

Bài tập tổng hợp cuối kỳ môn quản trị hệ thống

Kim Minh Thắng B2007210

Ngày 25 tháng 11 năm 2023

Mục lục

1	Cài đặt và cấu hình Server/Desktop	4
1.1	(10%) Sử dụng phần mềm VirtualBox cài đặt Server và Desktop:	4
1.2	(10%) Tạo các người dùng và nhóm người dùng	16
1.2.1	Tạo người dùng	17
1.2.2	Tạo nhóm người dùng và thêm người dùng vào nhóm	18
1.2.3	Cấp quyền sudo cho user nami	20
1.3	(10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server	21
1.3.1	Cài đặt dịch vụ ssh	22
1.3.2	Cấu hình chỉ cho phép thành viên trong ban giám đốc và tài khoản b2007210 mới có quyền điều khiển từ xa	22
1.3.3	Chỉ cho phép chứng thực bằng private key	23
1.4	(10%) Tạo và phân quyền cho thư mục /data	26
1.5	(5%) Cài đặt và cấu hình tường lửa trên Server	27
1.6	(5%) Cài đặt và cấu hình dịch vụ DHCP trên Server để cấu hình mạng tự động cho các máy Desktop trong nhánh mạng	28
1.6.1	Cài đặt dịch vụ DHCP	29
1.6.2	Cấu hình dịch vụ dhcp	29
1.6.3	Khởi động dịch vụ dhcp	31
1.6.4	Kiểm tra lại dịch vụ dhcp	31
1.7	(5%) Cài đặt và cấu hình dịch vụ máy chủ Web trên Server sử dụng Docker	32
1.7.1	Xây dựng trang web	33
1.7.2	Cấu hình Docker và nginx	33
1.7.3	Chạy trang web trên máy host	36
1.8	(5%) Cài đặt và cấu hình dịch vụ SAMBA trên Server	37

Danh sách hình vẽ

1	Sơ đồ hệ thống mạng của công ty Straw Hat	4
2	Cấu hình NAT Network QTHT	4
3	Số Core CPU cho Server	6

4	Dung lượng RAM cho Server	7
5	Dung lượng ổ cứng cho Server	8
6	Cấu hình mạng máy Server (1)	9
7	Cấu hình mạng máy Server (2)	10
8	Số Core CPU cho máy Desktop	11
9	Dung lượng RAM cho máy Desktop	12
10	Dung lượng ổ đĩa cho máy Desktop	13
11	Cấu hình mạng cho máy Desktop	14
12	Dừng tường lửa bằng cách sử dụng systemctl stop firewalld	15
13	Ngăn tường lửa tự khởi động lại bằng cách sử dụng systemctl disable firewalld	16
14	Tạo và đặt mật khẩu cho tài khoản luffy	17
15	Tạo và đặt mật khẩu cho các người dùng còn lại	18
16	Tạo nhóm bangiamdoc và thêm người dùng vào	19
17	Tạo các nhóm còn lại và thêm người dùng vào	20
18	Cấp quyền sudo cho user nami	21
19	Cài đặt và kích hoạt dịch vụ ssh	22
20	Cho phép nhóm bangiamdoc và user b2007210 có quyền điều khiển máy tính từ xa	23
21	Cấu hình cho phép truy cập dịch vụ ssh bằng private key	24
22	Tạo private key và public key	25
23	Đổi tên và phân quyền cho tập tin public key	25
24	Tạo và phân quyền cho thư mục /data	26
25	Cấu hình tường lửa trên Server	28
26	Cài đặt dhcp-server	29
27	Cấu hình dịch vụ dhcp	30
28	Khởi động dịch vụ dhcp	31
29	Truy cập vào internet bằng máy Desktop	32
30	Kiểm tra địa chỉ IP của máy desktop (192.168.1.100)	32
31	Cấu trúc trang web strawhat.com	33
32	Chạy trang web bằng lệnh docker compose up	36
33	Giao diện trang web strawhat.com	36
34	Chỉnh sửa file /etc/hosts để trỏ tên miền strawhat.com về địa chỉ localhost	37
35	Truy cập vào trang web từ server qua địa chỉ http://strawhat.com	37

Danh sách bảng

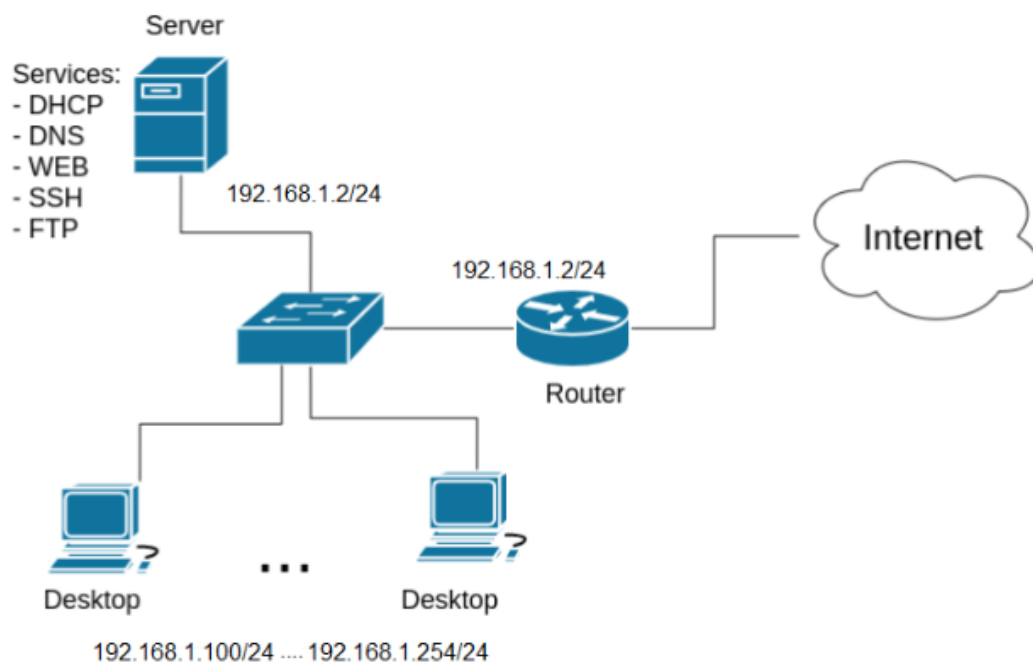
1	Cấu hình máy Server	5
2	Cấu hình máy Desktop	5
3	Danh sách người dùng và nhóm người dùng	16

Listings

1	Dùng tường lửa	15
2	Ngăn tường lửa tự khởi động lại	16
3	Tạo và đặt mật khẩu cho tài khoản luffy	17
4	Tạo và đặt mật khẩu cho các người dùng còn lại	18
5	Tạo nhóm bangiamdoc và thêm người dùng vào	19
6	Tạo các nhóm còn lại và thêm người dùng vào	20
7	Cấp quyền sudo cho user nami	21
8	Cài đặt và kích hoạt dịch vụ ssh	22
9	Đổi tên tập tin public key	26
10	Phân quyền cho tập tin authorized_keys	26
11	Tạo thư mục /data	26
12	Phân quyền cho ban giám đốc	27
13	Phân quyền cho trưởng phòng	27
14	Phân quyền cho nhân viên	27
15	Tạo zone mới có tên là services	28
16	Thêm các dịch vụ DNS, DHCP, SSH, Web, SAMBA vào zone services	28
17	Cài đặt dịch vụ DHCP	29
18	Nội dung file /etc/dhcp/dhcpd.conf	30
19	Khởi động dịch vụ dhcp	31
20	Nội dung file /Dockerfile	33
21	Nội dung file /docker-compose.up	35
22	Nội dung file /.nginx/nginx.conf	35

