Настройка безопасного удалённого доступа по SSH

Лабораторная работа №11

Элсаиед Адел

6 января 2026

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

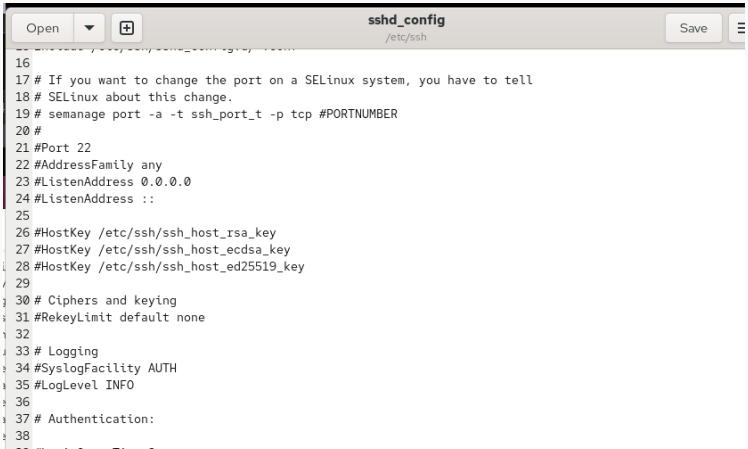
Цель лабораторной работы

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

Выполнение работы

Запрет доступа по SSH для пользователя root

На сервере выполнен запрет удалённого входа для root с помощью параметра `PermitRootLogin no`. Повторная попытка входа фиксируется в журналах и завершается отказом на стадии аутентификации.



Контроль попыток входа root в журнале

При попытке SSH-входа под root на сервере регистрируются события отказа/завершения сессии, что подтверждает применение настроек безопасности.

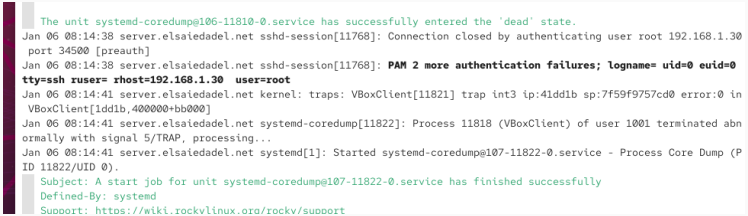
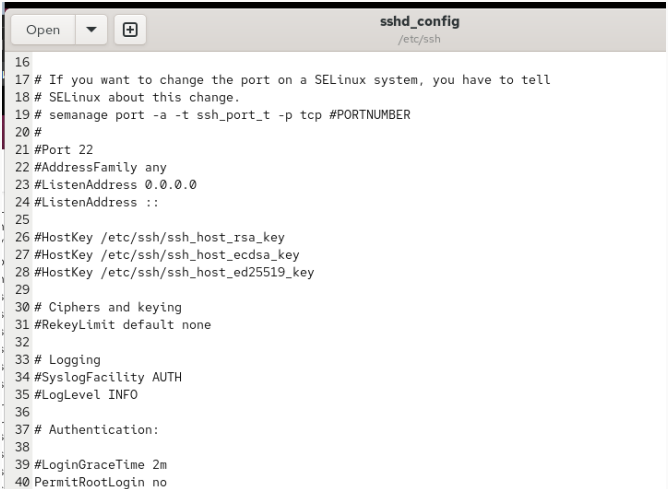


