

Лабораторная работа

№11

Настройка безопасного удалённого доступа по
протоколу SSH

Студент: Пакавира Арсениу Висенте Луиш
Группа: НФИбд 02–23

дисциплина: Администрирование сетевых подсистем (Lab 11)

Цель работы

Целью данной работы является приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

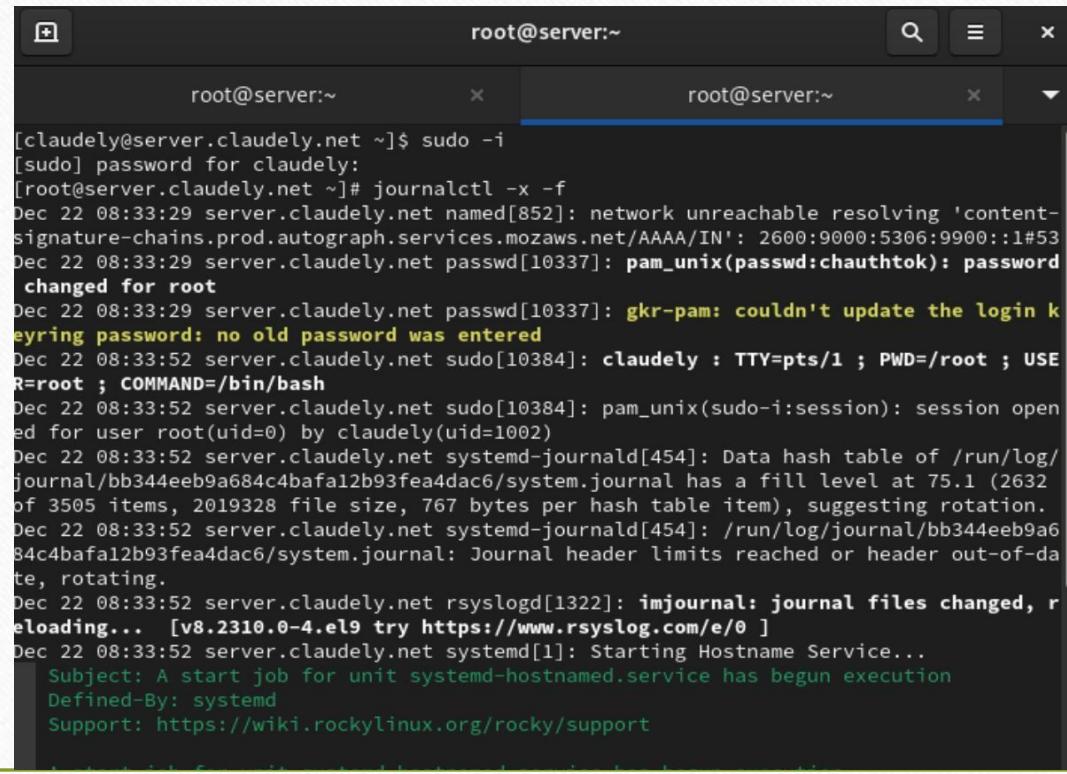
Запрет удалённого доступа по SSH для пользователя root

The screenshot shows two terminal windows side-by-side. The left window, titled 'root@server:~', displays the command `sudo -i` being run by user 'claudely'. It prompts for a password and then grants root privileges, changing the prompt to '[root@server.claudely.net ~]#'. The right window, titled 'claudely@server:~', shows the user 'claudely' running the `passwd root` command to change the root password. The terminal interface includes standard Linux-style prompts and feedback.

```
root@server:~ [claudely@server.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@server.claudely.net ~]# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server.claudely.net ~]#
```