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:

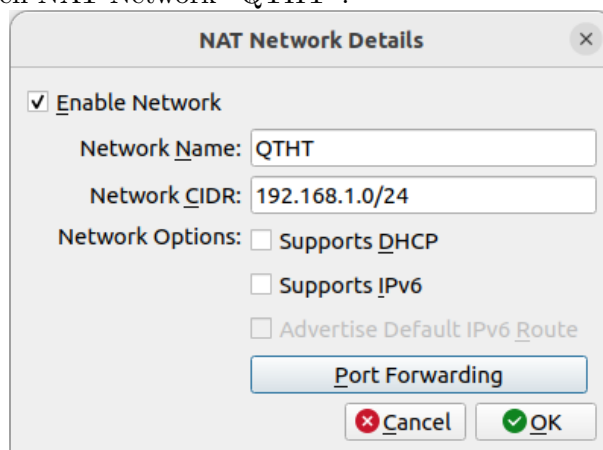


Hình 1: Sơ đồ hệ thống mạng của công ty Straw Hat

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

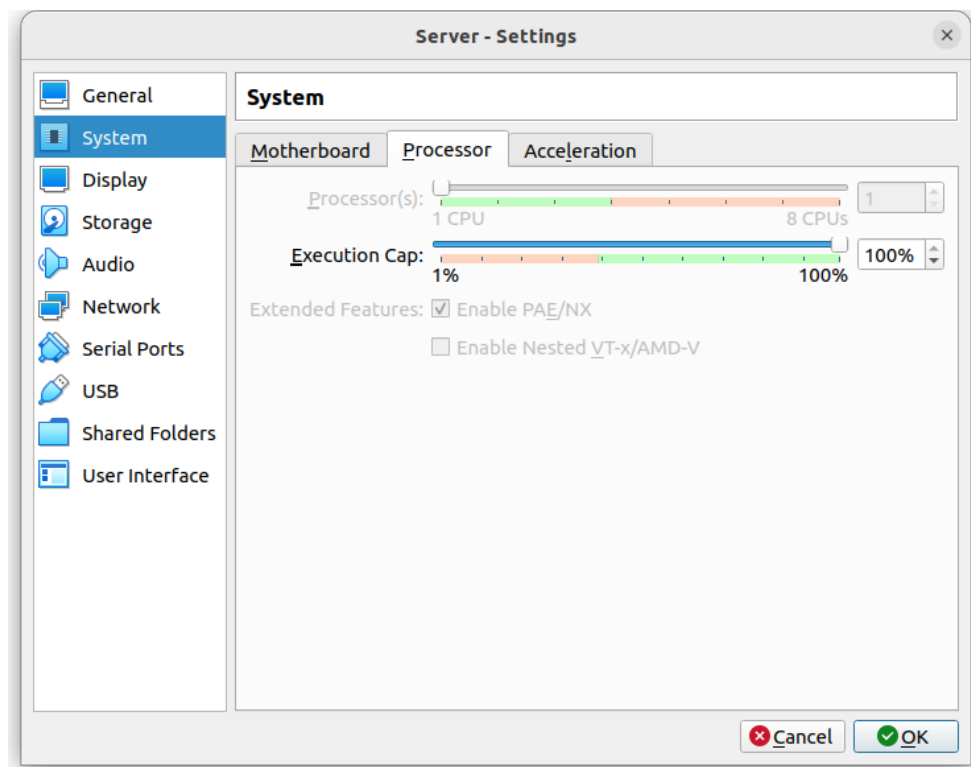
Hostname	Server
Hệ điều hành	CentOS 9
CPU / RAM / DISK	1core/2G/10G Hoặc tùy chỉnh theo cấu hình máy của sinh viên
Network	NAT Network Name: "QTHT"
IP	192.168.1.2
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS	192.168.1.1

Bảng 2: Cấu hình máy Desktop

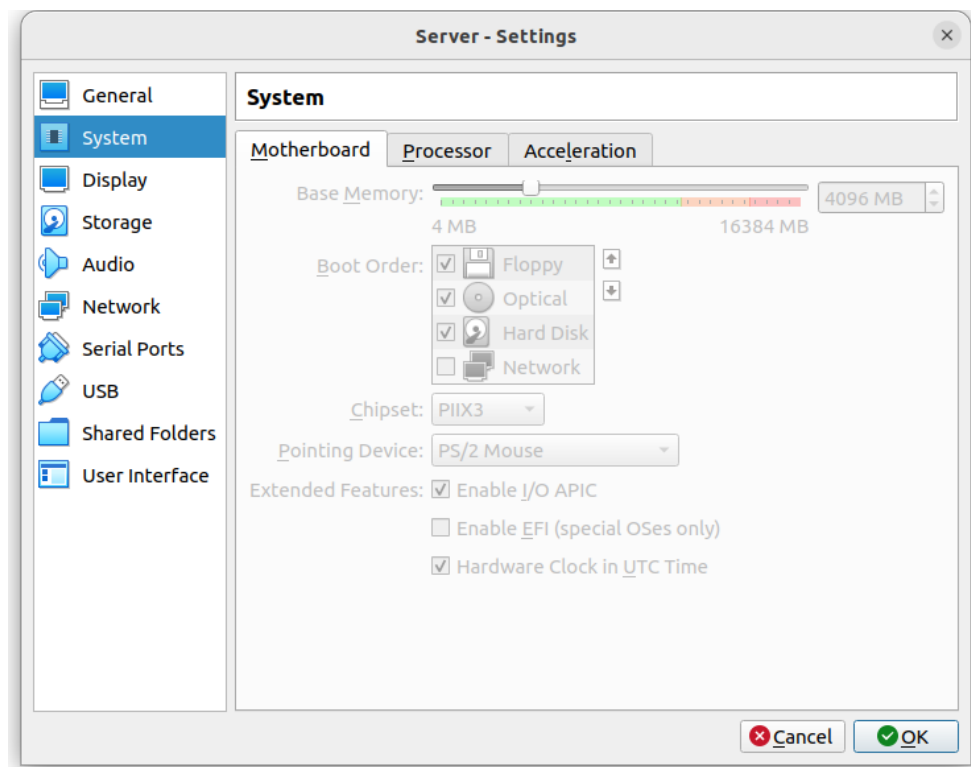
Hostname	Desktop
Hệ điều hành	Lubuntu 22.04, hoặc bất kỳ hệ điều hành khác
CPU / RAM / DISK	1core/2G/10G Hoặc tùy chỉnh theo cấu hình máy của sinh viên
Network	NAT Network Name: "QTHT"
IP	Cấu hình tự động sử dụng dịch vụ DHCP
Subnet mask	
Gateway	
DNS	