Рис. 2: Попытка входа root после запрета

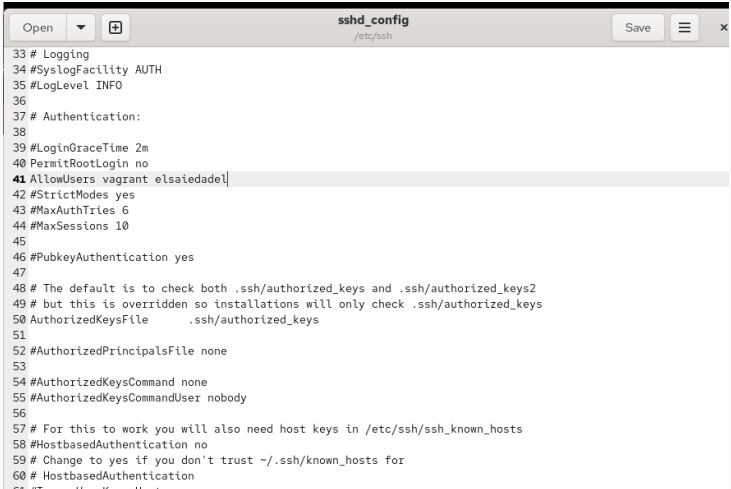
Ограничение списка пользователей (AllowUsers)

Для контроля удалённого доступа задан список разрешённых пользователей. При включении `AllowUsers vagrant` подключения прочих пользователей отклоняются.



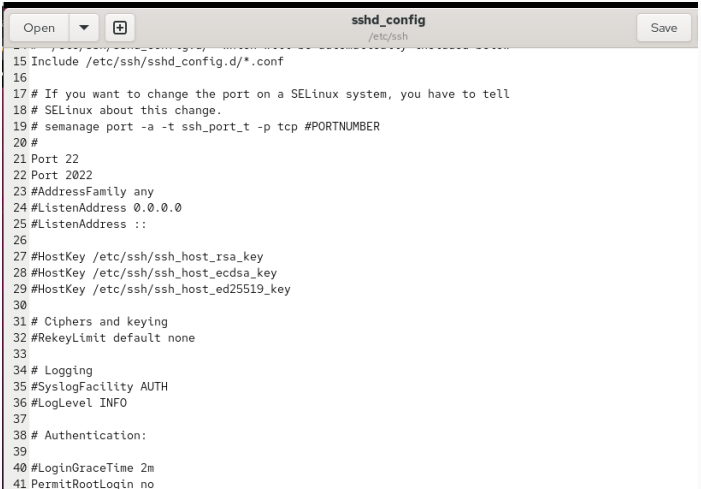
Восстановление доступа добавлением пользователя в AllowUsers

Для разрешения подключения добавлен пользователь `elsaiedadel` в список. После перезапуска sshd удалённый вход становится доступен.



Перенос SSH на порт 2022: корректная конфигурация

Для работы SSH на порту 2022 в конфигурации заданы отдельные директивы `Port 22` и `Port 2022`, что обеспечивает одновременное прослушивание двух портов.