Рис. 1.1. Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

Запрет удалённого доступа по SSH для пользователя root

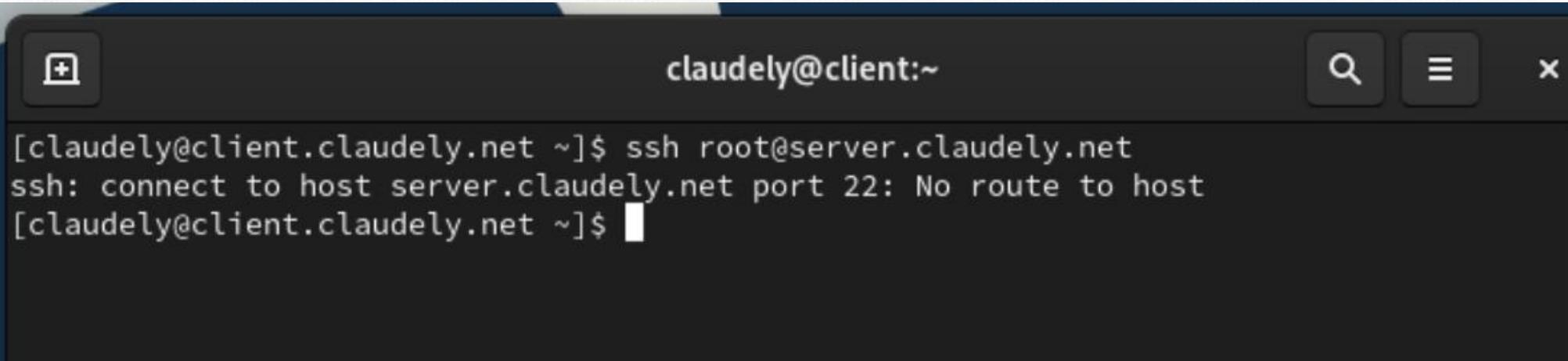


The screenshot shows a terminal window titled "root@server:~". It contains the following log entries:

```
[claudely@server.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@server.claudely.net ~]# journalctl -x -f
Dec 22 08:33:29 server.claudely.net named[852]: network unreachable resolving 'content-signature-chains.prod.autograph.services.mozaws.net/AAAA/IN': 2600:9000:5306:9900::1#53
Dec 22 08:33:29 server.claudely.net passwd[10337]: pam_unix(passwd:chauthtok): password changed for root
Dec 22 08:33:29 server.claudely.net passwd[10337]: gkr-pam: couldn't update the login keyring password: no old password was entered
Dec 22 08:33:52 server.claudely.net sudo[10384]: claudely : TTY=pts/1 ; PWD=/root ; USE_Root ; COMMAND=/bin/bash
Dec 22 08:33:52 server.claudely.net sudo[10384]: pam_unix(sudo-i:session): session opened for user root(uid=0) by claudely(uid=1002)
Dec 22 08:33:52 server.claudely.net systemd-journald[454]: Data hash table of /run/log/journal/bb344eeb9a684c4bafa12b93fea4dac6/system.journal has a fill level at 75.1 (2632 of 3505 items, 2019328 file size, 767 bytes per hash table item), suggesting rotation.
Dec 22 08:33:52 server.claudely.net systemd-journald[454]: /run/log/journal/bb344eeb9a684c4bafa12b93fea4dac6/system.journal: Journal header limits reached or header out-of-date, rotating.
Dec 22 08:33:52 server.claudely.net rsyslogd[1322]: imjournal: journal files changed, reloading... [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Dec 22 08:33:52 server.claudely.net systemd[1]: Starting Hostname Service...
Subject: A start job for unit systemd-hostnamed.service has begun execution
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support
```

Рис. 1.2. Запуск в дополнительном терминале мониторинга системных событий.

Запрет удалённого доступа по SSH для пользователя root



```
[claudely@client.claudely.net ~]$ ssh root@server.claudely.net
ssh: connect to host server.claudely.net port 22: No route to host
[claudely@client.claudely.net ~]$ █
```

Запрет удалённого доступа по SSH для

Рис. 1.3. Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.

Запрет удалённого доступа по SSH для пользователя root

```
root@server:~          root@server:~  
  
#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
```

Рис. 1.4. Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd для редактирования и запрет входа на сервер пользователю root.

Запрет удалённого доступа по SSH для пользователя root

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]# █
```

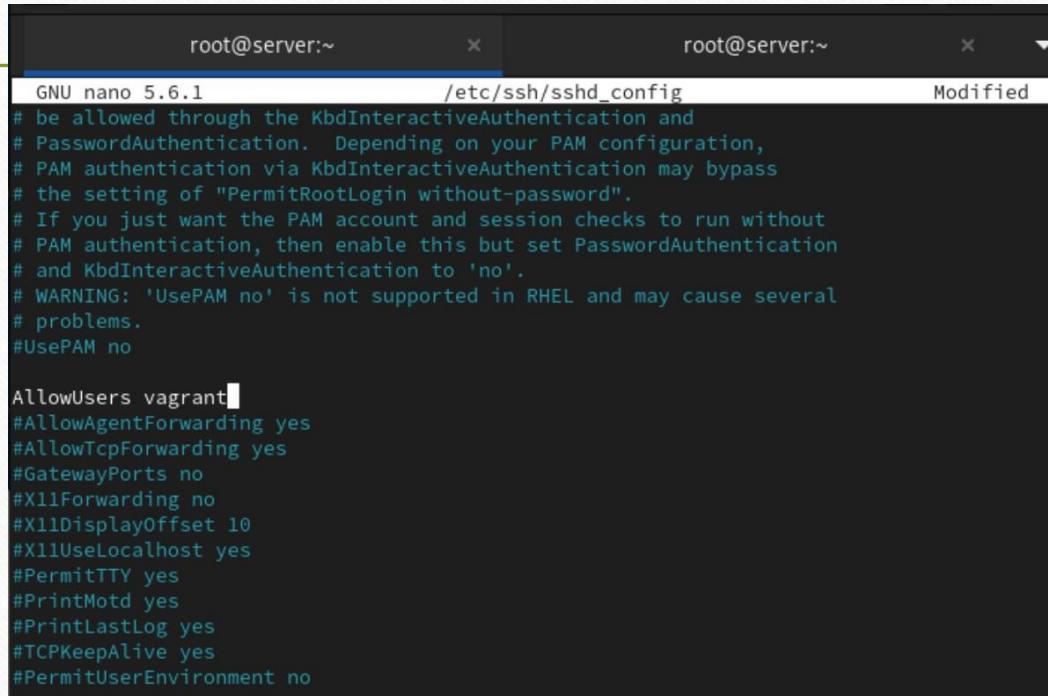
Рис. 1.5. Перезапуск sshd.

Ограничение списка пользователей

для

удалённого доступа по SSH

Ограничение списка пользователей для



The screenshot shows two terminal windows side-by-side. Both windows have the title bar 'root@server:~' and the status bar 'Modified'. The left window displays the command 'GNU nano 5.6.1 /etc/ssh/sshd_config'. The right window shows the same path. The file content is as follows:

```
GNU nano 5.6.1          /etc/ssh/sshd_config          Modified
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