1. Server có cấu hình như sau:

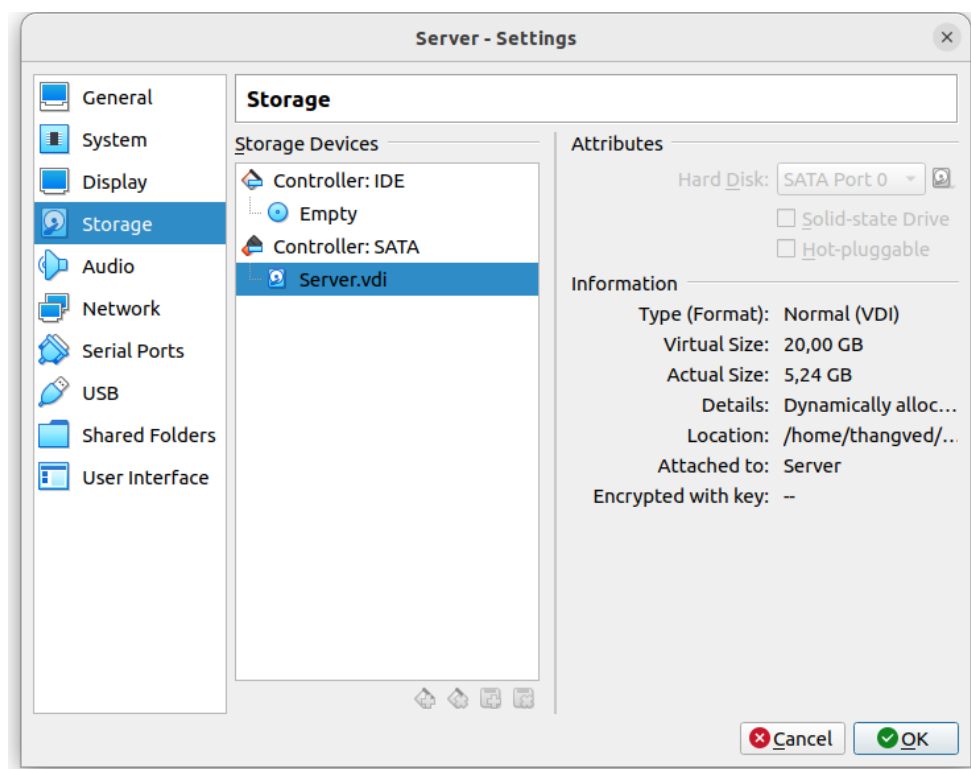
- Hệ điều hành: CentOS 9
- CPU: 1 Core (*Hình 3*)
- Ram: 4GB (*Hình 4*)
- Disk: 20GB (*Hình 5*)
- Network: NAT Network "QTHT" (*Hình 6*)
- IPv4: 192.168.1.2 (*Hình 7*)
- Subnet mask: 255.255.255.0 (*Hình 7*)
- Gateway: 192.168.1.1 (*Hình 7*)
- DNS: 192.168.1.1 (*Hình 7*)



