

Bài tập tổng hợp cuối kỳ môn quản trị hệ thống

Kim Minh Thắng B2007210

Ngày 24 tháng 11 năm 2023

Mục lục

1	Cài đặt và cấu hình Server/Desktop	3
1.1	(10%) Sử dụng phần mềm VirtualBox cài đặt Server và Desktop:	3
1.2	(10%) Tạo các người dùng và nhóm người dùng	11
1.3	(10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server	16
1.4	(10%) Tạo và phân quyền cho thư mục <code>/data</code>	20
1.5	(5%) Cài đặt và cấu hình tường lửa trên Server	22

Danh sách hình vẽ

1	Sơ đồ hệ thống mạng của công ty Straw Hat	3
2	Cấu hình NAT Network QHTT	3
3	Số Core CPU cho Server	5
4	Dung lượng RAM cho Server	5
5	Dung lượng ổ cứng cho Server	6
6	Cấu hình mạng máy Server (1)	6
7	Cấu hình mạng máy Server (2)	7
8	Số Core CPU cho máy Desktop	8
9	Dung lượng RAM cho máy Desktop	8
10	Dung lượng ổ đĩa cho máy Desktop	9
11	Cấu hình mạng cho máy Desktop	9
12	Dừng tường lửa bằng cách sử dụng <code>systemctl stop firewalld</code>	10
13	Ngăn tường lửa tự khởi động lại bằng cách sử dụng <code>systemctl disable firewalld</code>	11
14	Tạo và đặt mật khẩu cho tài khoản luffy	12
15	Tạo và đặt mật khẩu cho các người dùng còn lại	13
16	Tạo nhóm bangiamdoc và thêm người dùng vào	14
17	Tạo các nhóm còn lại và thêm người dùng vào	15
18	Cấp quyền sudo cho user nami	16
19	Cài đặt và kích hoạt dịch vụ ssh	17

20	Cho phép nhóm bangiamdoc và user b2007210 có quyền điều khiển máy tính từ xa	18
21	Cấu hình cho phép truy cập dịch vụ ssh bằng private key	19
22	Tạo private key và public key	19
23	Đổi tên và phân quyền cho tập tin public key	20
24	Tạo và phân quyền cho thư mục /data	21
25	Cấu hình tường lửa trên Server	22

Danh sách bảng

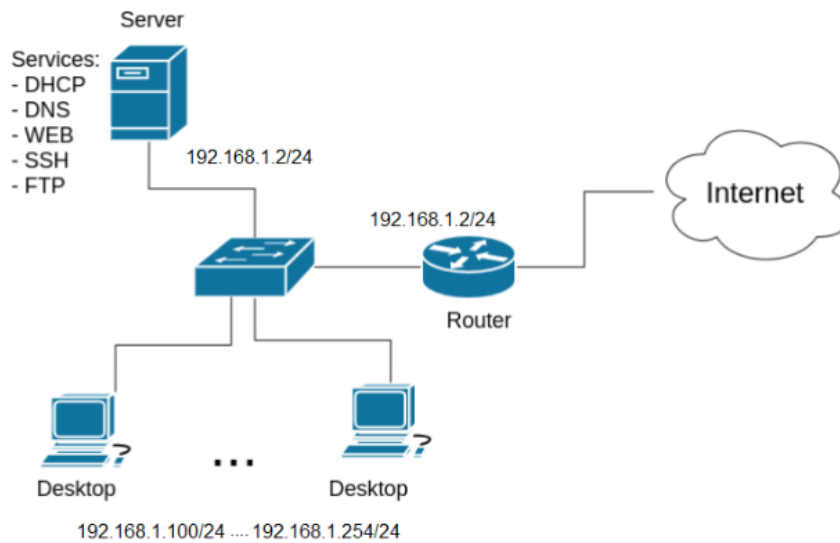
1	Cấu hình máy Server	4
2	Cấu hình máy Desktop	4
3	Danh sách người dùng và nhóm người dùng	11

Listings

1	Dùng tường lửa	10
2	Ngăn tường lửa tự khởi động lại	11
3	Tạo và đặt mật khẩu cho tài khoản luffy	12
4	Tạo và đặt mật khẩu cho các người dùng còn lại	13
5	Tạo nhóm bangiamdoc và thêm người dùng vào	14
6	Tạo các nhóm còn lại và thêm người dùng vào	15
7	Cấp quyền sudo cho user nami	16
8	Cài đặt và kích hoạt dịch vụ ssh	17
9	Tạo thư mục /data	21
10	Phân quyền cho ban giám đốc	21
11	Phân quyền cho trưởng phòng	21
12	Phân quyền cho nhân viên	22
13	Tạo zone mới có tên là services	22
14	Thêm các dịch vụ DNS, DHCP, SSH, Web, SAMBA vào zone services	22

Mô tả bài tập

Công ty Straw Hat chuyên kinh doanh hải sản có nhu cầu xây dựng hệ thống mạng cục bộ phục vụ cho công việc của công ty như sau:

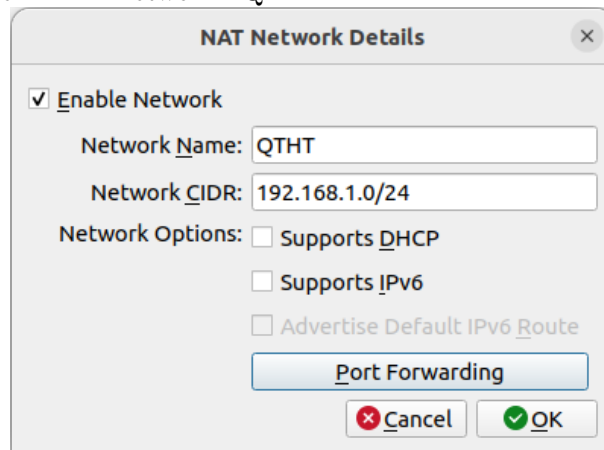


Hình 1: Sơ đồ hệ thống mạng của công ty Straw Hat

1 Cài đặt và cấu hình Server/Desktop

1.1 (10%) Sử dụng phần mềm VirtualBox cài đặt Server và Desktop:

- Tạo 1 NAT Network tên "QTHT" có địa chỉ mạng là 192.168.1.0/24. Tắt dịch vụ DHCP có sẵn trên NAT Network "QTHT".



Hình 2: Cấu hình NAT Network QTHT

Để tắt dịch vụ DHCP mặc định của NAT Network trong VirtualBox, ta bỏ tích tùy chọn "Supports DHCP".