AllowUsers vagrant
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
```

Рис. 2.2. Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd на редактирование и добавление нужной строки.

Ограничение списка пользователей

для

удалённого доступа по SSH

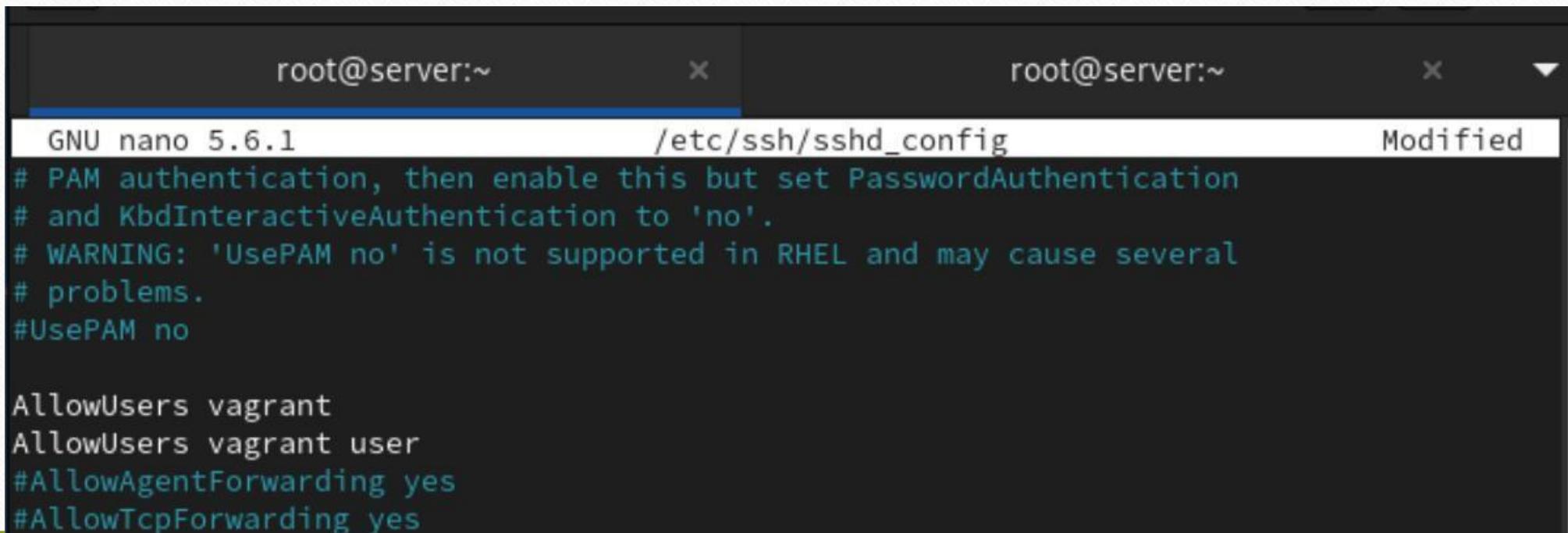
```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 2.3. Перезапуск sshd.

Ограничение списка пользователей

для

удалённого доступа по SSH



The screenshot shows two terminal windows side-by-side. Both windows have a dark background and white text. The left window title bar says "root@server:~" and the right window title bar also says "root@server:~". The left window has a blue horizontal bar at the top with the text "GNU nano 5.6.1". The right window has a similar bar with the text "/etc/ssh/sshd_config Modified". The content of the file is displayed in both windows:

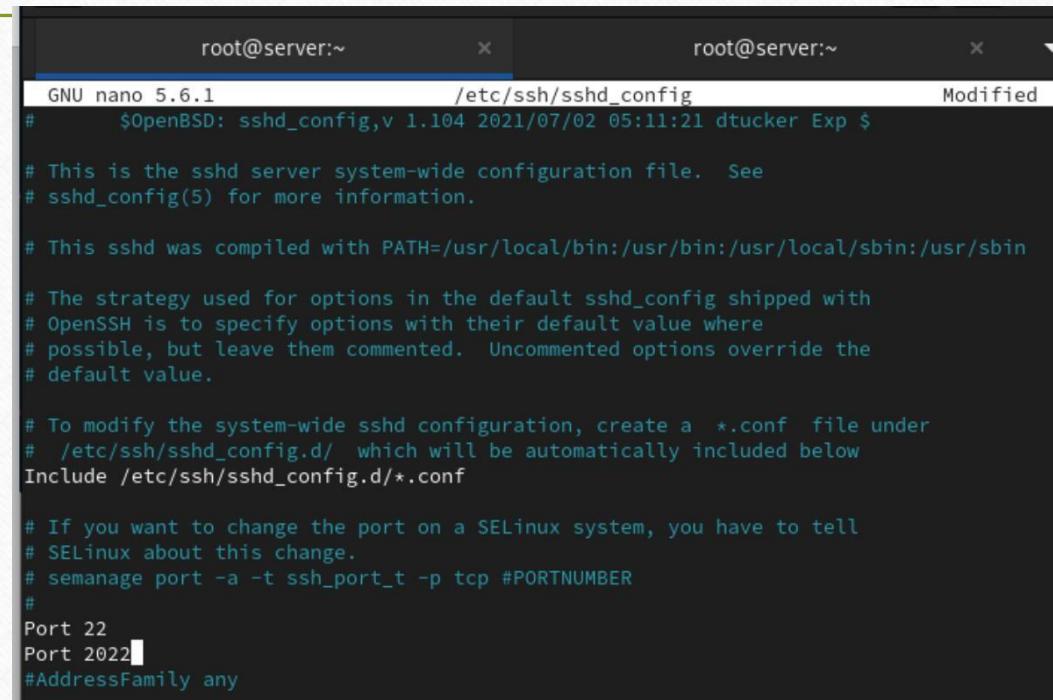
```
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

AllowUsers vagrant
AllowUsers vagrant user
#AllowAgentForwarding yes
#AllowTcpForwarding yes
```

Ограничение списка пользователей для

Рис. 2.5. Внесение изменения в файле /etc/ssh/sshd_config конфигурации sshd.