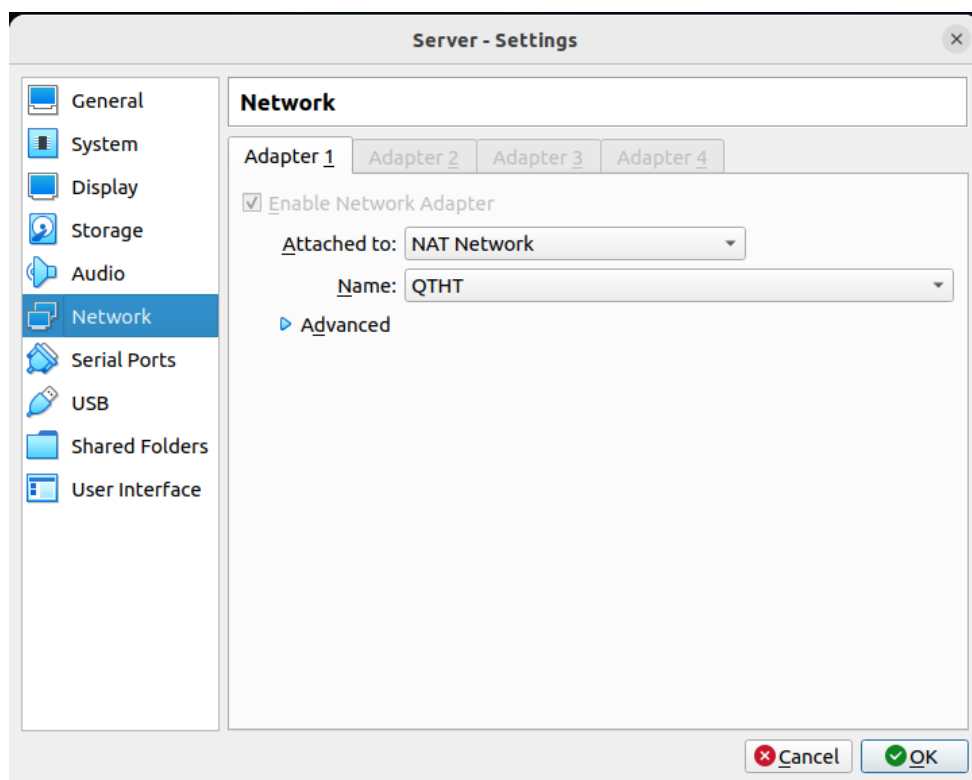
Hình 3: Số Core CPU cho Server



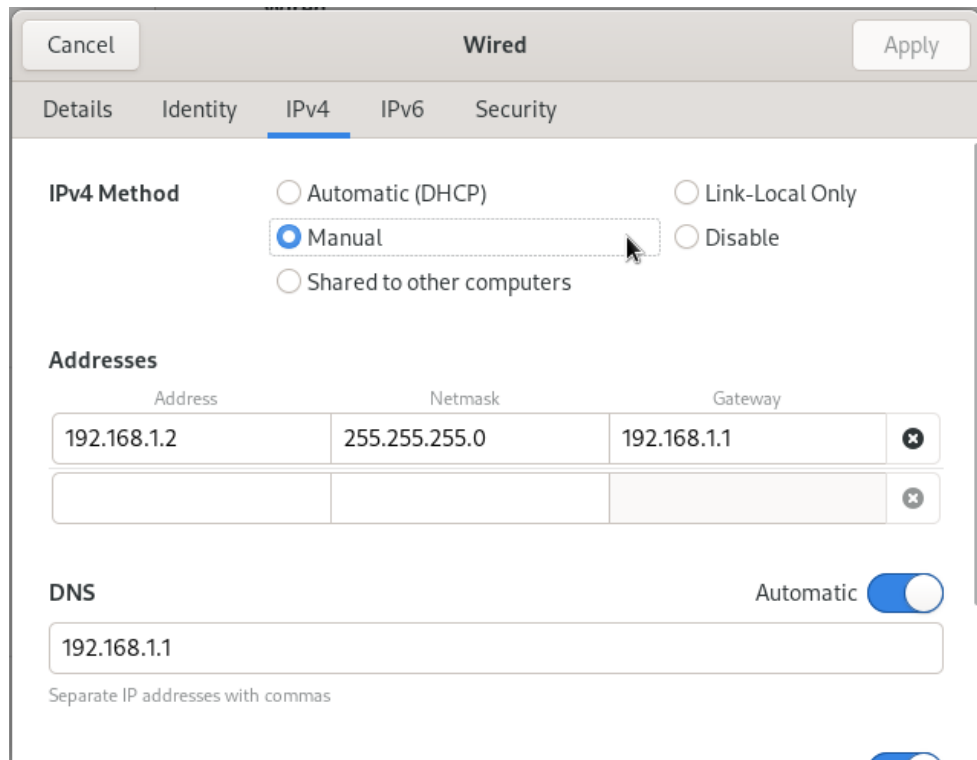
Hình 4: Dung lượng RAM cho Server



Hình 5: Dung lượng ổ cứng cho Server



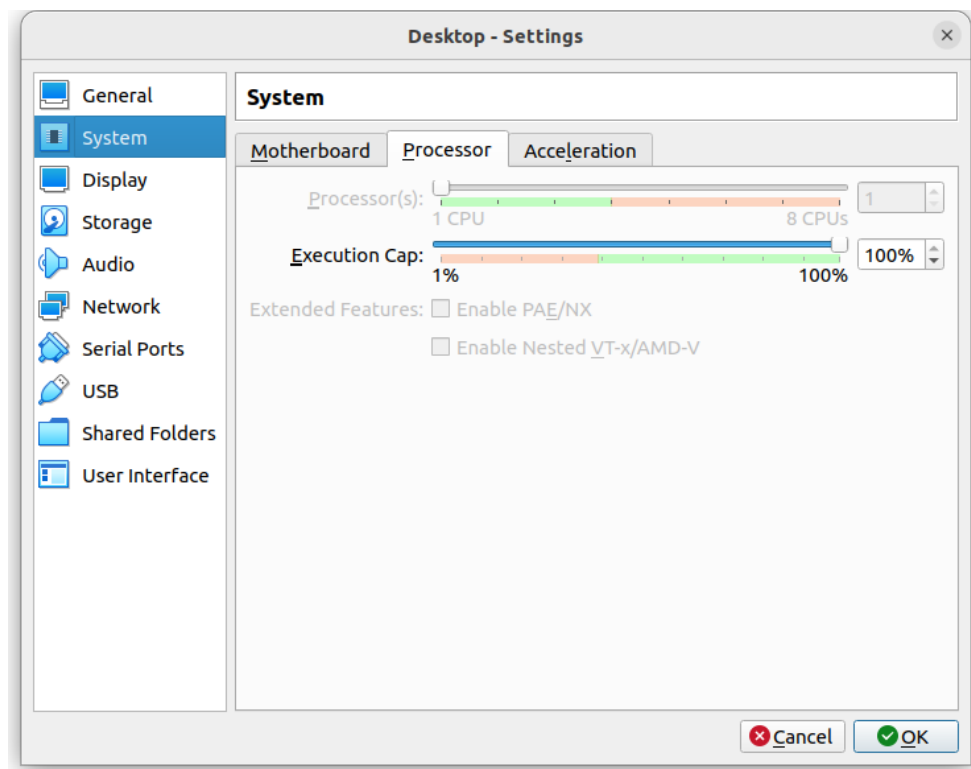
Hình 6: Cấu hình mạng máy Server (1)



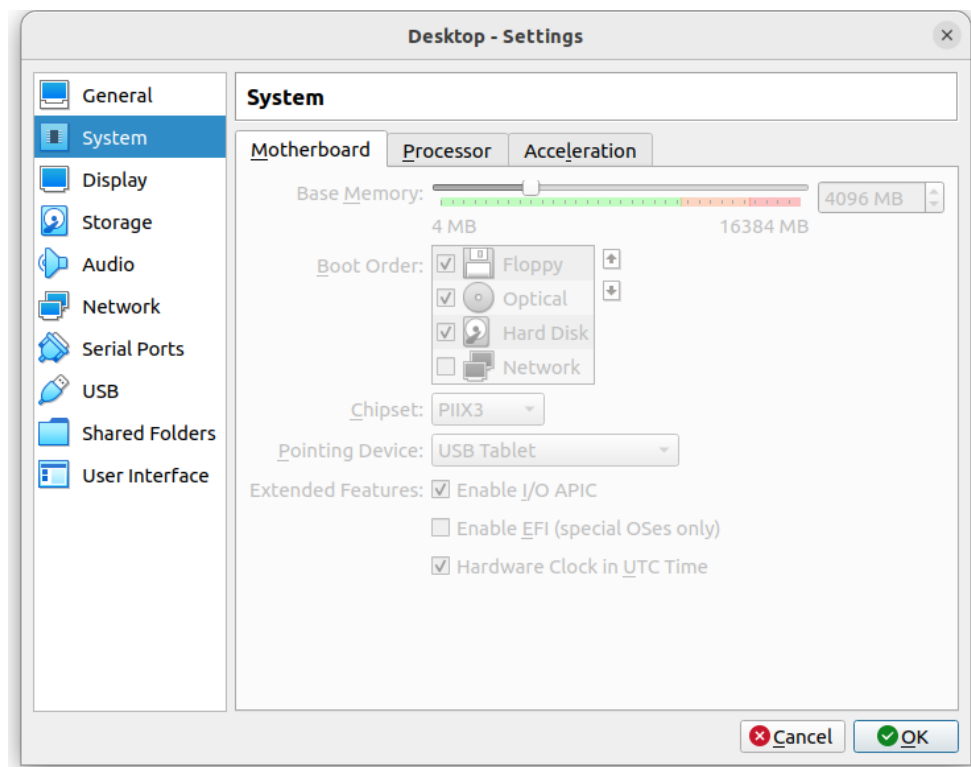
Hình 7: Cấu hình mạng máy Server (2)

2. Máy Desktop có cấu hình như sau:

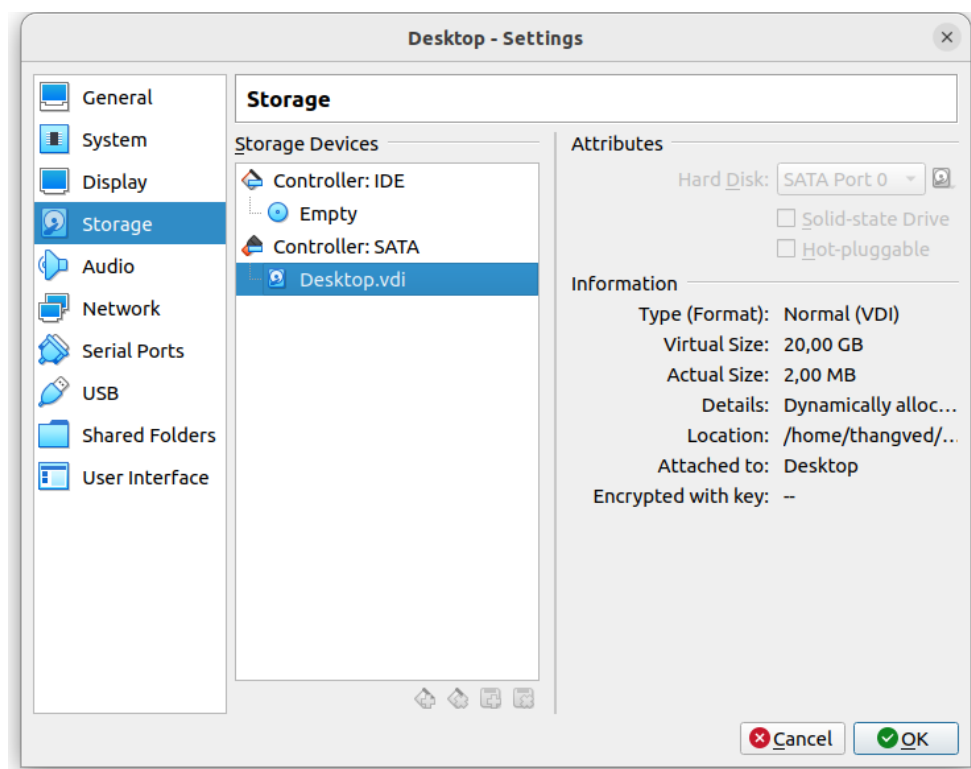
- Hệ điều hành: Lubuntu 22.04.3 LTS (Jammy Jellyfish)
- CPU: 1 Core (Hình 8)
- Ram: 4GB (Hình 9)
- Disk: 20GB (Hình 10)
- Network: NAT Network "QTHT" (Hình 11)