- Tạo 2 máy ảo với thông tin như sau:

Bảng 1: Cấu hình máy Server

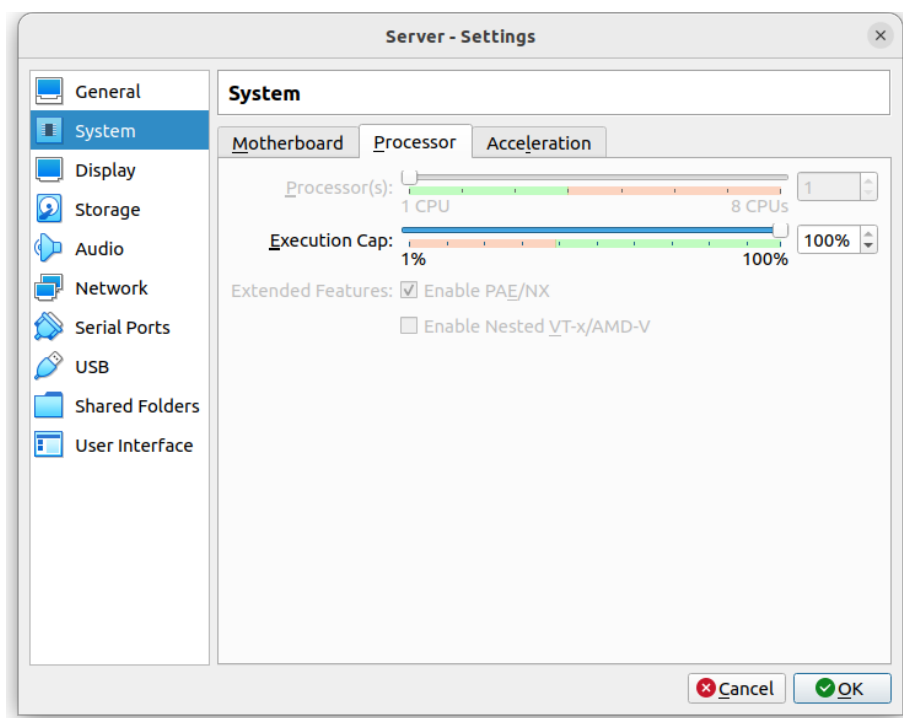
Hostname	Server
Hệ điều hành	CentOS 9
CPU / RAM / DISK	1core/2G/10G Hoặc tùy chỉnh theo cấu hình máy của sinh viên
Network	NAT Network Name: "QTHT"
IP	192.168.1.2
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS	192.168.1.1

Bảng 2: Cấu hình máy Desktop

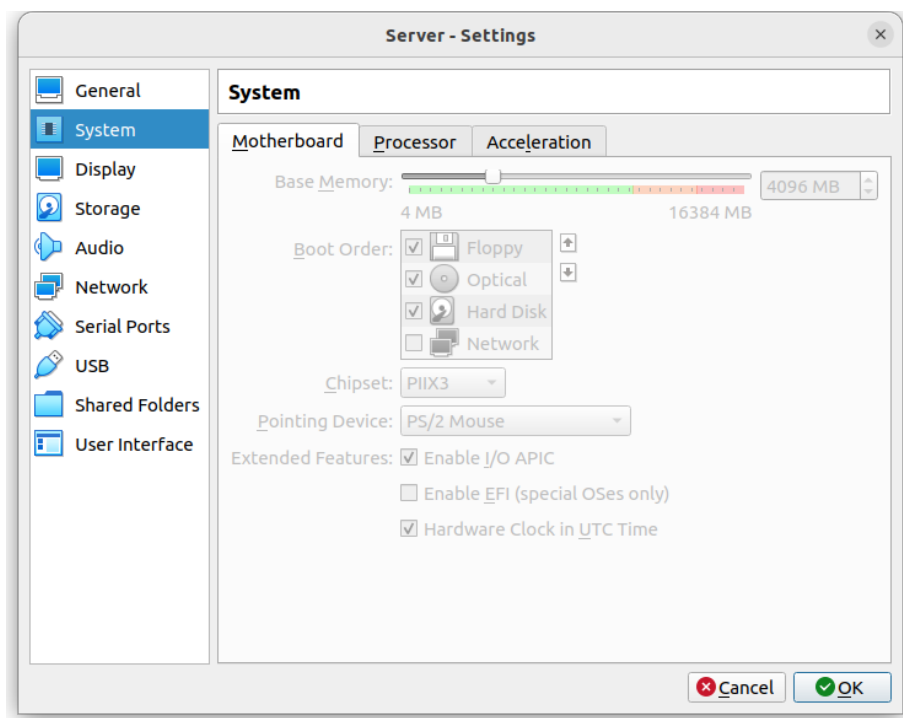
Hostname	Desktop
Hệ điều hành	Lubuntu 22.04, hoặc bất kỳ hệ điều hành khác
CPU / RAM / DISK	1core/2G/10G Hoặc tùy chỉnh theo cấu hình máy của sinh viên
Network	NAT Network Name: "QTHT"
IP Subnet mask Gateway DNS	Cấu hình tự động sử dụng dịch vụ DHCP

1. Server có cấu hình như sau:

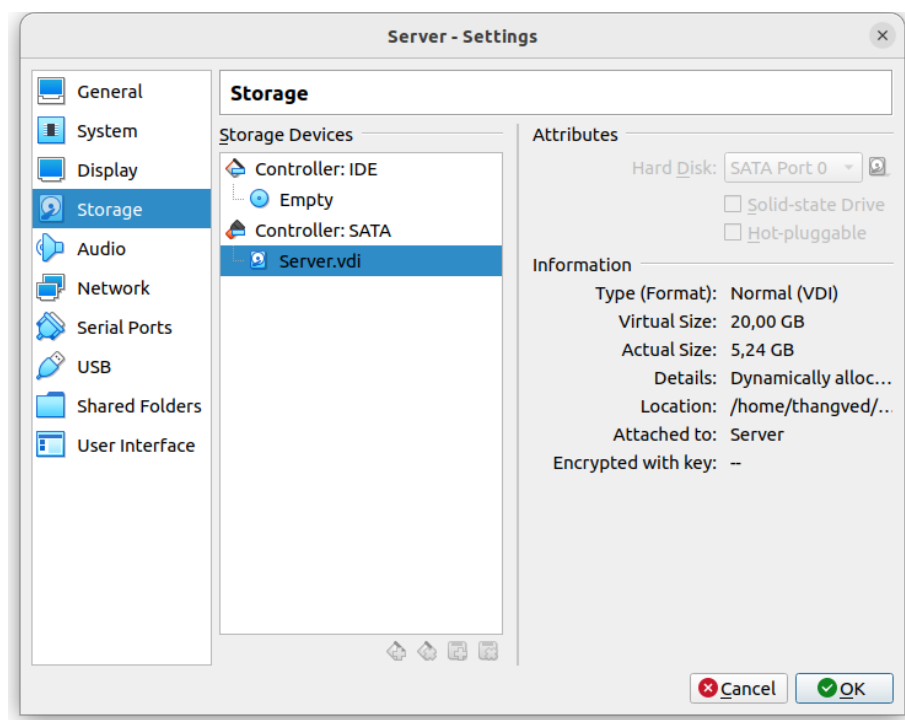
- Hệ điều hành: CentOS 9
- CPU: 1 Core (*Hình 3*)
- Ram: 4GB (*Hình 4*)
- Disk: 20GB (*Hình 5*)
- Network: NAT Network "QTHT" (*Hình 6*)
- IPv4: 192.168.1.2 (*Hình 7*)
- Subnet mask: 255.255.255.0 (*Hình 7*)
- Gateway: 192.168.1.1 (*Hình 7*)
- DNS: 192.168.1.1 (*Hình 7*)



