Администрирование системных подсистем

Настройка безопасного удалённого доступа по SSH

Сейдалиев Тагиетдин Ровшенович

05 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Приобрести практические навыки настройки защищённого SSH-доступа,
включая работу с пользователями, ключевой аутентификацией, портами и туннелями.

Запрет доступа root

Попытка входа root

- Система запрашивает пароль, но не допускает root
- В журнале фиксируются отказанные попытки входа
- В конфигурации установлен `PermitRootLogin no`

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

Конфигурация

```
#
#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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

Ограничение пользователей SSH

Вход пользователя trseidaliev

Успешное подключение:

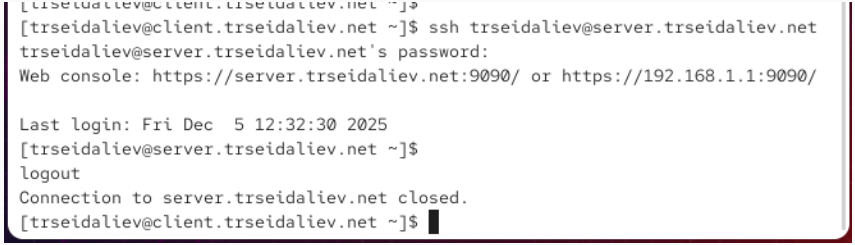

Рис. 3: Успешный вход

AllowUsers

Разрешён только `vagrant`:

```
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
```

Добавление второго пользователя

После добавления trseidaliev:

```
#
#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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

Настройка нескольких портов SSH

Добавление порта 2022

```
#
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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

AllowUsers vagrant trseidaliev

#PubkeyAuthentication yes
```

Ошибка SELinux

```
[root@server.trseidaliev.net ~]# gedit /etc/ssh/sshd_config
[root@server.trseidaliev.net ~]# systemctl restart sshd
[root@server.trseidaliev.net ~]#
[root@server.trseidaliev.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 Fri 2025-12-05 12:46:03 MSK; 14s ago
 Invocation: 3f1ec6e9d3734f5ab3f5efc5e3ca54e5
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 17151 (sshd)
      Tasks: 1 (limit: 10381)
     Memory: 1M (peak: 1.2M)
        CPU: 4ms
     CGroup: /system.slice/sshd.service
             └─17151 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 05 12:46:03 server.trseidaliev.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Dec 05 12:46:03 server.trseidaliev.net (sshd)[17151]: sshd.service: Referenced but unset environment variable evaluat>
Dec 05 12:46:03 server.trseidaliev.net sshd[17151]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Dec 05 12:46:03 server.trseidaliev.net sshd[17151]: error: Bind to port 2022 on :: failed: Permission denied.
Dec 05 12:46:03 server.trseidaliev.net sshd[17151]: Server listening on 0.0.0.0 port 22.
Dec 05 12:46:03 server.trseidaliev.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Dec 05 12:46:03 server.trseidaliev.net sshd[17151]: Server listening on :: port 22.
[root@server.trseidaliev.net ~]#
```

Рис. 9: Permission denied port 2022

SELinux блокирует нестандартный порт до назначения корректной метки.

Исправление и запуск

После настройки SELinux и firewall — оба порта работают:

```
[root@server.trseidaliev.net ~]#
[root@server.trseidaliev.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.trseidaliev.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.trseidaliev.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.trseidaliev.net ~]# systemctl restart sshd
[root@server.trseidaliev.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 Fri 2025-12-05 12:48:02 MSK; 4s ago
 Invocation: d3524c722be745e0a65d9009ceadf0ab
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 17436 (sshd)
      Tasks: 1 (limit: 10381)
     Memory: 1M (peak: 1.3M)
        CPU: 5ms
     CGroup: /system.slice/sshd.service
             └─17436 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 05 12:48:02 server.trseidaliev.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Dec 05 12:48:02 server.trseidaliev.net (sshd)[17436]: sshd.service: Referenced but unset environment variable evaluat>
Dec 05 12:48:02 server.trseidaliev.net sshd[17436]: Server listening on 0.0.0.0 port 2022.
Dec 05 12:48:02 server.trseidaliev.net sshd[17436]: Server listening on :: port 2022.
Dec 05 12:48:02 server.trseidaliev.net sshd[17436]: Server listening on 0.0.0.0 port 22.
Dec 05 12:48:02 server.trseidaliev.net sshd[17436]: Server listening on :: port 22.
Dec 05 12:48:02 server.trseidaliev.net systemd[1]: Started sshd.service - OpenSSH server daemon.
[root@server.trseidaliev.net ~]#
```

