

Администрирование сетевых подсистем

Настройка безопасного удалённого доступа по протоколу SSH

Метвалли Ахмед Фарг Набеев

25 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Освоить приёмы настройки SSH-сервера:

- ограничение удалённого доступа для пользователя root,
- разрешение входа определённым пользователям,
- настройка работы через дополнительные порты,
- организация SSH-туннелей и аутентификации по ключам.

Выполнение лабораторной работы

Запрет входа root по SSH

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

Рис. 1: Ошибка подключения по SSH под root

Запрет входа root по SSH

```
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
41 PermitRootLogin no
42
43 #StrictModes yes
44 #MaxAuthTries 6
45 #MaxSessions 10
46
47 #PubkeyAuthentication yes
```

```
[anmedfarg@client.anmedfarg.net ~]#  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net  
ahmedfarg@server.ahmedfarg.net's password:  
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Oct 20 08:39:42 2025  
[ahmedfarg@server.ahmedfarg.net ~]$  
logout  
Connection to server.ahmedfarg.net closed.  
[ahmedfarg@client.ahmedfarg.net ~]$
```

Рис. 3: Успешное подключение ahmedfarg

Ограничение доступа пользователей

```
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
41 PermitRootLogin no
42
43 AllowUsers vagrant|
44
45 #StrictModes yes
46 #MaxAuthTries 6
47 #MaxSessions 10
48
```

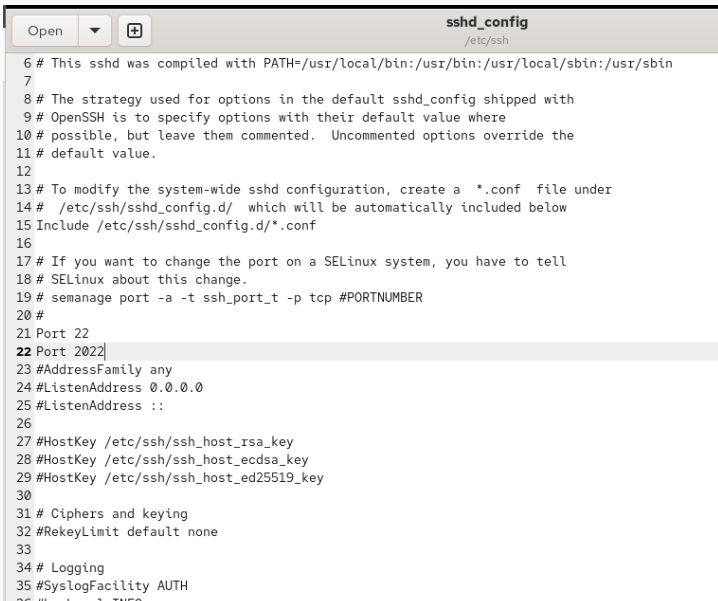


```
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net
ahmedfarg@server.ahmedfarg.net's password:
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/

Last failed login: Mon Oct 20 08:50:20 UTC 2025 from 192.168.1.30 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Mon Oct 20 08:49:13 2025 from 192.168.1.30
[ahmedfarg@server.ahmedfarg.net ~]$
logout
Connection to server.ahmedfarg.net closed.
[ahmedfarg@client.ahmedfarg.net ~]$
```

Рис. 5: Успешное подключение после разрешения

Настройка дополнительных портов SSH



```
sshd_config
/etc/ssh

6 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
7
8 # The strategy used for options in the default sshd_config shipped with
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
33
34 # Logging
35 #SyslogFacility AUTH
36 #LogLevel INFO
```

Настройка дополнительных портов SSH

```
[root@server.ahmedfarg.net ~]# systemctl restart sshd
[root@server.ahmedfarg.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 Mon 2025-10-20 08:55:08 UTC; 14s ago
  Invocation: b94659f23eda424898f09d1c0a0a2011
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 16098 (sshd)
    Tasks: 1 (limit: 10381)
   Memory: 1M (peak: 1.2M)
      CPU: 4ms
   CGroup: /system.slice/sshd.service
           └─16098 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 08:55:08 server.ahmedfarg.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Oct 20 08:55:08 server.ahmedfarg.net (sshd)[16098]: sshd.service: Referenced but unset environment variable evalu
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: error: Bind to port 2022 on :: failed: Permission denied.
Oct 20 08:55:08 server.ahmedfarg.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: Server listening on 0.0.0.0 port 22.
Oct 20 08:55:08 server.ahmedfarg.net sshd[16098]: Server listening on :: port 22.
[root@server.ahmedfarg.net ~]#
```