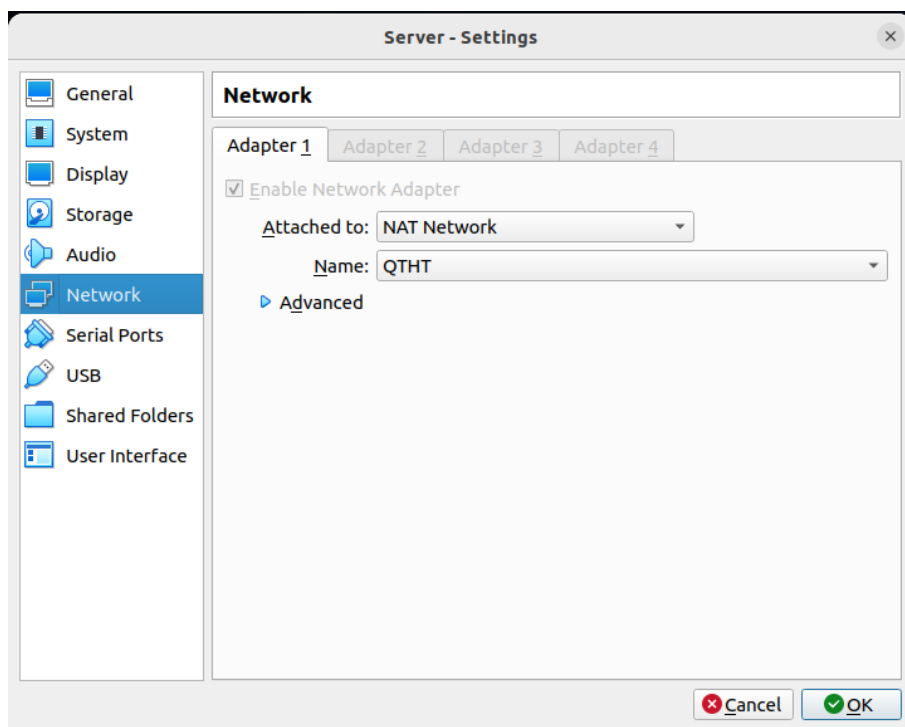
Hình 3: Số Core CPU cho Server



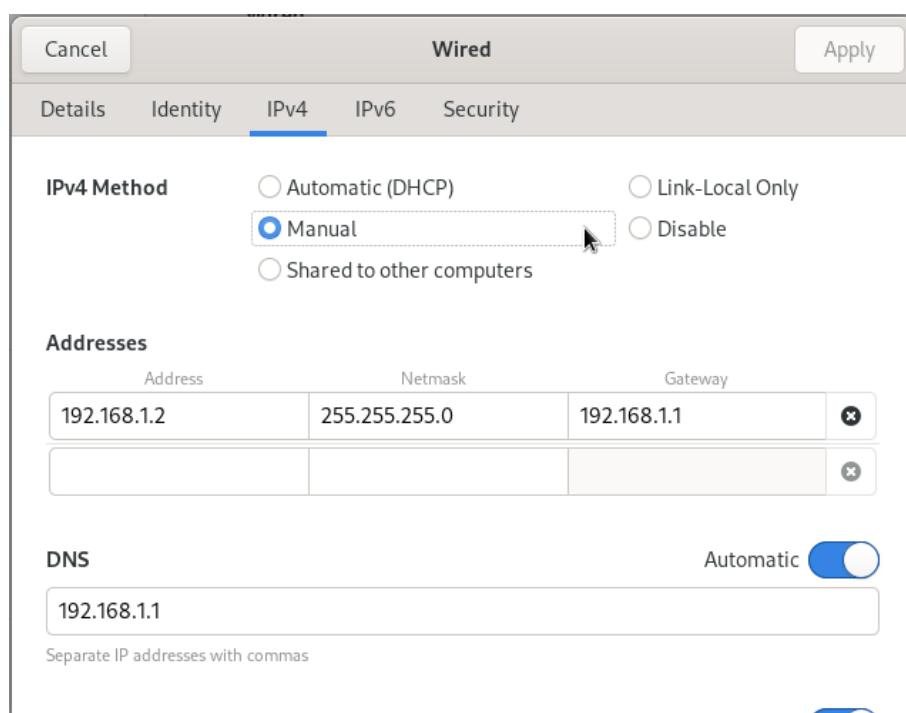
Hình 4: Dung lượng RAM cho Server



Hình 5: Dung lượng ổ cứng cho Server



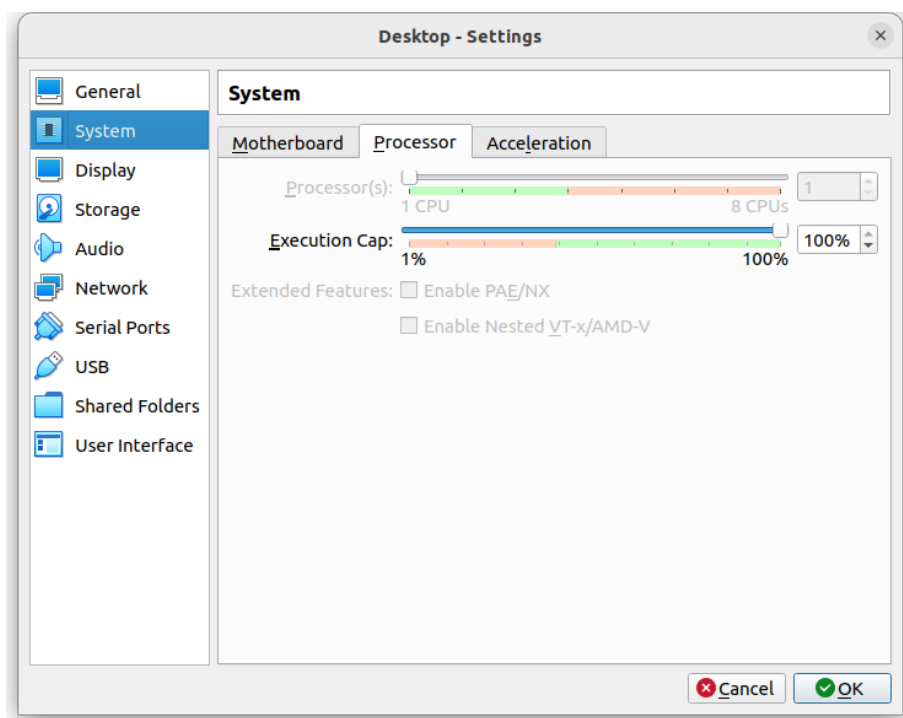
Hình 6: Cấu hình mạng máy Server (1)



