressFamily any
24 #ListenAddress 0.0.0.0
25 #ListenAddress ::
26
27 #HostKey /etc/ssh/ssh_host_rsa_key
28 #HostKey /etc/ssh/ssh_host_ecdsa_key
29 #HostKey /etc/ssh/ssh_host_ed25519_key
30
31 # Ciphers and keying
32 #RekeyLimit default none
```

Параллельные порты SSH (22 и 2022)

```
[root@server.smahmudov.net ~]#  
[root@server.smahmudov.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 Sat 2025-10-18 06:46:16 UTC; 11s ago  
     Invocation: cb77408fbd984b0fb4b00e57e4d54fe8  
       Docs: man:sshd(8)  
             man:sshd_config(5)  
    Main PID: 11049 (sshd)  
      Tasks: 1 (limit: 10381)  
     Memory: 1M (peak: 1.2M)  
        CPU: 4ms  
    CGroup: /system.slice/sshd.service  
            └─11049 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Oct 18 06:46:16 server.smahmudov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...  
Oct 18 06:46:16 server.smahmudov.net (sshd)[11049]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS  
Oct 18 06:46:16 server.smahmudov.net sshd[11049]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.  
Oct 18 06:46:16 server.smahmudov.net sshd[11049]: error: Bind to port 2022 on :: failed: Permission denied.  
Oct 18 06:46:16 server.smahmudov.net sshd[11049]: Server listening on 0.0.0.0 port 22.  
Oct 18 06:46:16 server.smahmudov.net sshd[11049]: Server listening on :: port 22.  
Oct 18 06:46:16 server.smahmudov.net systemd[1]: Started sshd.service - OpenSSH server daemon.  
[root@server.smahmudov.net ~]#
```

Рис. 12: Статус: отказ при привязке к 2022/tcp

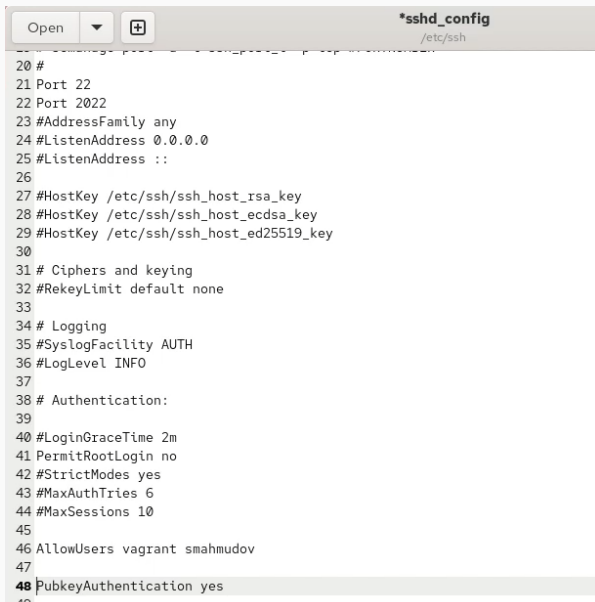
```
[root@server.smahmudov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.smahmudov.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.smahmudov.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.smahmudov.net ~]# systemctl restart sshd
[root@server.smahmudov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-10-18 06:47:43 UTC; 2s ago
     Invocation: 31af615e6b634559b513a92f5be6d96c
       Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 11267 (sshd)
      Tasks: 1 (limit: 10381)
     Memory: 1M (peak: 1.2M)
        CPU: 5ms
    CGroup: /system.slice/ssh.service
            └─11267 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 18 06:47:43 server.smahmudov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Oct 18 06:47:43 server.smahmudov.net (sshd)[11267]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
Oct 18 06:47:43 server.smahmudov.net sshd[11267]: Server listening on 0.0.0.0 port 2022.
Oct 18 06:47:43 server.smahmudov.net sshd[11267]: Server listening on :: port 2022.
Oct 18 06:47:43 server.smahmudov.net sshd[11267]: Server listening on 0.0.0.0 port 22.
Oct 18 06:47:43 server.smahmudov.net sshd[11267]: Server listening on :: port 22.
Oct 18 06:47:43 server.smahmudov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
[root@server.smahmudov.net ~]#
```

Рис. 13: sshd слушает 22 и 2022

```
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net  
smahmudov@server.smahmudov.net's password:  
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/  
  
Last login: Sat Oct 18 06:44:45 2025 from 192.168.1.30  
[smahmudov@server.smahmudov.net ~]$ sudo -i  
[sudo] password for smahmudov:  
[root@server.smahmudov.net ~]#  
logout  
[smahmudov@server.smahmudov.net ~]$  
logout  
Connection to server.smahmudov.net closed.  
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ ssh -p2022 smahmudov@server.smahmudov.net  
smahmudov@server.smahmudov.net's password:  
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/  
  
Last login: Sat Oct 18 06:50:26 2025 from 192.168.1.30  
[smahmudov@server.smahmudov.net ~]$ sudo -i  
[sudo] password for smahmudov:  
[root@server.smahmudov.net ~]#  
logout  
[smahmudov@server.smahmudov.net ~]$  
logout  
Connection to server.smahmudov.net closed.  
[smahmudov@client.smahmudov.net ~]$
```

Аутентификация по ключу (PubkeyAuthentication)