Рис. 7: Ошибка SELinux при порте 2022

Настройка дополнительных портов SSH

```
[root@server.ahmedfarg.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.ahmedfarg.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.ahmedfarg.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.ahmedfarg.net ~]# systemctl restart sshd
[root@server.ahmedfarg.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 Mon 2025-10-20 08:56:36 UTC; 3s ago
     Invocation: d9ec207bf99548e592468acaa354ba97
       Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 16527 (sshd)
      Tasks: 1 (limit: 10381)
     Memory: 1M (peak: 1.1M)
        CPU: 5ms
    CGroup: /system.slice/sshd.service
            └─16527 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 08:56:36 server.ahmedfarg.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Oct 20 08:56:36 server.ahmedfarg.net (sshd)[16527]: sshd.service: Referenced but unset environment variable evalu
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on 0.0.0.0 port 2022.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on :: port 2022.
Oct 20 08:56:36 server.ahmedfarg.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on 0.0.0.0 port 22.
Oct 20 08:56:36 server.ahmedfarg.net sshd[16527]: Server listening on :: port 22.
[root@server.ahmedfarg.net ~]#
```

Рис. 8: Успешный запуск sshd с двумя портами

Подключение по ключу

```
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
42 PermitRootLogin no
43
44 AllowUsers vagrant ahmedfarg
45
46 #StrictModes yes
47 #MaxAuthTries 6
48 #MaxSessions 10
49 |
50 PubkeyAuthentication yes
51
```

Подключение по ключу

```
-----+
| . . . += . . = +0 E |
| o o . oo + . o . B * |
| . o . = . . o . . o . + |
| . = o . . o * o . . |
| . . . . S + + . . |
| . B . . o |
| . + . |
| . |
|-----+
+-----[SHA256]-----+
```

```
[ahmedfarg@client.ahmedfarg.net ~]$ ssh-copy-id ahmedfarg@server.ahmedfarg.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 t
he new keys
ahmedfarg@server.ahmedfarg.net's password:
```

Number of key(s) added: 1

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

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

Last login: Mon Oct 20 08:59:39 2025 from 192.168.1.30

```
[ahmedfarg@server.ahmedfarg.net ~]$
```

logout

Connection to server.ahmedfarg.net closed.

```
[ahmedfarg@client.ahmedfarg.net ~]$ █
```

```
[ahmedfarg@client.ahmedfarg.net ~]$  
[ahmedfarg@client.ahmedfarg.net ~]$ lsof | grep TCP  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -fNL 8080:localhost:80 ahmedfarg@server.ahmedfarg.net  
[ahmedfarg@client.ahmedfarg.net ~]$ lsof | grep TCP  
ssh          16058          ahmedfarg    3u      IPv4          106560      0t0      TCP clie  
nt.ahmedfarg.net:33522->server.ahmedfarg.net:ssh (ESTABLISHED)  
ssh          16058          ahmedfarg    4u      IPv6          106567      0t0      TCP loca  
lhost:webcache (LISTEN)  
ssh          16058          ahmedfarg    5u      IPv4          106568      0t0      TCP loca  
lhost:webcache (LISTEN)  
[ahmedfarg@client.ahmedfarg.net ~]$
```