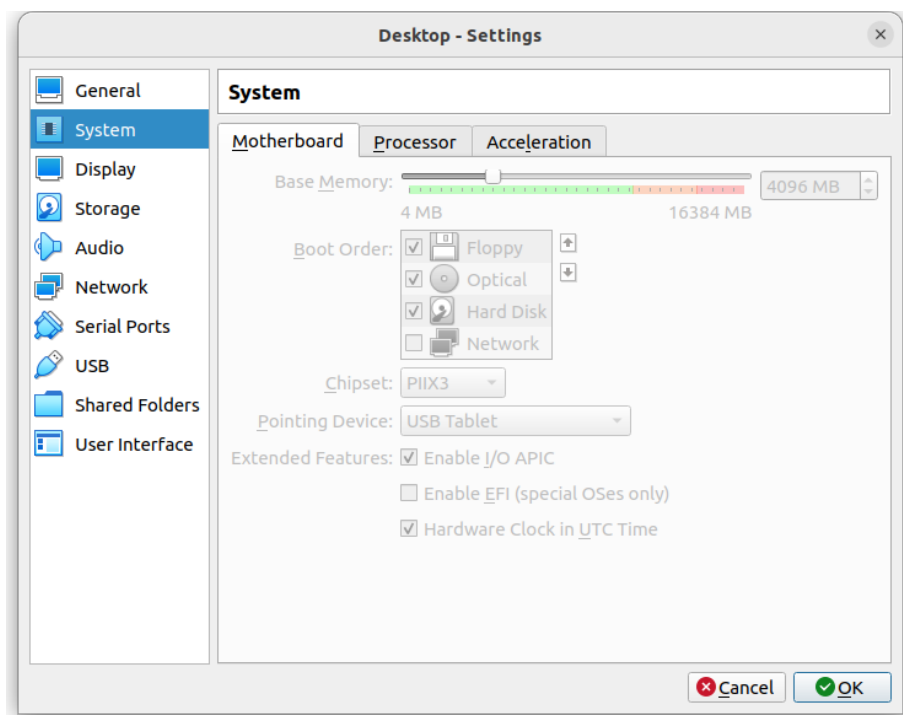
Hình 7: Cấu hình mạng máy Server (2)

2. Máy Desktop có cấu hình như sau:

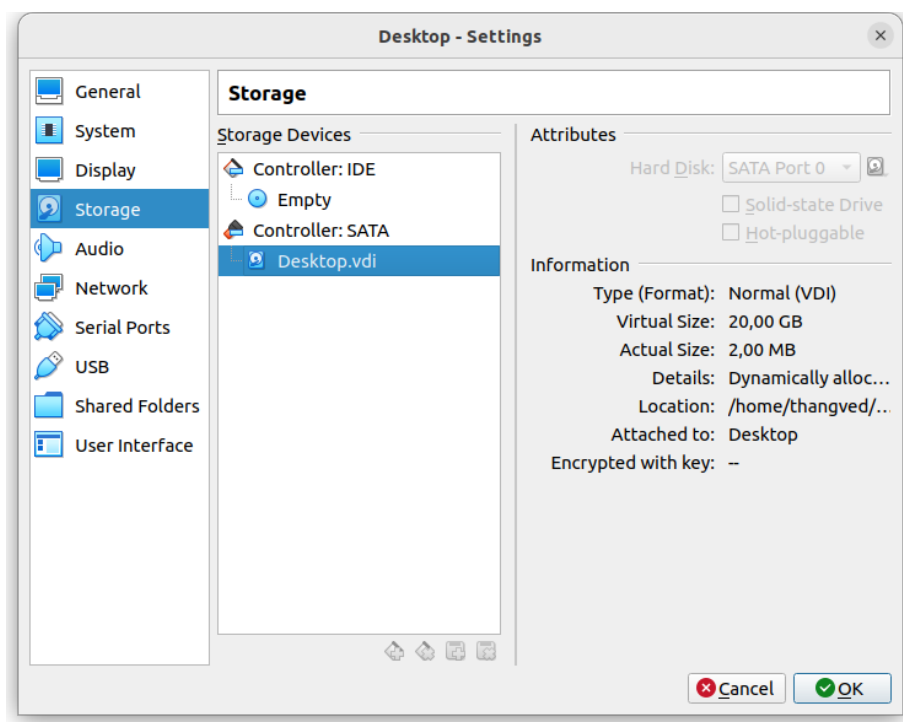
- Hệ điều hành: Lubuntu 22.04.3 LTS (Jammy Jellyfish)
- CPU: 1 Core (Hình 8)
- Ram: 4GB (Hình 9)
- Disk: 20GB (Hình 10)
- Network: NAT Network "QTHT" (Hình 11)