```
*sshd_config
/etc/ssh

20 #
21 Port 22
22 Port 2022
23 #AddressFamily any
24 #ListenAddress 0.0.0.0
25 #ListenAddress ::
26
27 #HostKey /etc/ssh/ssh_host_rsa_key
28 #HostKey /etc/ssh/ssh_host_ecdsa_key
29 #HostKey /etc/ssh/ssh_host_ed25519_key
30
31 # Ciphers and keying
32 #RekeyLimit default none
33
34 # Logging
35 #SyslogFacility AUTH
36 #LogLevel INFO
37
38 # Authentication:
39
40 #LoginGraceTime 2m
41 PermitRootLogin no
42 #StrictModes yes
43 #MaxAuthTries 6
44 #MaxSessions 10
45
46 AllowUsers vagrant smahmudov
47
48 PubkeyAuthentication yes
49
```

Аутентификация по ключу (PubkeyAuthentication)

```
|oX .. o      |
|X.=+o  E o    |
|.==+o.  S .   |
|oo.=.o.o .    |
|++= . =. .    |
|o+.o . +. .   |
|... . .+.     |
+----[SHA256]-----+
[smahmudov@client.smahmudov.net ~]$ ssh-copy-id smahmudov@server.smahmudov.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 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
smahmudov@server.smahmudov.net's password:

Number of key(s) added: 1

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

[smahmudov@client.smahmudov.net ~]$
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net
Web console: https://server.smahmudov.net:9090/ or https://10.0.2.15:9090/

Last login: Sat Oct 18 06:51:35 2025 from 192.168.1.30
[smahmudov@server.smahmudov.net ~]$
logout
Connection to server.smahmudov.net closed.
[smahmudov@client.smahmudov.net ~]$
```

Рис. 16: Результат ssh-copy-id и вход без пароля

```
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ lsof | grep TCP  
[smahmudov@client.smahmudov.net ~]$ ssh -fNL 8080:localhost:80 smahmudov@server.smahmudov.net  
[smahmudov@client.smahmudov.net ~]$ lsof | grep TCP  
ssh          11504              smahmudov    3u      IPv4        88240      0t0      TCP  
client.smahmudov.net:39610->server.smahmudov.net:ssh (ESTABLISHED)  
ssh          11504              smahmudov    4u      IPv6        88245      0t0      TCP  
localhost:webcache (LISTEN)  
ssh          11504              smahmudov    5u      IPv4        88246      0t0      TCP  
localhost:webcache (LISTEN)  
[smahmudov@client.smahmudov.net ~]$
```

Рис. 17: Проверка TCP до/после создания туннеля

Запуск консольных приложений через SSH

```
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net hostname
server.smahmudov.net
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net ls -Al
total 56
-rw-----. 1 smahmudov smahmudov 345 Oct 18 06:50 .bash_history
-rw-r--r--. 1 smahmudov smahmudov 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 smahmudov smahmudov 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 smahmudov smahmudov 549 Sep 7 13:30 .bashrc
drwx-----. 11 smahmudov smahmudov 4096 Sep 11 14:45 .cache
drwx-----. 10 smahmudov smahmudov 4096 Sep 14 07:45 .config
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Desktop
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Documents
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Downloads
drwx-----. 4 smahmudov smahmudov 32 Sep 7 13:33 .local
drwx-----. 5 smahmudov smahmudov 4096 Oct 13 13:24 Maildir
drwxr-xr-x. 5 smahmudov smahmudov 54 Sep 11 14:45 .mozilla
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Music
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Pictures
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Public
drwx-----. 2 smahmudov smahmudov 29 Oct 18 06:54 .ssh
drwxr-xr-x. 2 smahmudov smahmudov 6 Sep 7 13:33 Templates
```

Рис. 18: hostname и содержимое домашнего каталога

Запуск консольных приложений через SSH

```
[smahmudov@client.smahmudov.net ~]$  
[smahmudov@client.smahmudov.net ~]$ ssh smahmudov@server.smahmudov.net MAIL=~/.Maildir mail  
s-nail version v14.9.24. Type '?' for help  
/home/smahmudov/Maildir: 3 messages 1 unread  
   1 smahmudov          2025-10-10 05:29   18/651   "test1           "  
   2 smahmudov@client.sma 2025-10-13 12:40   21/834   "LMTP test       "  
▶U  3 smahmudov          2025-10-13 13:24   22/829   "test hello      "  
q  
Held 3 messages in /home/smahmudov/Maildir  
[smahmudov@client.smahmudov.net ~]$
```

Рис. 19: Просмотр почты пользователя

Результаты и выводы

- Запрет входа root и точечный допуск пользователей повышают безопасность.
- Многопортовый доступ с корректной настройкой SELinux и firewalld работает надёжно.
- Аутентификация по ключу исключает пароль и упрощает доступ.
- Туннели SSH обеспечивают безопасное перенаправление сервисов.
- Базовая автоматизация ускоряет развертывание и снижает ошибки.