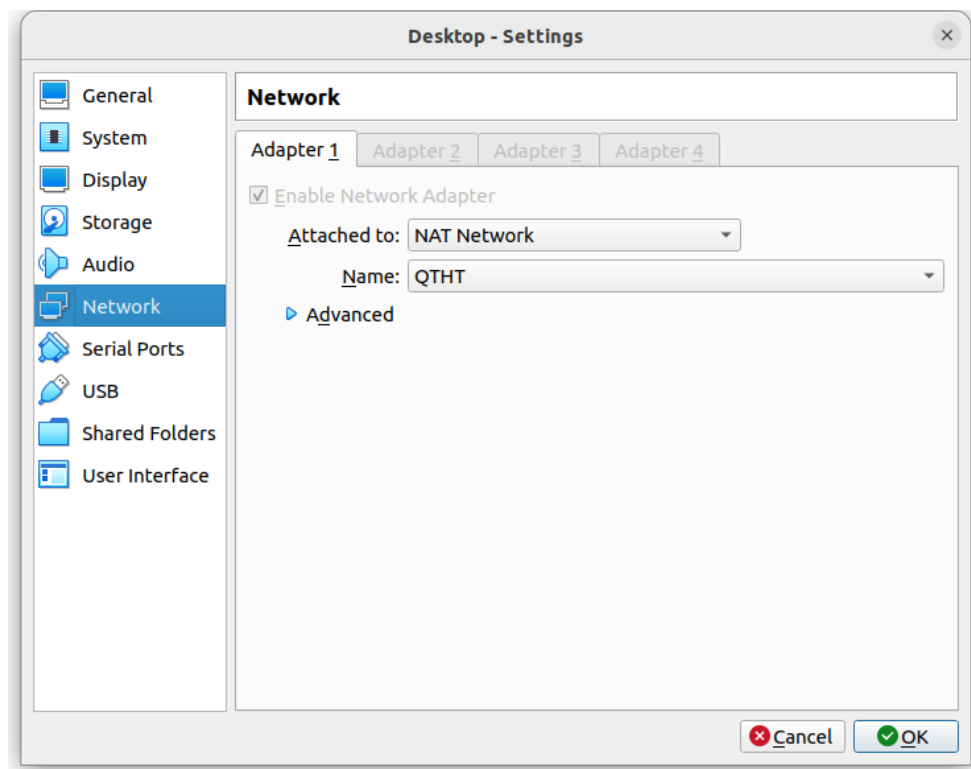
Hình 8: Số Core CPU cho máy Desktop



Hình 9: Dung lượng RAM cho máy Desktop

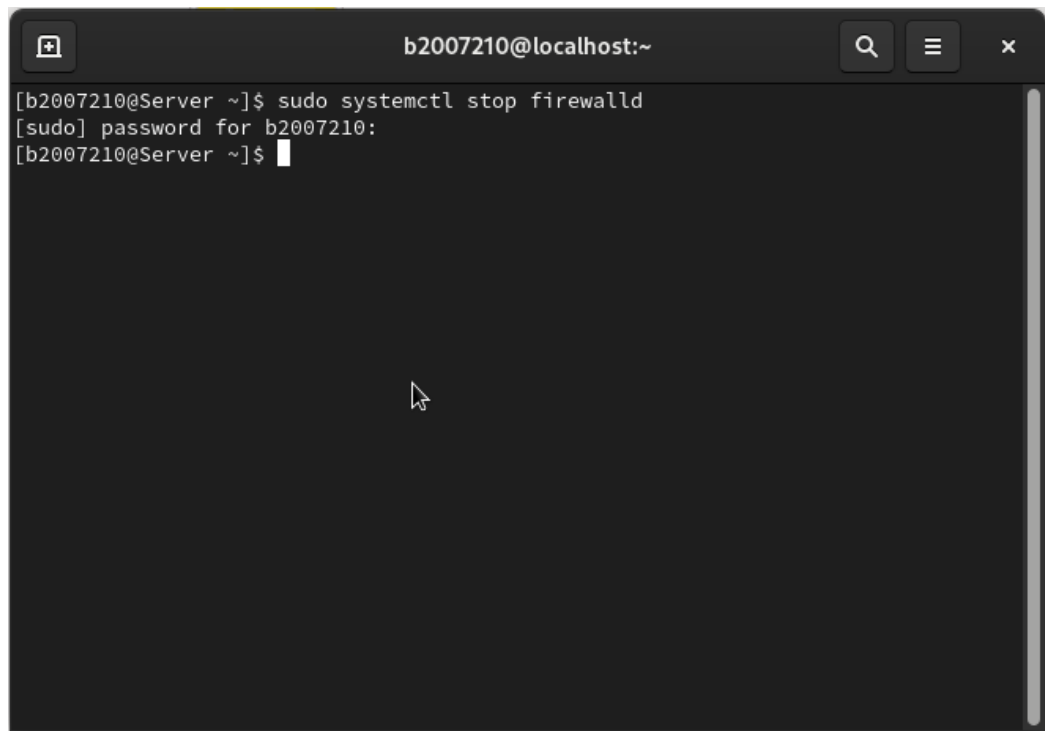


Hình 10: Dung lượng ổ đĩa cho máy Desktop



Hình 11: Cấu hình mạng cho máy Desktop

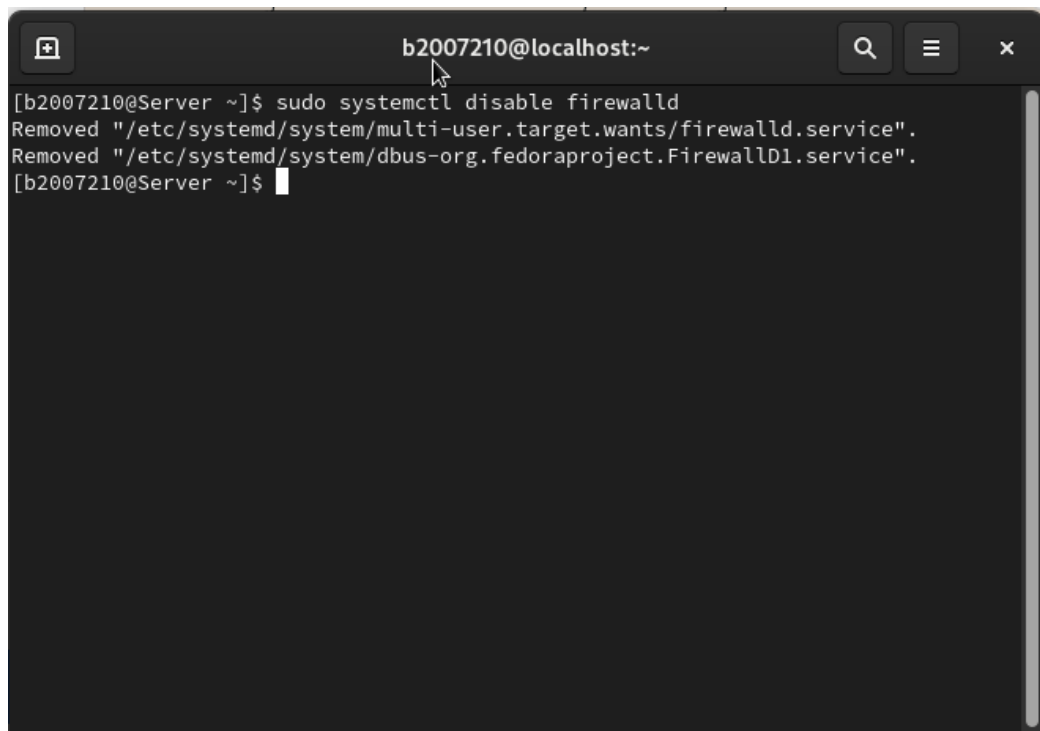
- Trong quá trình cài hệ điều hành CentOS 9, tạo 1 tài khoản với username là <Mã số sinh viên>; firstname và lastname là họ tên của sinh viên. Cấp quyền quản trị (sudo) cho tài khoản. Sử dụng tài khoản vừa tạo để thực hiện bài tập tổng hợp (không dùng tài khoản root).
- Tắt dịch vụ tường lửa trên Server. 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



```
b2007210@localhost:~
[b2007210@Server ~]$ sudo systemctl disable firewalld
Removed "/etc/systemd/system/multi-user.target.wants/firewalld.service".
Removed "/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service".
[b2007210@Server ~]$
```