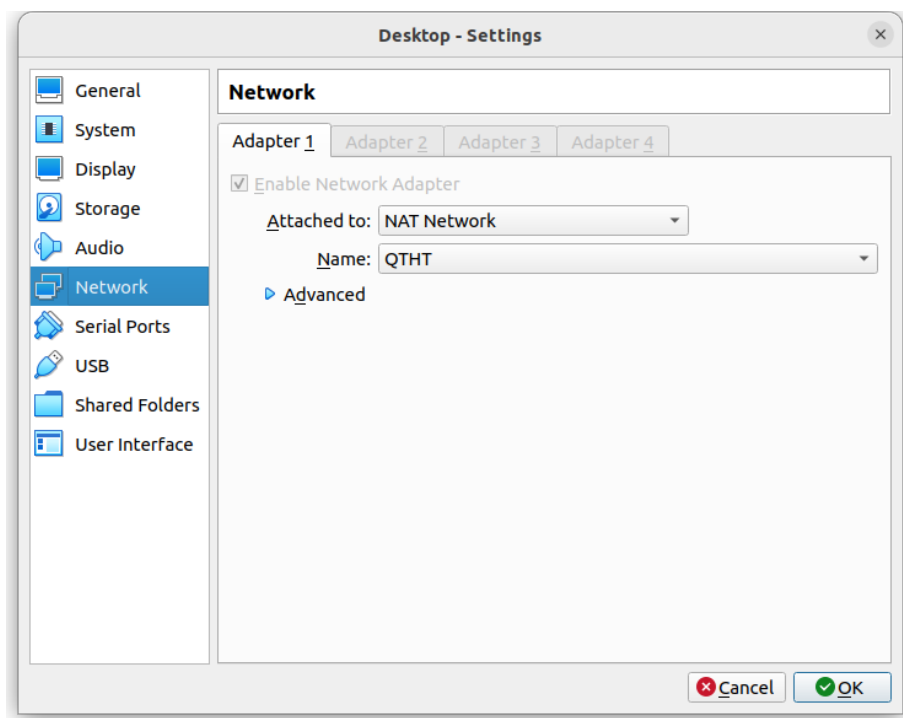
Hình 8: Số Core CPU cho máy Desktop



Hình 9: Dung lượng RAM cho máy Desktop

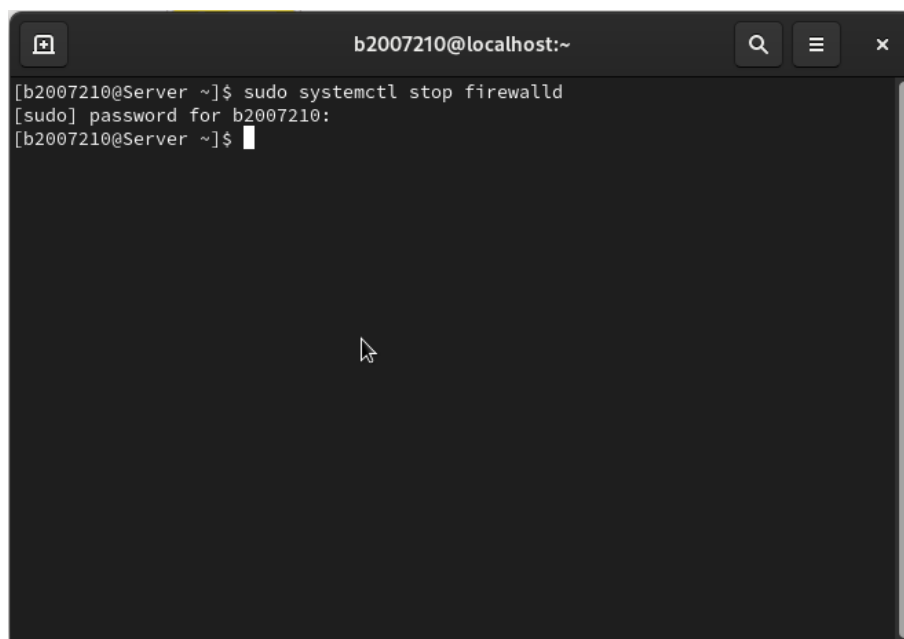


Hình 10: Dung lượng ổ đĩa cho máy Desktop



Hình 11: Cấu hình mạng cho máy Desktop

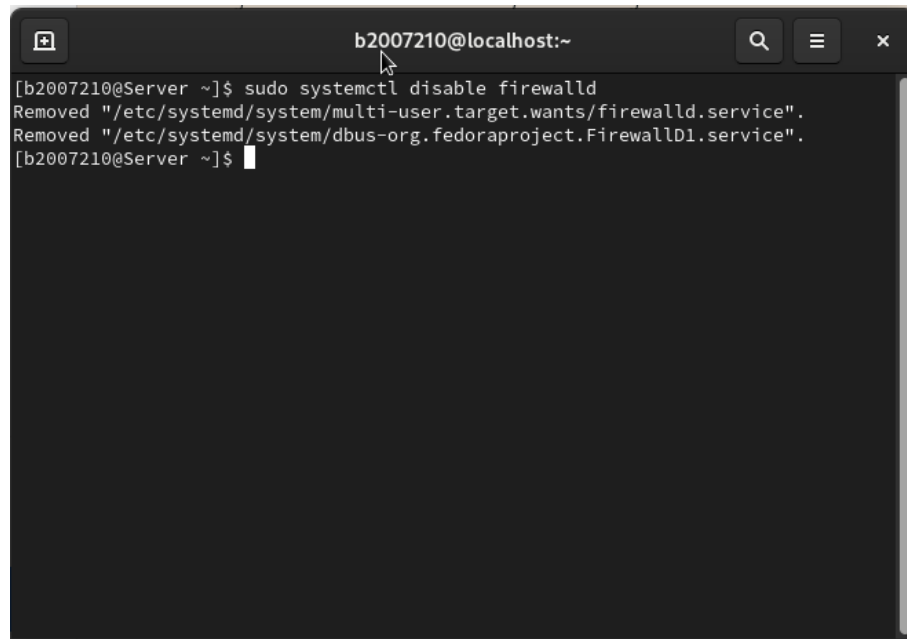
- Trong quá trình cài hệ điều hành CentOS 9, tạo 1 tài khoản với username là <Mã số sinh viên>; firstname và lastname là họ tên của sinh viên. Cấp quyền quản trị (sudo) cho tài khoản. Sử dụng tài khoản vừa tạo để thực hiện bài tập tổng hợp (không dùng tài khoản root).
- Tắt dịch vụ tường lửa trên Server.
Để tắt tường lửa ta có thể sử dụng lệnh **systemctl** hoặc **service**. Ở đây ta sẽ sử dụng lệnh **systemctl** để làm việc này (*xem Hình 12*) và *Hình 13*.



Hình 12: Dừng tường lửa bằng cách sử dụng **systemctl stop firewalld**

```
1 sudo systemctl stop firewalld
```

Listing 1: Dừng tường lửa



Hình 13: Ngăn tường lửa tự khởi động lại bằng cách sử dụng `systemctl disable firewalld`

```
1 sudo systemctl disable firewalld
```

Listing 2: Ngăn tường lửa tự khởi động lại

Lệnh `systemctl stop firewalld` (Hình 12) dùng để dừng tường lửa ngay lập tức và lệnh `systemctl disable firewalld` (Hình 13) sẽ ngăn việc tường lửa tự khởi động lại sau khi reboot.

1.2 (10%) Tạo các người dùng và nhóm người dùng

Để quản lý các bộ phận và người dùng trong công ty, hãy tạo các nhóm người dùng (group) và người dùng (user) trên server như sau. Cấp quyền sudo cho người dùng Nami.

Bảng 3: Danh sách người dùng và nhóm người dùng

STT	Họ tên	Nhóm	Username	Pasword	Mô tả
1	Luffy	bangiamdoc	luffy	luffy	Giám đốc
2	Nami	bangiamdoc	nami	nami	Phó giám đốc
3	Zoro	banhang	zoro	zoro	Trưởng phòng
4	Usopp	banhang	usopp	usopp	Nhân viên
5	Robin	banhang	robin	robin	Nhân viên
6	Sanji	hanhchinh	sanji	sanji	Trưởng phòng
7	Chopper	hanhchinh	chopper	chopper	Nhân viên

Để tạo người dùng trên CentOS, ta có thể sử dụng lệnh `useradd <username>` và dùng lệnh `passwd <username>` để đặt mật khẩu cho user. Sau đây là ví dụ về việc tạo tài khoản và đặt mật khẩu cho tài khoản luffy (*Hình 14*).