SELinux и firewall для порта 2022

Выполнена настройка SELinux для разрешения контекста `ssh_port_t` на 2022 и открытие `2022/tcp` в межсетевом экране. После исправления конфигурации sshd успешно запущен и слушает порт 2022.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.elsaiedadel.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.elsaiedadel.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.elsaiedadel.net ~]# systemctl restart sshd
Job for sshd.service failed because the control process exited with error code.
See "systemctl status sshd.service" and "journalctl -xeu sshd.service" for details.
[root@server.elsaiedadel.net ~]# gedit /etc/ssh/sshd_config
[root@server.elsaiedadel.net ~]# systemctl restart sshd
[root@server.elsaiedadel.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 Tue 2026-01-06 08:24:10 UTC; 7s ago
 Invocation: ba1b0d80cedf4037ae0d8c06fe41fc2d
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 13484 (sshd)
      Tasks: 1 (limit: 10275)
     Memory: 1.3M (peak: 1.5M)
        CPU: 5ms
     CGroup: /system.slice/sshd.service
             └─13484 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 06 08:24:10 server.elsaiedadel.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Jan 06 08:24:10 server.elsaiedadel.net sshd[13484]: Server listening on 0.0.0.0 port 2022.
Jan 06 08:24:10 server.elsaiedadel.net sshd[13484]: Server listening on :: port 2022.
Jan 06 08:24:10 server.elsaiedadel.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Jan 06 08:24:10 server.elsaiedadel.net sshd[13484]: Server listening on 0.0.0.0 port 22.
```

Проверка подключений по портам 22 и 2022

С клиента подтверждено, что соединение устанавливается как по порту 22 (по умолчанию), так и по порту 2022 при явном указании параметров подключения.

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

Last login: Tue Jan  6 08:19:52 2026 from 192.168.1.30
[elsaiedadel@server.elsaiedadel.net ~]$ sudo -i
[sudo] password for elsaiedadel:
[root@server.elsaiedadel.net ~]#
logout
[elsaiedadel@server.elsaiedadel.net ~]$
logout
Connection to server.elsaiedadel.net closed.
[elsaiedadel@client.elsaiedadel.net ~]$
[elsaiedadel@client.elsaiedadel.net ~]$ ssh elsaiedadel@server.elsaiedadel.net -p2022
elsaiedadel@server.elsaiedadel.net's password:
Web console: https://server.elsaiedadel.net:9090/ or https://192.168.1.1:9090/

Last login: Tue Jan  6 08:28:07 2026 from 192.168.1.30
[elsaiedadel@server.elsaiedadel.net ~]$ sudo -i
[sudo] password for elsaiedadel:
[root@server.elsaiedadel.net ~]#
logout
[elsaiedadel@server.elsaiedadel.net ~]$
logout
Connection to server.elsaiedadel.net closed.
[elsaiedadel@client.elsaiedadel.net ~]$
```

Аутентификация по ключу (PubkeyAuthentication)

На сервере включена аутентификация по ключу. На клиенте создана пара ключей и открытый ключ установлен на сервер, после чего вход выполняется без запроса пароля.

```
[elsaiedadel@client.elsaiedadel.net ~]$ ssh-copy-id elsaiedadel@server.elsaiedadel.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 alread
y 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
elsaiedadel@server.elsaiedadel.net's password:

Number of key(s) added: 1

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

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

Last login: Tue Jan  6 08:28:27 2026 from 192.168.1.30
[elsaiedadel@server.elsaiedadel.net ~]$
logout
Connection to server.elsaiedadel.net closed.
[elsaiedadel@client.elsaiedadel.net ~]$
```

Рис. 8: Копирование ключа на сервер и вход без пароля

SSH-туннель: перенаправление порта 8080 на 80

Организовано перенаправление: локальный порт 8080 обслуживается процессом SSH и проксирует доступ к удалённому сервису на порту 80. Состояние подтверждается появлением локального LISTEN и активного SSH-соединения.

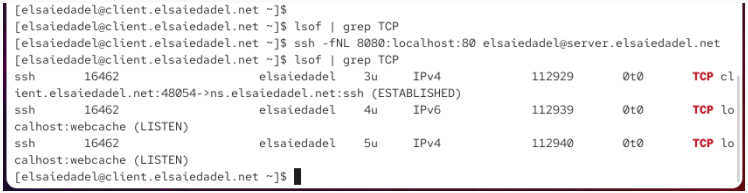


Рис. 9: TCP-сокеты до/после создания туннеля

Проверка туннеля в браузере

При открытии `localhost:8080` на клиенте отображается приветственная страница, что подтверждает корректную работу туннеля и перенаправления.