Проверка соединений

Через порт 22 и 2022:

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

Last login: Fri Dec  5 12:44:14 2025 from 192.168.1.30
[trseidaliev@server.trseidaliev.net ~]$ sudo -i
[sudo] password for trseidaliev:
[root@server.trseidaliev.net ~]#
logout
[trseidaliev@server.trseidaliev.net ~]$
logout
Connection to server.trseidaliev.net closed.
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$ ssh trseidaliev@server.trseidaliev.net -p2022
trseidaliev@server.trseidaliev.net's password:
Web console: https://server.trseidaliev.net:9090/ or https://192.168.1.1:9090/

Last login: Fri Dec  5 12:48:34 2025 from 192.168.1.30
[trseidaliev@server.trseidaliev.net ~]$ sudo -i
[sudo] password for trseidaliev:
[root@server.trseidaliev.net ~]#
logout
[trseidaliev@server.trseidaliev.net ~]$
logout
```

Подключение по ключам

Включение PubkeyAuthentication

```
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 trseidaliev
47
48 PubkeyAuthentication yes
```

Установка ключей и подключение

Сгенерированы ключи, публичный импортирован на сервер.

Подключение выполняется без пароля:

```
|*+*.B .          |
|==+=.*           |
|.  =+=o o        |
|  ooB .o .       |
+----[SHA256]-----+
[trseidaliev@client.trseidaliev.net ~]$ ssh-copy-id trseidaliev@server.trseidaliev.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 i
nstall the new keys
trseidaliev@server.trseidaliev.net's password:

Number of key(s) added: 1

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

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

Last login: Fri Dec  5 12:48:57 2025 from 192.168.1.30
[trseidaliev@server.trseidaliev.net ~]$
```

SSH-туннели и перенаправление портов

Создание туннеля

До туннеля — список соединений пуст.

После создания туннеля:

```
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$ lsof | grep TCP
[trseidaliev@client.trseidaliev.net ~]$ ssh -fNL 8080:localhost:80 trseidaliev@server.trseidaliev
.net
[trseidaliev@client.trseidaliev.net ~]$ lsof | grep TCP
ssh       11726                    trseidaliev    3u     IPv4              73679       0t0
TCP client.trseidaliev.net:39702->mail.trseidaliev.net:ssh (ESTABLISHED)
ssh       11726                    trseidaliev    4u     IPv6              73691       0t0
TCP localhost:webcache (LISTEN)
ssh       11726                    trseidaliev    5u     IPv4              73692       0t0
TCP localhost:webcache (LISTEN)
[trseidaliev@client.trseidaliev.net ~]$
```

Рис. 14: Список TCP

Проверка

Переход на `localhost:8080` открывает страницу сервера:

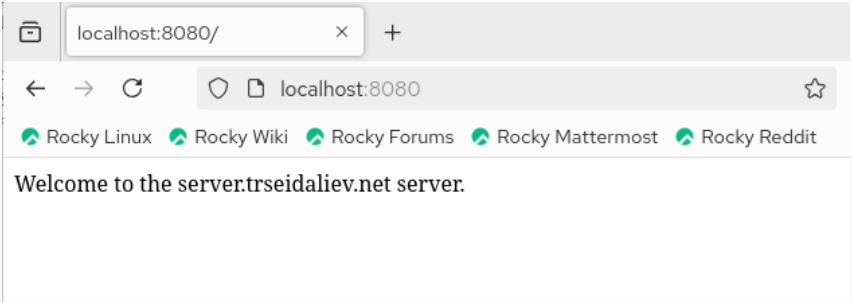

Рис. 15: Прокси веб-сервера

Удалённый запуск приложений

hostname:

```
[trseidaliev@client.trseidaliev.net ~]$ ssh trseidaliev@server.trseidaliev.net hostname
server.trseidaliev.net
[trseidaliev@client.trseidaliev.net ~]$ ssh trseidaliev@server.trseidaliev.net ls -Al
total 56
-rw-------.  1 trseidaliev trseidaliev  656 Dec  5 12:48 .bash_history
-rw-r--r--.  1 trseidaliev trseidaliev   18 Oct 29  2024 .bash_logout
-rw-r--r--.  1 trseidaliev trseidaliev  144 Oct 29  2024 .bash_profile
-rw-r--r--.  1 trseidaliev trseidaliev  549 Nov 19 10:19 .bashrc
drwx------. 11 trseidaliev trseidaliev 4096 Nov 19 18:22 .cache
drwx------. 12 trseidaliev trseidaliev 4096 Nov 30 11:07 .config
drwxr-xr-x.  2 trseidaliev trseidaliev    6 Nov 19 10:19 Desktop
drwxr-xr-x.  2 trseidaliev trseidaliev    6 Nov 19 10:19 Documents
drwxr-xr-x.  2 trseidaliev trseidaliev    6 Nov 19 10:19 Downloads
drwx------.  4 trseidaliev trseidaliev   32 Nov 19 10:19 .local
drwx------.  5 trseidaliev trseidaliev 4096 Nov 30 11:37 Maildir
drwxr-xr-x.  5 trseidaliev trseidaliev   54 Nov 19 18:22 .mozilla
drwxr-xr-x.  2 trseidaliev trseidaliev    6 Nov 19 10:19 Music
drwxr-xr-x.  2 trseidaliev trseidaliev    6 Nov 19 10:19 Pictures
```

Рис. 16: hostname

Maildir:

```
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$ ssh trseidaliev@server.trseidaliev.net MAIL=~/Maildir mai
l
s-nail version v14.9.24.  Type `?' for help
/home/trseidaliev/Maildir: 3 messages 1 unread
    1 trseidaliev           2025-11-30 10:46   18/685   "test1                "
    2 trseidaliev@client.t  2025-11-30 11:11   21/880   "LMTP TEST            "
▸U  3 trseidaliev           2025-11-30 11:37   22/861   "test3                "
q
Held 3 messages in /home/trseidaliev/Maildir
[trseidaliev@client.trseidaliev.net ~]$
```

Рис. 17: Maildir

X11-переадресация

Включение X11Forwarding

```
#
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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

AllowUsers vagrant trseidaliev

PubkeyAuthentication yes

X11Forwarding yes
```

Ошибка запуска GUI

```
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$ ssh -YC trseidaliev@server.trseidaliev.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
[trseidaliev@client.trseidaliev.net ~]$
[trseidaliev@client.trseidaliev.net ~]$ ssh -YC trseidaliev@server.trseidaliev.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
[trseidaliev@client.trseidaliev.net ~]$
```

Рис. 19: Ошибка X11

Причина: на клиенте отсутствует активный X-сервер.

Автоматизация провижининга

Создание каталога и скрипта

В каталог `/vagrant/provision/server/ssh/etc/ssh` помещён рабочий sshd_config.

Файл `ssh.sh` автоматизирует все ручные действия.

```
#!/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. 20: ssh.sh

Итоги

Основные результаты

- Ограничен список разрешённых пользователей
- Включена работа SSH на портах 22 и 2022
- Реализована аутентификация по ключам
- Созданы SSH-туннели и проверена их работа
- Выполнен удалённый запуск консольных приложений