A screenshot of a terminal window titled 'b2007210@firewall:~'. The terminal shows the following commands and output: [b2007210@Server ~]\$ sudo useradd luffy, [b2007210@Server ~]\$ sudo passwd luffy. The output includes: Changing password for user luffy., New password:, BAD PASSWORD: The password is shorter than 8 characters, Retype new password:, passwd: all authentication tokens updated successfully., and [b2007210@Server ~]\$ followed by a cursor. The terminal window has a dark background and standard window controls at the top.

```
b2007210@firewall:~
[b2007210@Server ~]$ sudo useradd luffy
[b2007210@Server ~]$ sudo passwd luffy

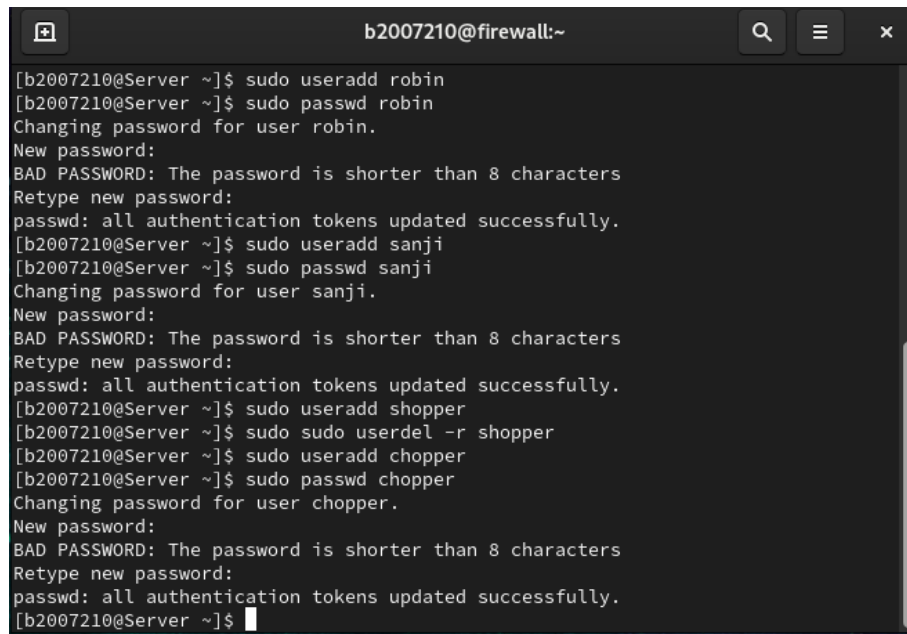
Changing password for user luffy.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[b2007210@Server ~]$
```

Hình 14: Tạo và đặt mật khẩu cho tài khoản luffy

```
1 sudo useradd luffy
2 sudo passwd luffy
```

Listing 3: Tạo và đặt mật khẩu cho tài khoản luffy

Tương tự như thế với các tài khoản còn lại (*Hình 15*).



```
b2007210@firewall:~  
[b2007210@Server ~]$ sudo useradd robin  
[b2007210@Server ~]$ sudo passwd robin  
Changing password for user robin.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[b2007210@Server ~]$ sudo useradd sanji  
[b2007210@Server ~]$ sudo passwd sanji  
Changing password for user sanji.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[b2007210@Server ~]$ sudo useradd shopper  
[b2007210@Server ~]$ sudo sudo userdel -r shopper  
[b2007210@Server ~]$ sudo useradd chopper  
[b2007210@Server ~]$ sudo passwd chopper  
Changing password for user chopper.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[b2007210@Server ~]$
```

Hình 15: Tạo và đặt mật khẩu cho các người dùng còn lại

```
1 sudo useradd nami  
2 sudo passwd nami  
3 sudo useradd zoro  
4 sudo passwd zoro  
5 sudo useradd usopp  
6 sudo passwd usopp  
7 sudo useradd robin  
8 sudo passwd robin  
9 sudo useradd sanji  
10 sudo passwd sanji  
11 sudo useradd chopper  
12 sudo passwd chopper
```

Listing 4: Tạo và đặt mật khẩu cho các người dùng còn lại

Để thêm nhóm người dùng, ta sử dụng lệnh `groupadd <group-name>` và thêm người dùng vào nhóm bằng lệnh `usermod -aG <group-name> <username>`. Sau đây là ví dụ tạo nhóm `bangiamdoc` và thêm `luffy` và `nami` vào nhóm này (Hình 16).

A terminal window titled 'b2007210@firewall:~' with search, menu, and close buttons. It shows three commands being executed: 'sudo groupadd bangiamdoc', 'sudo usermod -aG bangiamdoc luffy', and 'sudo usermod -aG bangiamdoc nami'. The prompt returns to the shell after each command.

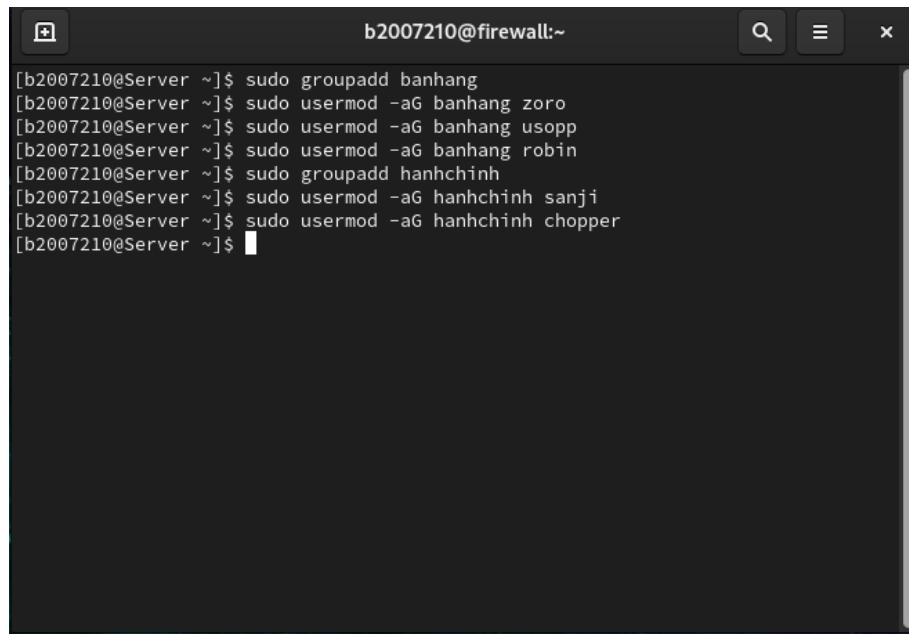
```
b2007210@firewall:~  
[b2007210@Server ~]$ sudo groupadd bangiamdoc  
[b2007210@Server ~]$ sudo usermod -aG bangiamdoc luffy  
[b2007210@Server ~]$ sudo usermod -aG bangiamdoc nami  
[b2007210@Server ~]$
```

Hình 16: Tạo nhóm bangiamdoc và thêm người dùng vào

```
1 sudo groupadd bangiamdoc  
2 sudo usermod -aG bangiamdoc luffy  
3 sudo usermod -aG bangiamdoc nami
```

Listing 5: Tạo nhóm bangiamdoc và thêm người dùng vào

Thực hiện tương tự với các nhóm còn lại (*Hình 17*).