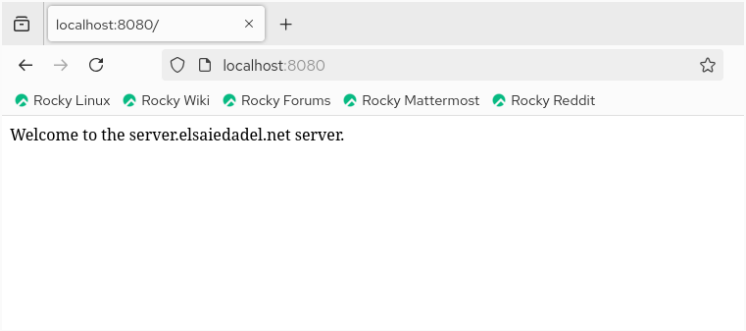


Рис. 10: Страница Welcome через localhost:8080

Запуск удалённых консольных команд через SSH

Проверен запуск команд на сервере без интерактивной сессии: получение имени хоста, просмотр файлов и проверка почты. Это демонстрирует применение SSH как инструмента удалённого администрирования.

```
[elsaiedadel@client.elsaiedadel.net ~]$ ssh elsaiedadel@server.elsaiedadel.net hostname
server.elsaiedadel.net
[elsaiedadel@client.elsaiedadel.net ~]$ ssh elsaiedadel@server.elsaiedadel.net ls -Al
total 56
-rw-------.  1 elsaiedadel elsaiedadel  460 Jan  6 08:28 .bash_history
-rw-r--r--.  1 elsaiedadel elsaiedadel   18 Oct 29  2024 .bash_logout
-rw-r--r--.  1 elsaiedadel elsaiedadel  144 Oct 29  2024 .bash_profile
-rw-r--r--.  1 elsaiedadel elsaiedadel  549 Jan  2 08:51 .bashrc
drwx------. 11 elsaiedadel elsaiedadel 4096 Jan  4 07:44 .cache
drwx------. 10 elsaiedadel elsaiedadel 4096 Jan  2 10:57 .config
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Desktop
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Documents
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Downloads
drwx------.  4 elsaiedadel elsaiedadel   32 Jan  2 08:52 .local
drwx------.  5 elsaiedadel elsaiedadel 4096 Jan  4 09:21 Maildir
drwxr-xr-x.  5 elsaiedadel elsaiedadel   54 Jan  4 07:44 .mozilla
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Music
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Pictures
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Public
drwx------.  2 elsaiedadel elsaiedadel   29 Jan  6 08:33 .ssh
drwxr-xr-x.  2 elsaiedadel elsaiedadel    6 Jan  2 08:52 Templates
-rw-r-----.  1 elsaiedadel elsaiedadel    6 Jan  6 08:05 .vboxclient-clipboard-tty2-control.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    7 Jan  6 08:36 .vboxclient-clipboard-tty2-service.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    6 Jan  6 08:05 .vboxclient-draganddrop-tty2-control.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    6 Jan  6 08:05 .vboxclient-hostversion-tty2-control.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    6 Jan  6 08:05 .vboxclient-seamless-tty2-control.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    6 Jan  6 08:05 .vboxclient-vmsvga-session-tty2-control.pid
-rw-r-----.  1 elsaiedadel elsaiedadel    5 Jan  6 08:05 .vboxclient-vmsvga-session-tty2-service.pid
```

X11 Forwarding: попытка запуска графического приложения

Разрешено `X11Forwarding yes`, затем выполнена попытка удалённого запуска Firefox. На клиенте получена ошибка, связанная с отсутствием DISPLAY и невозможностью X11-перенаправления, что указывает на необходимость настроенного X-сервера на стороне клиента.

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

Рис. 12: Ошибка X11: отсутствует DISPLAY

Автоматизация настроек: provisioning-скрипт ssh.sh

Подготовлен скрипт, который копирует эталонную конфигурацию SSH, восстанавливает контексты SELinux, настраивает firewall для 2022 и перезапускает sshd. Это обеспечивает воспроизводимое применение настроек при запуске ВМ.

Vagrantfile ssh.sh

```
#!/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
```

Выводы

Вывод

В ходе работы выполнена настройка безопасного SSH-доступа: запрещён вход root, ограничены пользователи, настроены ключи, выполнен перенос SSH на порт 2022 с поддержкой SELinux и firewall, проверены туннели и удалённый запуск команд. Подготовлен provisioning-скрипт для автоматизации конфигурации SSH в среде виртуализации.