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

1.2.1 Tạo người dùng

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*).



```

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

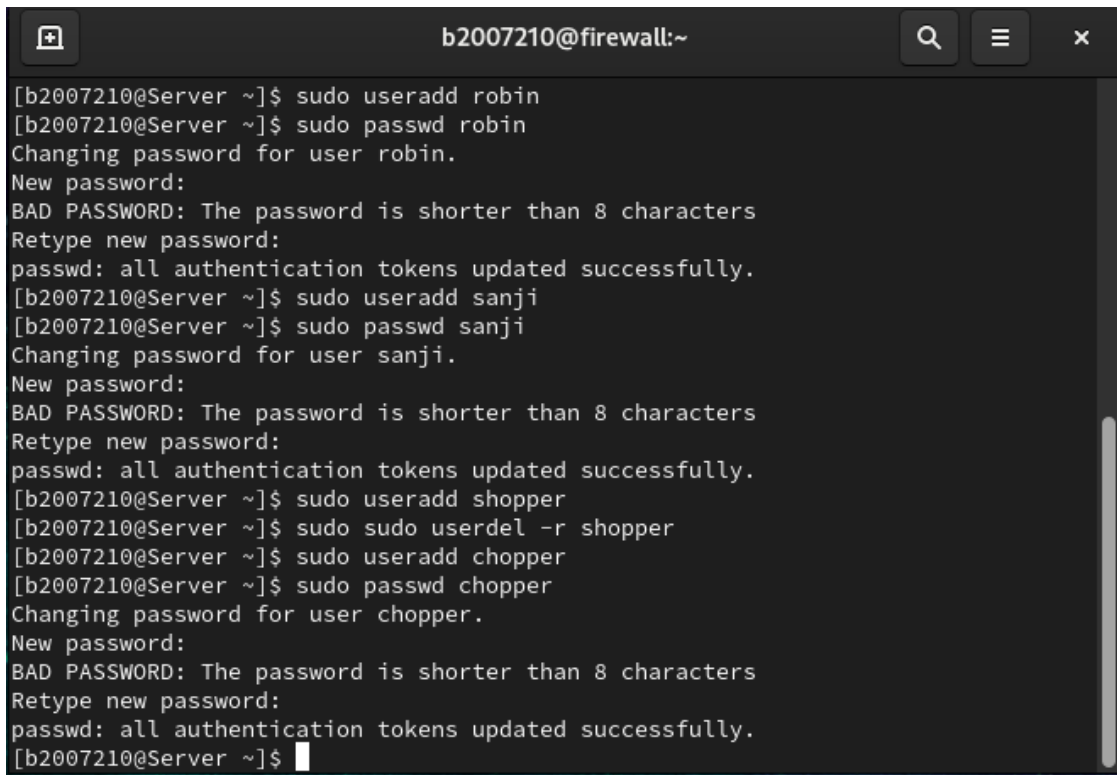
```

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 ~]$
```

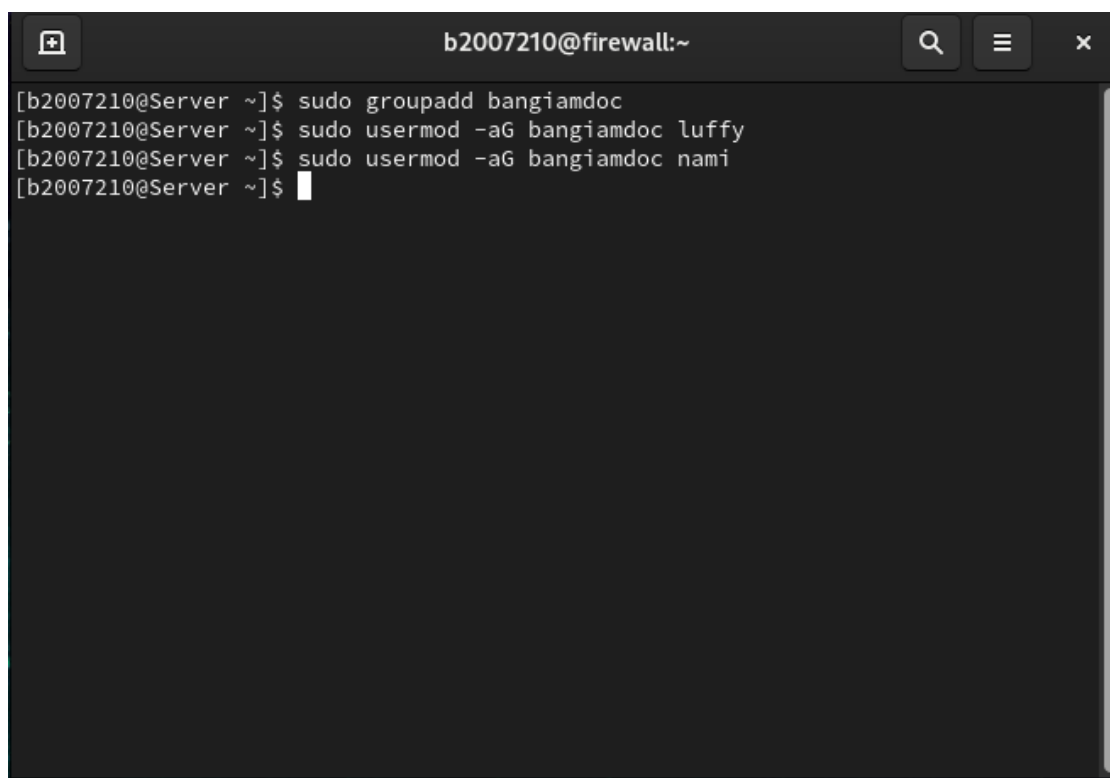
Hình 15: Tạo và đặt mật khẩu cho các người dùng còn lại

```
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

1.2.2 Tạo nhóm người dùng và thêm người dùng vào nhóm

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).



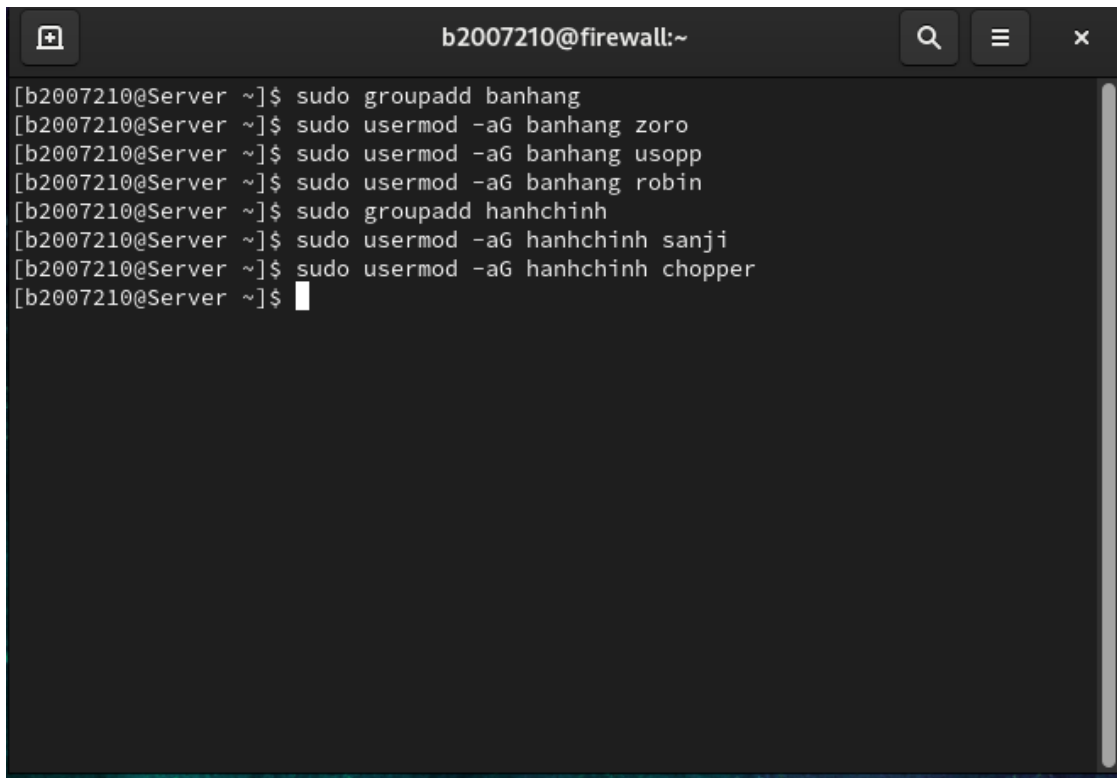
```
b2007210@firewall:~  
[b2007210@Server ~]$ sudo groupadd bangiamdoc  
[b2007210@Server ~]$ sudo usermod -aG bangiamdoc luffy  
[b2007210@Server ~]$ sudo usermod -aG bangiamdoc nami  
[b2007210@Server ~]$
```