Hình 17: Tạo các nhóm còn lại và thêm người dùng vào

```
1 sudo groupadd banhang
2 sudo usermod -aG banhang zoro
3 sudo usermod -aG banhang usopp
4 sudo usermod -aG banhang robin
5
6 sudo groupadd hanhchinh
7 sudo usermod -aG hanhchinh sanji
8 sudo usermod -aG hanhchinh chopper
```

Listing 6: Tạo các nhóm còn lại và thêm người dùng vào

Để cấp quyền sudo cho một user, ta chỉ cần thêm user đó vào nhóm **sudo** hoặc **wheel**. Trong trường hợp này, ta sẽ thêm vào nhóm **wheel**.



Hình 18: Cấp quyền sudo cho user nami

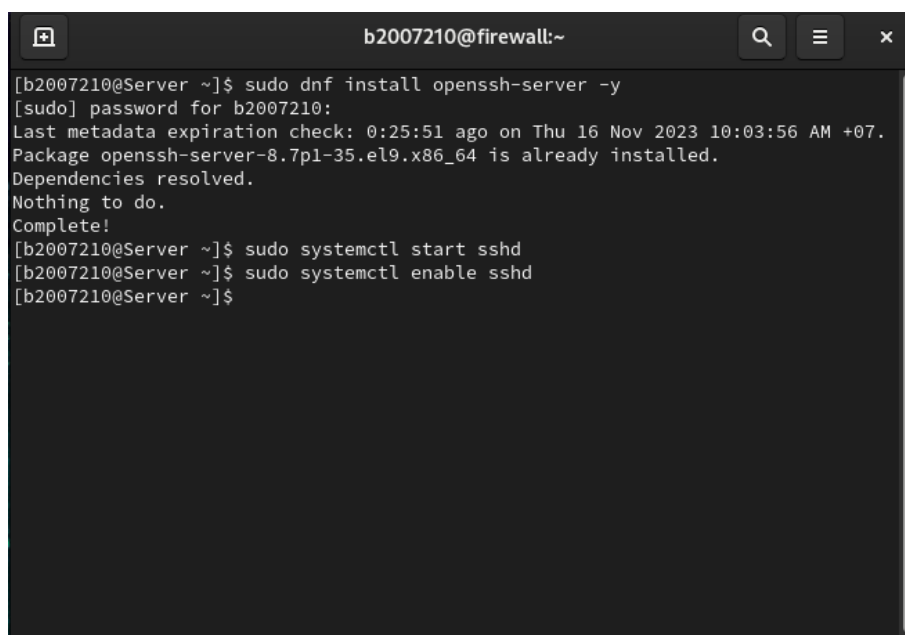
```
1 sudo usermod -aG wheel nami
```

Listing 7: Cấp quyền sudo cho user nami

1.3 (10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server

- Chỉ có thành viên ban giám đốc và tài khoản <Mã số sinh viên> mới có quyền điều khiển từ xa Server. Tài khoản root không được nối kết tới server từ xa.
- Chỉ cho phép chứng thực bằng private key, không cho phép chứng thực bằng password. Tạo private/public key cho người dùng <Mã số sinh viên> để có thể SSH tới server.

1. Cài đặt dịch vụ ssh

A terminal window titled 'b2007210@firewall:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

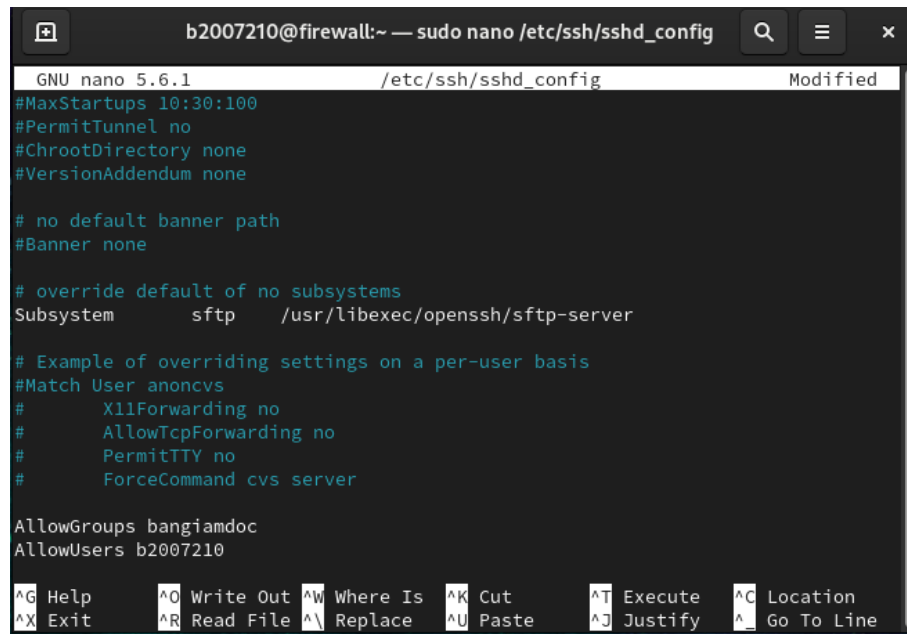
```
[b2007210@Server ~]$ sudo dnf install openssh-server -y
[sudo] password for b2007210:
Last metadata expiration check: 0:25:51 ago on Thu 16 Nov 2023 10:03:56 AM +07.
Package openssh-server-8.7p1-35.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[b2007210@Server ~]$ sudo systemctl start sshd
[b2007210@Server ~]$ sudo systemctl enable sshd
[b2007210@Server ~]$
```

Hình 19: Cài đặt và kích hoạt dịch vụ ssh

```
1 sudo dnf install openssh-server
2 sudo systemctl enable sshd
3 sudo systemctl start sshd
```