Настройка дополнительных портов для удалённого доступа по SSH



```
root@server:~          root@server:~          Modified
GNU nano 5.6.1          /etc/ssh/sshd_config
#      $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

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

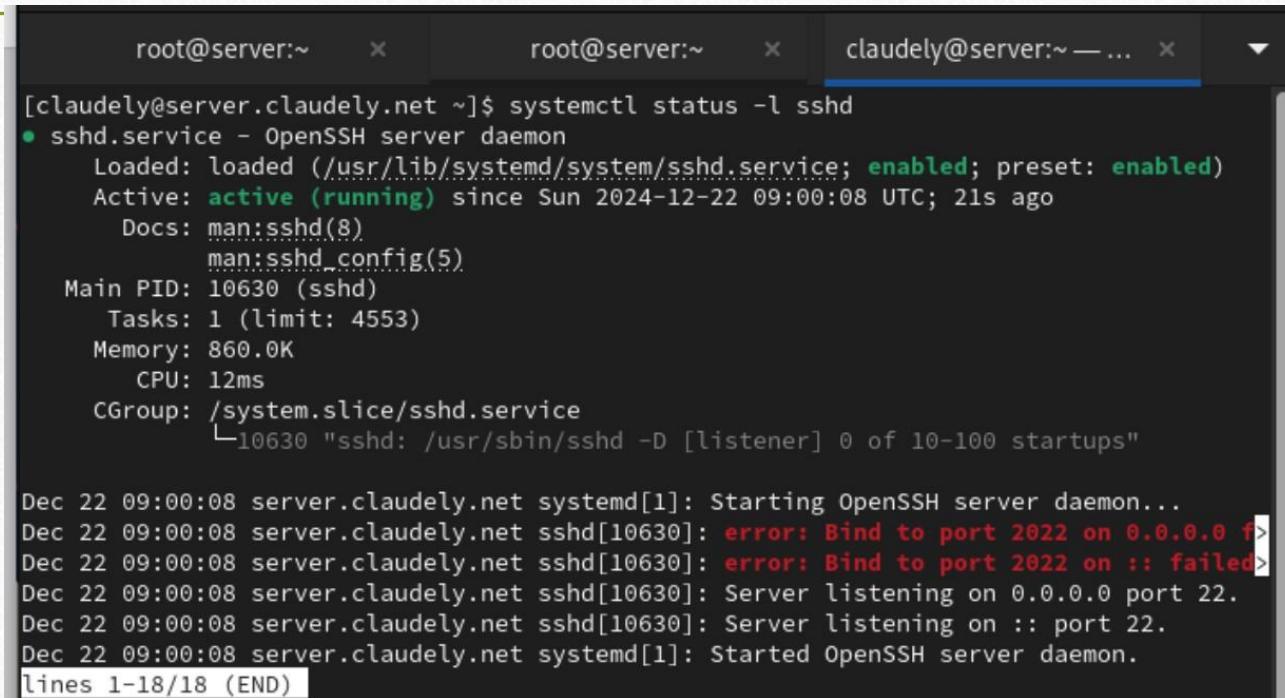
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# 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
```

Рис. 3.1. Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.

Настройка дополнительных портов для удалённого доступа по SSH



The screenshot shows a terminal window with three tabs. The active tab is for the user 'claudely' at the server. The command run is:

```
[claudely@server.claudely.net ~]$ systemctl status -l sshd
```

The output shows the following details about the sshd service:

- sshd.service - OpenSSH server daemon
 - Loaded: loaded (/usr/lib/systemd/system/sshd.service; **enabled**; preset: **enabled**)
 - Active: **active (running)** since Sun 2024-12-22 09:00:08 UTC; 21s ago
 - Docs: man:sshd(8)
man:sshd_config(5)
 - Main PID: 10630 (sshd)
 - Tasks: 1 (limit: 4553)
 - Memory: 860.0K
 - CPU: 12ms
 - CGroup: /system.slice/sshd.service
└─10630 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Below the service status, the terminal displays log messages from the sshd daemon:

```
Dec 22 09:00:08 server.claudely.net systemd[1]: Starting OpenSSH server daemon...
Dec 22 09:00:08 server.claudely.net sshd[10630]: error: Bind to port 2022 on 0.0.0.0 failed
Dec 22 09:00:08 server.claudely.net sshd[10630]: error: Bind to port 2022 on :: failed
Dec 22 09:00:08 server.claudely.net sshd[10630]: Server listening on 0.0.0.0 port 22.
Dec 22 09:00:08 server.claudely.net sshd[10630]: Server listening on :: port 22.
Dec 22 09:00:08 server.claudely.net systemd[1]: Started OpenSSH server daemon.
```

At the bottom of the terminal window, it says "lines 1-18/18 (END)".

Рис. 3.2. Нерезапуск sshd и просмотр расширенного статуса работы.

Настройка дополнительных портов для удалённого доступа по SSH

```
ged@18.service: Deactivated successfully.  
Subject: Unit succeeded  
Defined-By: systemd  
Support: https://wiki.rockylinux.org/rocky/support  
  
The unit dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@18.service has successfully entered the 'dead' state.  
Dec 22 09:43:31 client.claudely.net systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@18.service: Consumed 2.294s CPU time.  
Subject: Resources consumed by unit runtime  
Defined-By: systemd  
Support: https://wiki.rockylinux.org/rocky/support  
  
The unit dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@18.service completed and consumed the indicated resources.  
Dec 22 09:43:34 client.claudely.net systemd[1]: setroubleshootd.service: Deactivated successfully  
.  
Subject: Unit succeeded  
Defined-By: systemd  
Support: https://wiki.rockylinux.org/rocky/support  
  
The unit setroubleshootd.service has successfully entered the 'dead' state.  
Dec 22 09:43:34 client.claudely.net systemd[1]: setroubleshootd.service: Consumed 1.234s CPU time  
.  
Subject: Resources consumed by unit runtime  
Defined-By: systemd  
Support: https://wiki.rockylinux.org/rocky/support  
  
The unit setroubleshootd.service completed and consumed the indicated resources.
```