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

1.2.3 Cấp quyền sudo cho user nami

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

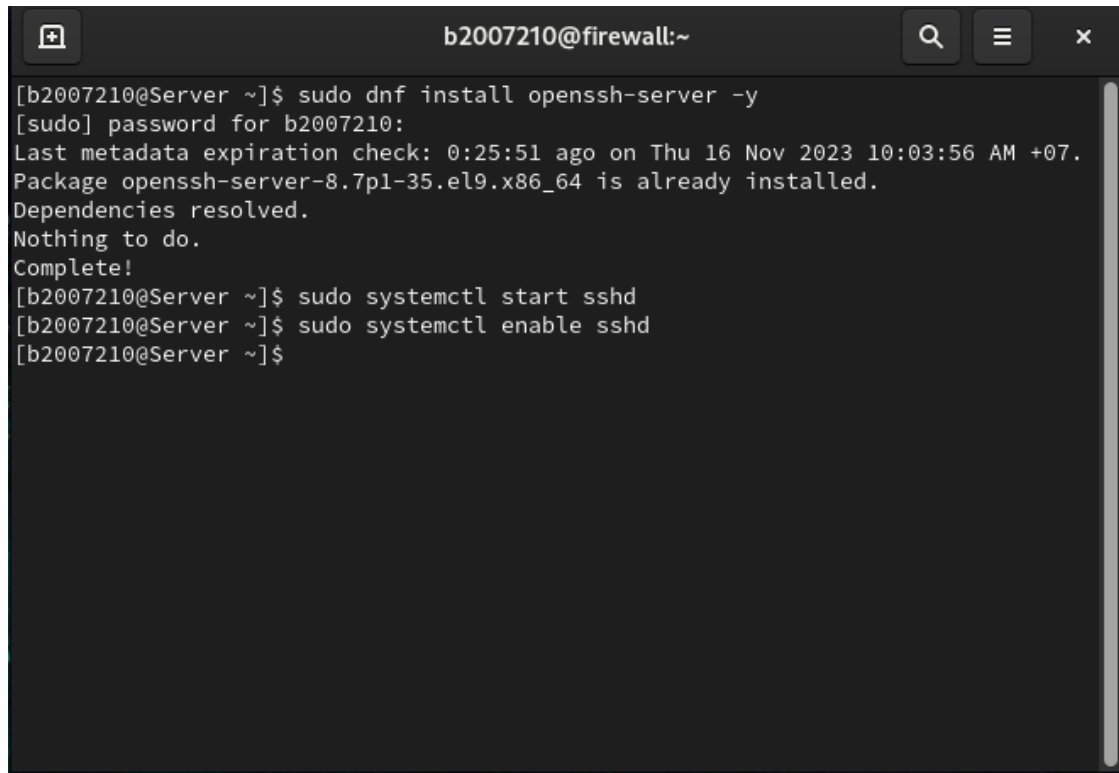
```
1 sudo usermod -aG wheel nami
```

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.

1.3.1 Cài đặt dịch vụ ssh



```
b2007210@firewall:~  
[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 ~]$
```

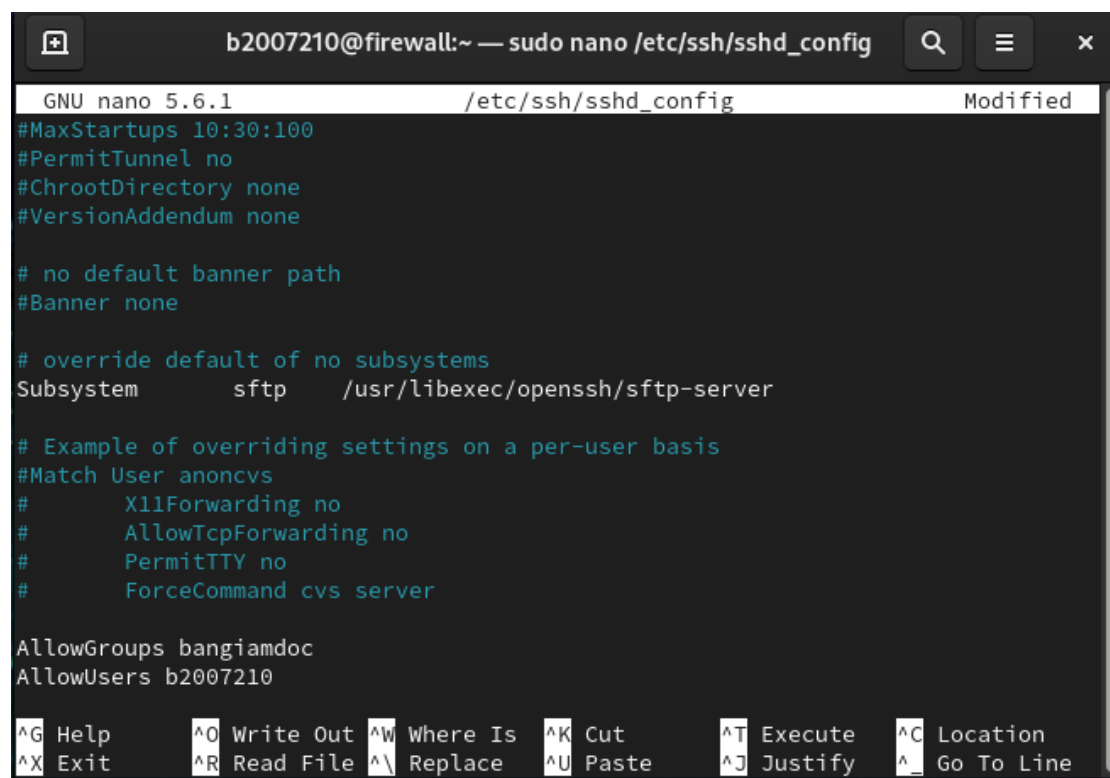
Hình 19: Cài đặt và kích hoạt dịch vụ ssh

```
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

1.3.2 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).