Рис. 11: Создание SSH-туннеля и проверка TCP

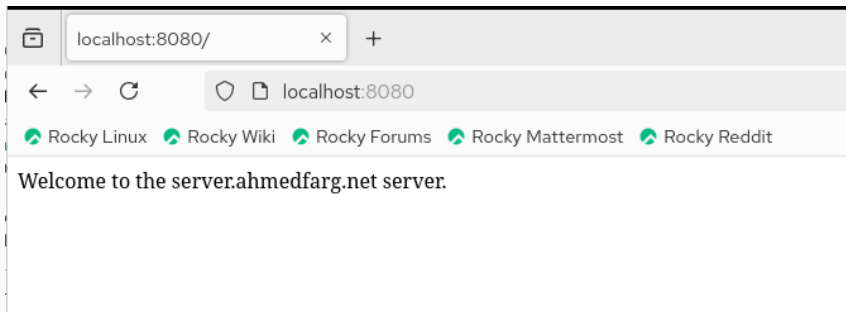


Рис. 12: Отображение страницы через туннель

Запуск приложений через SSH

```
[anmedfarg@client.anmedfarg.net ~]$  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net hostname  
server.ahmedfarg.net  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh ahmedfarg@server.ahmedfarg.net ls -Al  
total 56  
-rw-----, 1 ahmedfarg ahmedfarg 368 Oct 15 10:10 .bash_history  
-rw-r--r--, 1 ahmedfarg ahmedfarg 18 Oct 29 2024 .bash_logout  
-rw-r--r--, 1 ahmedfarg ahmedfarg 144 Oct 29 2024 .bash_profile  
-rw-r--r--, 1 ahmedfarg ahmedfarg 549 Sep 17 08:04 .bashrc  
drwx-----, 11 ahmedfarg ahmedfarg 4096 Sep 17 08:17 .cache  
drwx-----, 10 ahmedfarg ahmedfarg 4096 Sep 17 09:48 .config  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Desktop  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Documents  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Downloads  
drwx-----, 4 ahmedfarg ahmedfarg 32 Sep 17 08:17 .local  
drwx-----, 5 ahmedfarg ahmedfarg 4096 Oct 15 10:06 Maildir  
drwxr-xr-x, 5 ahmedfarg ahmedfarg 54 Sep 17 08:17 .mozilla  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Music  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Pictures  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Public  
drwx-----, 2 ahmedfarg ahmedfarg 29 Oct 20 09:02 .ssh  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Templates  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-clipboard-tty2-control.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 09:05 .vboxclient-clipboard-tty2-service.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-draganddrop-tty2-control.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-hostversion-tty2-control.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-seamless-tty2-control.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-vmtoolsd-session-tty2-control.pid  
-rw-r-----, 1 ahmedfarg ahmedfarg 6 Oct 20 08:39 .vboxclient-vmtoolsd-session-tty2-service.pid  
drwxr-xr-x, 2 ahmedfarg ahmedfarg 6 Sep 17 08:17 Videos  
[ahmedfarg@client.ahmedfarg.net ~]$  
[ahmedfarg@client.ahmedfarg.net ~]$
```

Запуск приложений через SSH

```
85 #GSSAPICleanupCredentials yes
86 #GSSAPIStrictAcceptorCheck yes
87 #GSSAPIKeyExchange no
88 #GSSAPIEnablek5users no
89
90 # Set this to 'yes' to enable PAM authentication, account processing,
91 # and session processing. If this is enabled, PAM authentication will
92 # be allowed through the KbdInteractiveAuthentication and
93 # PasswordAuthentication. Depending on your PAM configuration,
94 # PAM authentication via KbdInteractiveAuthentication may bypass
95 # the setting of "PermitRootLogin prohibit-password".
96 # If you just want the PAM account and session checks to run without
97 # PAM authentication, then enable this but set PasswordAuthentication
98 # and KbdInteractiveAuthentication to 'no'.
99 # WARNING: 'UsePAM no' is not supported in this build and may cause several
100 # problems.
101 #UsePAM no
102
103 #AllowAgentForwarding yes
104 #AllowTcpForwarding yes
105 #GatewayPorts no
106 #X11Forwarding yes
107 #X11DisplayOffset 10
108 #X11UseLocalhost yes
109 #PermitTTY yes
110 #PrintMotd yes
111 #PrintLastLog yes
112 #TCPKeepAlive yes
113 #PermitUserEnvironment no
114 #Compression delayed
115 #ClientAliveInterval 0
116 #ClientAliveCountMax 3
117 #UseDNS no
```

Выводы по проделанной работе

В ходе лабораторной работы:

- освоены методы настройки SSH-сервера и контроля доступа;
- реализованы резервные порты и ключевая аутентификация;
- продемонстрирована работа SSH-туннелей;
- подготовлен скрипт автоматизации конфигурации.

Результаты подтвердили успешную настройку и безопасную работу SSH-сервера.