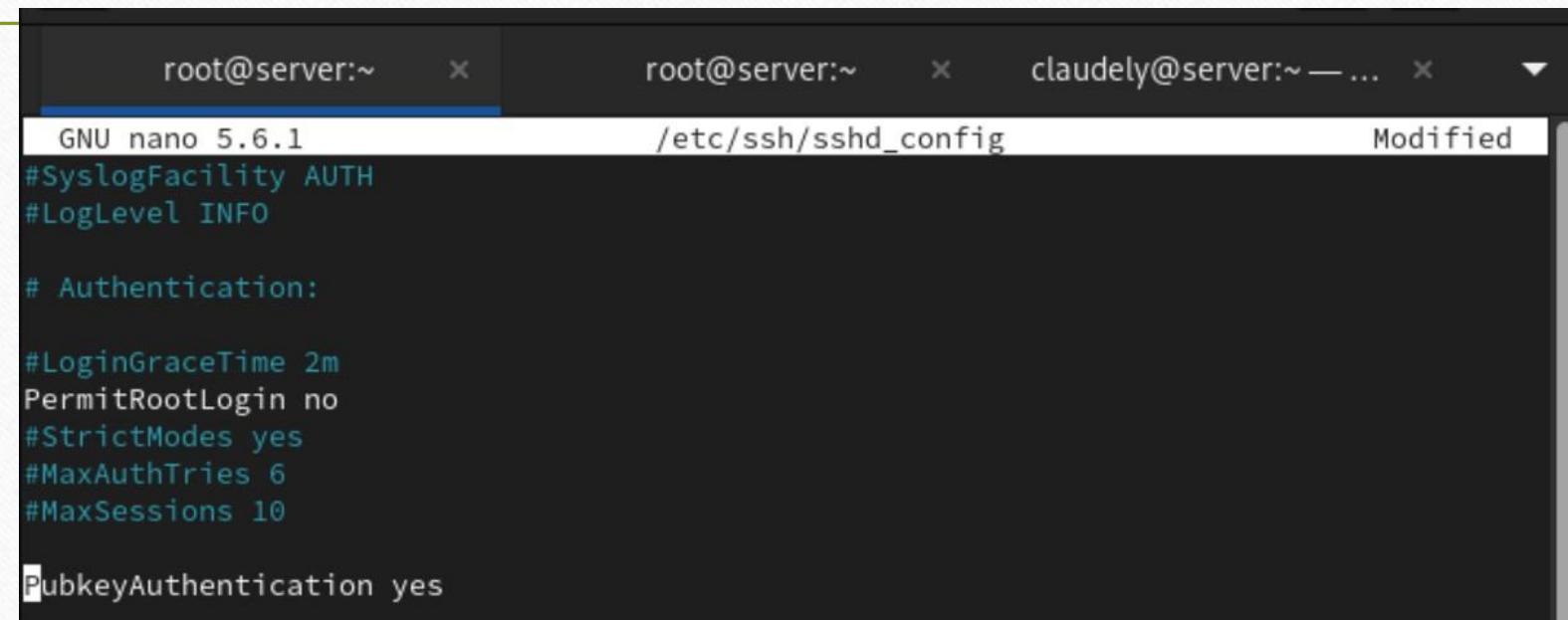
Рис. 3.3. Просмотр сообщения в терминале с мониторингом системных событий.

Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# semanage port -a -t ssh_port_t -p tcp 2022  
[root@server.claudely.net ~]#  
  
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# semanage port -a -t ssh_port_t -p tcp 2022  
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# firewall-cmd --add-port=2022/tcp  
success  
[root@server.claudely.net ~]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@server.claudely.net ~]#
```

Рис. 3.4. Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

Настройка удалённого доступа по SSH по ключу



The screenshot shows a terminal window with three tabs. The active tab is titled 'root@server:~' and contains the following configuration for the `/etc/ssh/sshd_config` file:

```
GNU nano 5.6.1
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

PubkeyAuthentication yes
```

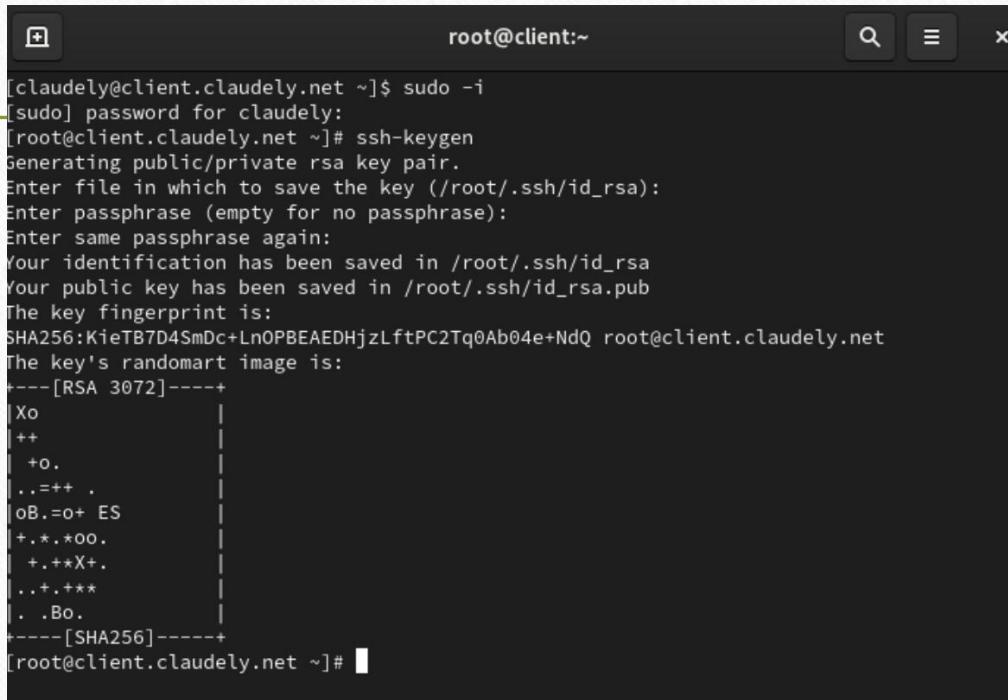
Рис. 4.1. Настройка параметра на сервере в конфигурационном файле `/etc/ssh/sshd_config`, разрешающего аутентификацию по ключу.

Настройка удалённого доступа по SSH по ключу

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 4.2. Перезапуск sshd.

Настройка удалённого доступа по SSH по ключу

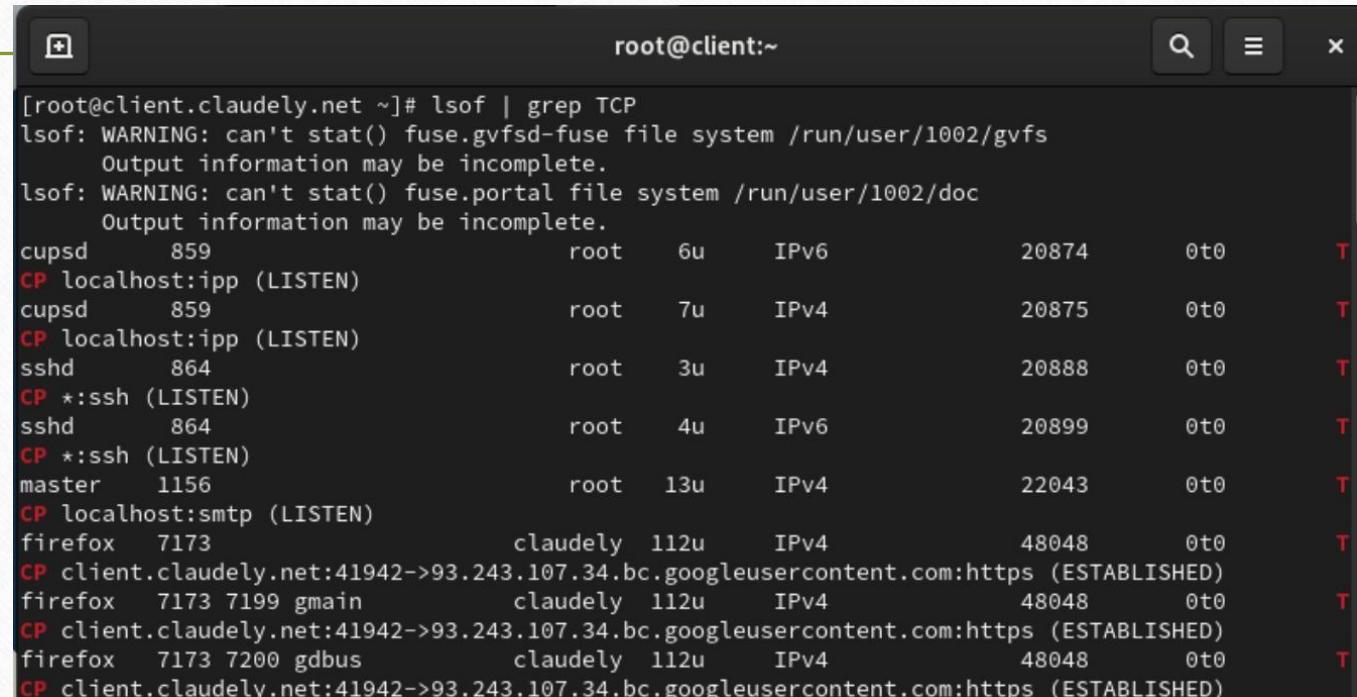


The screenshot shows a terminal window titled "root@client:~". The user is running the command "ssh-keygen" to generate an RSA key pair. The process involves entering a passphrase and saving the keys to the default location. The terminal also displays the SHA256 fingerprint and a randomart image.

```
[claudely@client.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@client.claudely.net ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:KieTB7D4SmDc+LnOPBEAEDHjzLftPC2Tq0Ab04e+NdQ root@client.claudely.net
The key's randomart image is:
+---[RSA 3072]---+
|Xo
|++
|+o.
|..=++ .
|oB.=o+ ES
|+.**oo.
|.+**X+.
|..+.***
| .Bo.
+---[SHA256]---+
[root@client.claudely.net ~]#
```

Рис. 4.3. Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.

Организация туннелей SSH, перенаправление TCP-портов

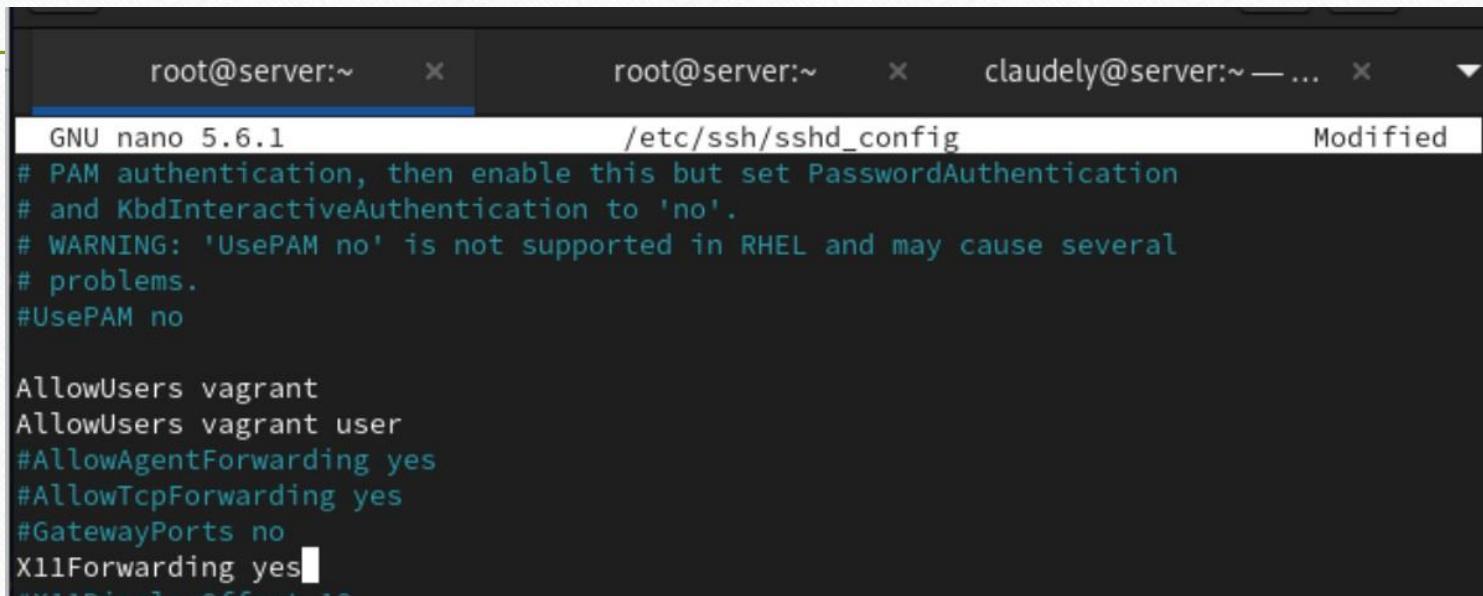


The screenshot shows a terminal window titled "root@client:~". The command "lsof | grep TCP" is run, displaying a list of processes using TCP connections. The output includes:

```
[root@client.claudely.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1002/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1002/doc
      Output information may be incomplete.
cupsd    859                  root   6u     IPv6            20874    0t0      T
CP localhost:ipp (LISTEN)
cupsd    859                  root   7u     IPv4            20875    0t0      T
CP localhost:ipp (LISTEN)
sshd     864                  root   3u     IPv4            20888    0t0      T
CP *:ssh (LISTEN)
sshd     864                  root   4u     IPv6            20899    0t0      T
CP *:ssh (LISTEN)
master   1156                 root  13u     IPv4            22043    0t0      T
CP localhost:smtp (LISTEN)
firefox  7173                claudely 112u     IPv4            48048    0t0      T
CP client.claudely.net:41942->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox  7173 7199 gmain       claudely 112u     IPv4            48048    0t0      T
CP client.claudely.net:41942->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox  7173 7200 gdbus       claudely 112u     IPv4            48048    0t0      T
CP client.claudely.net:41942->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
```

Рис. 5.1. Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.claudely.net на порт 8080 на локальной машине.

Запуск графических приложений через SSH (X11Forwarding)



The screenshot shows a terminal window with three tabs. The active tab is titled 'root@server:~' and contains the command 'GNU nano 5.6.1'. The content of the file is as follows:

```
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in RHEL and may cause several
# problems.
#UsePAM no

AllowUsers vagrant
AllowUsers vagrant user
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
```

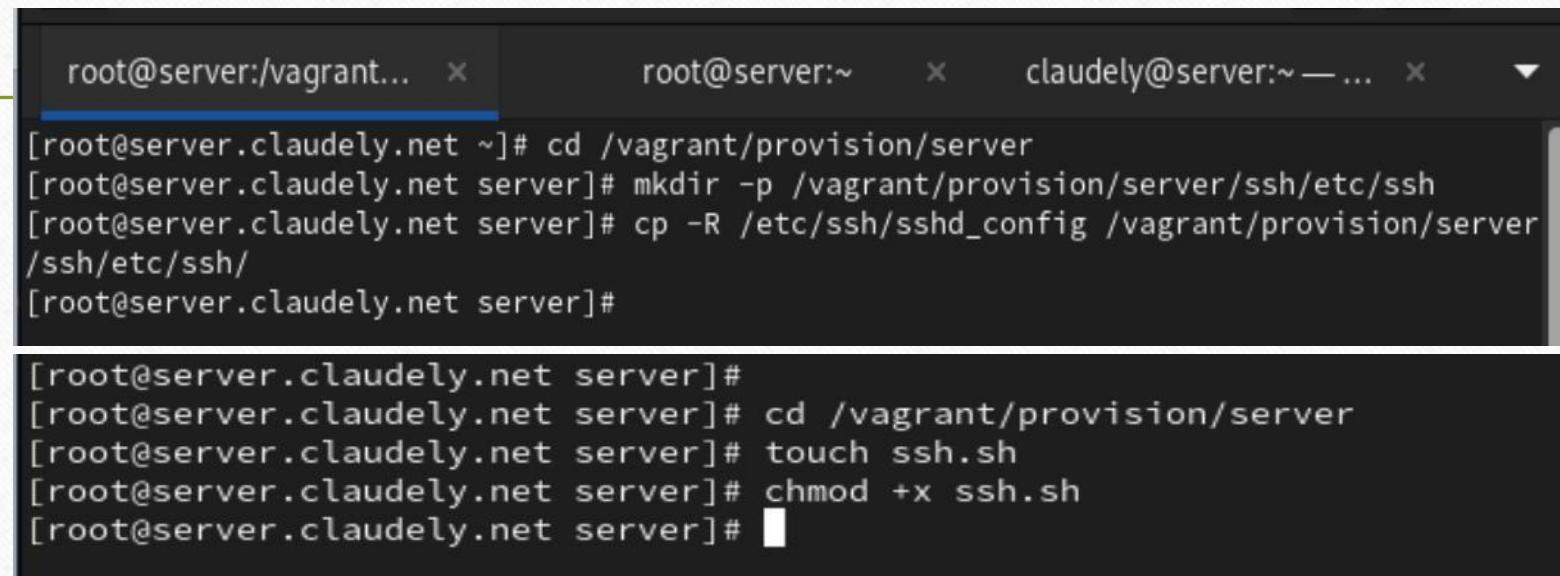
Рис. 7.1. Разрешение отображать на сервере в конфигурационном файле /etc/ssh/sshd_config на локальном клиентском компьютере графические интерфейсы X11.

Запуск графических приложений через SSH (X11Forwarding)