Listing 8: Cài đặt và kích hoạt dịch vụ ssh

2. Cấu hình chỉ cho phép thành viên trong ban giám đốc và tài khoản b2007210 mới có quyền điều khiển từ xa
Để cấu hình chỉ cho phép một nhóm người dùng hoặc người dùng có thể sử dụng dịch vụ ssh, ta sẽ cấu hình trong file `/etc/ssh/sshd_config` (Hình 20).



```
b2007210@firewall:~ — sudo nano /etc/ssh/sshd_config
GNU nano 5.6.1 /etc/ssh/sshd_config Modified
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server

AllowGroups bangiamdoc
AllowUsers b2007210

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Hình 20: Cho phép nhóm bangiamdoc và user b2007210 có quyền điều khiển máy tính từ xa

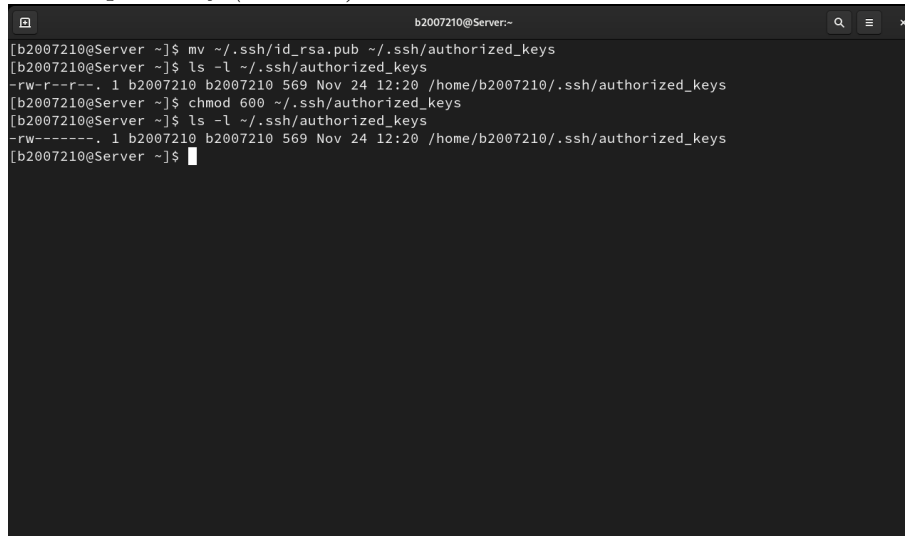
- AllowGroups bangiamdoc: Cho phép nhóm bangiamdoc sử dụng dịch vụ ssh.
- AllowUsers b2007210: Cho phép user b2007210 sử dụng dịch vụ ssh.

Ta cần khởi động lại dịch vụ ssh để áp dụng những thay đổi này (dùng lệnh `systemctl restart sshd`).

3. Chỉ cho phép chứng thực bằng private key

Để cấu hình chỉ cho phép chứng thực bằng private key, ta sẽ cấu hình trong file `/etc/ssh/sshd_config` (Hình 21).

quyền cho tập tin này (*Hình 23*).



```
b2007210@Server:~  
[b2007210@Server ~]$ mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys  
[b2007210@Server ~]$ ls -l ~/.ssh/authorized_keys  
-rw-r--r--. 1 b2007210 b2007210 569 Nov 24 12:20 /home/b2007210/.ssh/authorized_keys  
[b2007210@Server ~]$ chmod 600 ~/.ssh/authorized_keys  
[b2007210@Server ~]$ ls -l ~/.ssh/authorized_keys  
-rw-----. 1 b2007210 b2007210 569 Nov 24 12:20 /home/b2007210/.ssh/authorized_keys  
[b2007210@Server ~]$
```

Hình 23: Đổi tên và phân quyền cho tập tin public key

- `mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys`: Đổi tên tập tin public key thành `authorized_keys`.
- `chmod 600 ~/.ssh/authorized_keys`: Cho phép chủ sở hữu đọc và ghi vào tập tin `authorized_keys`.

1.4 (10%) Tạo và phân quyền cho thư mục /data

Tạo thư mục /data trên server và phân quyền sao cho thành viên ban giám đốc có toàn quyền (read, write và execute), các trưởng phòng có quyền read và execute, các nhân viên không có bất cứ quyền gì. Ngoài ra chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên tập tin trong thư mục /data.

Để tạo và phân quyền cho thư mục /data, ta thực hiện theo các bước như *Hình 24*.

```
b2007210@Server:~  
[b2007210@Server ~]$ sudo mkdir /data  
[b2007210@Server ~]$ sudo setfacl -m g:bangiamdoc:rwx /data  
[b2007210@Server ~]$ sudo groupadd truongphong  
[b2007210@Server ~]$ sudo usermod -aG truongphong zoro  
[b2007210@Server ~]$ sudo usermod -aG truongphong sanji  
[b2007210@Server ~]$ sudo setfacl -m g:truongphong:r-x /data  
[b2007210@Server ~]$ sudo setfacl -m other:--- /data  
[b2007210@Server ~]$ sudo chmod +t /data  
[b2007210@Server ~]$ sudo getfacl /data  
getfacl: Removing leading '/' from absolute path names  
# file: data  
# owner: root  
# group: root  
# flags: --t  
user::rwx  
group::r-x  
group:bangiamdoc:rwx  
group:truongphong:r-x  
mask::rwx  
other:---  
[b2007210@Server ~]$
```

Hình 24: Tạo và phân quyền cho thư mục /data

Cụ thể như sau:

1. Tạo thư mục /data.

```
1 sudo mkdir /data
```

Listing 9: Tạo thư mục /data

2. Ban giám đốc có toàn quyền (read, write, execute) trên thư mục /data

```
1 sudo setfacl -m g:bangiamdoc:rwx /data
```

Listing 10: Phân quyền cho ban giám đốc

3. Trưởng phòng có quyền read và execute trên thư mục /data

```
1 sudo groupadd truongphong  
2 sudo usermod -aG truongphong zoro  
3 sudo usermod -aG truongphong sanji  
4 sudo setfacl -m g:truongphong:rx /data
```

Listing 11: Phân quyền cho trưởng phòng

Dòng 1 Tạo nhóm **truongphong**.

Dòng 2 Thêm user **zoro** vào nhóm **truongphong**.

Dòng 3 Thêm user **sanji** vào nhóm **truongphong**.

Dòng 4 Phân quyền cho nhóm **truongphong** có quyền read và execute trên thư mục /data.

4. Nhân viên không có bất cứ quyền gì trên thư mục /data

```
1 sudo setfacl -m other:--- /data
```

Listing 12: Phân quyền cho nhân viên

- Chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên tập tin trong thư mục /data

```
1 sudo chmod +t /data
```

1.5 (5%) Cài đặt và cấu hình tường lửa trên Server

Có thể truy cập các dịch vụ DNS, DHCP, SSH, Web, SAMBA trên Server. Các dịch vụ khác KHÔNG truy cập được.

Ta sẽ cấu hình như *Hình 25*.

```

b2007210@Server:~$ sudo firewall-cmd --permanent --new-zone=services
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=dns
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=dhcp
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=ssh
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=http
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=samba
success
[b2007210@Server ~]$ sudo firewall-cmd --permanent --zone=services --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'services'.
success
[b2007210@Server ~]$ sudo systemctl restart firewalld
[b2007210@Server ~]$
  
```

Hình 25: Cấu hình tường lửa trên Server

Cụ thể như sau:

- Tạo một zone mới có tên là **services**

```
1 sudo firewall-cmd --permanent --new-zone=services
```

Listing 13: Tạo zone mới có tên là **services**

- Thêm các dịch vụ DNS, DHCP, SSH, Web, SAMBA vào zone **services**

```

1 sudo firewall-cmd --permanent --zone=services --add-service=dns
2 sudo firewall-cmd --permanent --zone=services --add-service=dhcp
3 sudo firewall-cmd --permanent --zone=services --add-service=ssh
4 sudo firewall-cmd --permanent --zone=services --add-service=http
5 sudo firewall-cmd --permanent --zone=services --add-service=samba
  
```

Listing 14: Thêm các dịch vụ DNS, DHCP, SSH, Web, SAMBA vào zone **services**

- Khởi động lại dịch vụ tường lửa để áp dụng những thay đổi này

```
1 sudo systemctl restart firewalld
```