```
[root@server.claudely.net ~]# nano /etc/ssh/sshd_config
[root@server.claudely.net ~]# systemctl restart sshd
[root@server.claudely.net ~]#
```

Рис. 7.2. Перезапуск sshd.

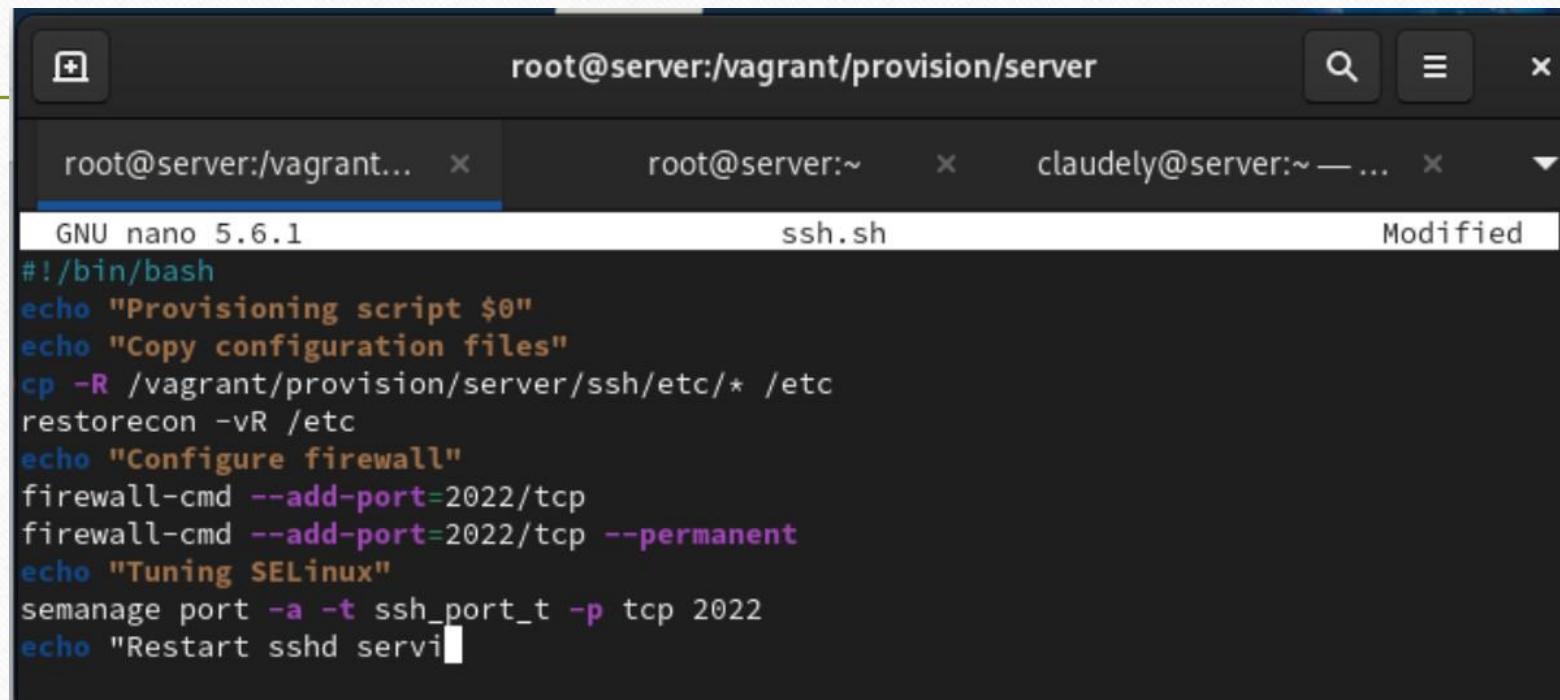
Внесение изменений в настройки внутреннего окружения виртуальной машины



```
root@server:vagrant... ~]# cd /vagrant/provision/server
[root@server.claudely.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.claudely.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.claudely.net server]#
[root@server.claudely.net server]# cd /vagrant/provision/server
[root@server.claudely.net server]# touch ssh.sh
[root@server.claudely.net server]# chmod +x ssh.sh
[root@server.claudely.net server]#
```

Рис. 8.1. Переход на виртуальной машине `server` в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `ssh`, в который поместили в соответствующие подкаталоги конфигурационный файл `sshd_config`. Создание в каталоге `/vagrant/provision/server` исполняемого файла `ssh.sh`.

Внесение изменений в настройки внутреннего окружения виртуальной машины



The screenshot shows a terminal window with three tabs at the top: 'root@server:/vagrant/provision/server' (active), 'root@server:~' (inactive), and 'claudely@server:~ — ...' (inactive). The main pane displays a file named 'ssh.sh' being edited with 'GNU nano 5.6.1'. The script contains the following code:

```
#!/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"
```

Рис. 8.2. Открытие файла на редактирование и написание в нём скрипта.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
type: "shell",
preserve_order: true,
path: "provision/server/firewall.sh"

server.vm.provision "server mail",
  type: "shell",
  preserve_order: true,
  path: "provision/server/mail.sh"
server.vm.provision "server ssh",
  type: "shell",
  preserve_order: true,
  path: "provision/server/ssh.sh"

server.vm.provider :virtualbox do |v|
```

Рис. 8.3. Редактирование конфигурационного файла Vagrantfile.

Вывод

В ходе выполнения лабораторной работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Спасибо за внимание!