```
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
```

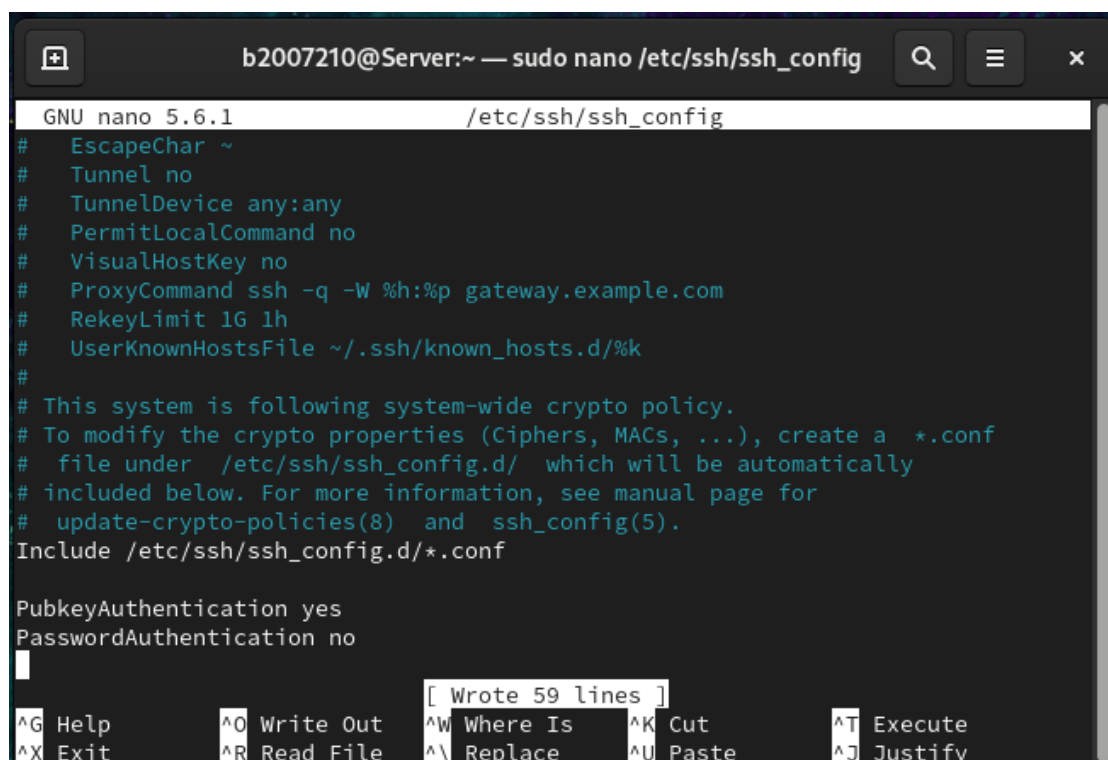
Hình 20: Cho phép nhóm bangiamdoc và user b2007210 có quyền điều khiển máy tính từ xa

- 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`).

1.3.3 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).



```
GNU nano 5.6.1 /etc/ssh/ssh_config
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
#
# This system is following system-wide crypto policy.
# To modify the crypto properties (Ciphers, MACs, ...), create a *.conf
# file under /etc/ssh/ssh_config.d/ which will be automatically
# included below. For more information, see manual page for
# update-crypto-policies(8) and ssh_config(5).
Include /etc/ssh/ssh_config.d/*.conf

PubkeyAuthentication yes
PasswordAuthentication no
[ Wrote 59 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Hình 21: Cấu hình cho phép truy cập dịch vụ ssh bằng private key

- `PubkeyAuthentication yes`: Cho phép chứng thực bằng private key.
- `PasswordAuthentication no`: Không cho phép chứng thực bằng password.

Sau khi cấu hình xong, ta cần khởi động lại dịch vụ ssh để áp dụng những thay đổi này (dùng lệnh `systemctl restart sshd`).

Để tạo private key và public key, ta sử dụng lệnh `ssh-keygen` (Hình 22).


```
b2007210@Server:~  
[b2007210@Server ~]$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/b2007210/.ssh/id_rsa):  
Created directory '/home/b2007210/.ssh'.  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/b2007210/.ssh/id_rsa  
Your public key has been saved in /home/b2007210/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:TRODIQETwHneKu4pY5+6bqUM8lxG5E6pccU5RzeLC9c b2007210@Server  
The key's randomart image is:  
+---[RSA 3072]-----+  
| ..o++o+oo= |  
| o o.=.o+ = |  
| = +.oo E |  
| . B .o + . |  
| B . S . |  
|o o.= |  
|++o+ |  
|o=+.. |  
|+B*o |  
+-----[SHA256]-----+  
[b2007210@Server ~]$
```

Hình 22: Tạo private key và public key

Sau đó, ta cần đổi lại tên của public key thành `authorized_keys` và phân lại 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

- Đổi tên tập tin public key thành `authorized_keys`.

```
1 mv ~/.ssh/id\_rsa.pub ~/.ssh/authorized\_keys
```

Listing 9: Đổi tên tập tin public key

- Cho phép chủ sở hữu đọc và ghi vào tập tin `authorized_keys`.

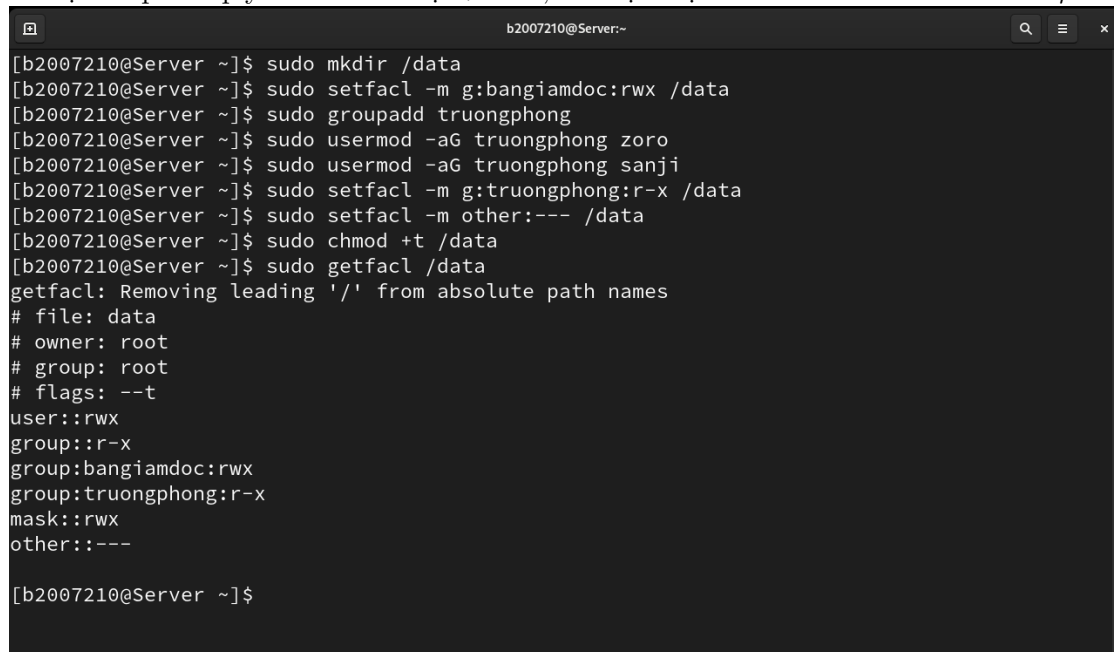
```
1 chmod 600 ~/.ssh/authorized\_keys
```

Listing 10: Phân quyền cho 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 11: 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 12: 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 13: 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 14: Phân quyền cho nhân viên

5. 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:~
[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:

1. Tạo một zone mới có tên là **services**

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

Listing 15: Tạo zone mới có tên là **services**

2. 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 16: Thêm các dịch vụ DNS, DHCP, SSH, Web, SAMBA vào zone **services**

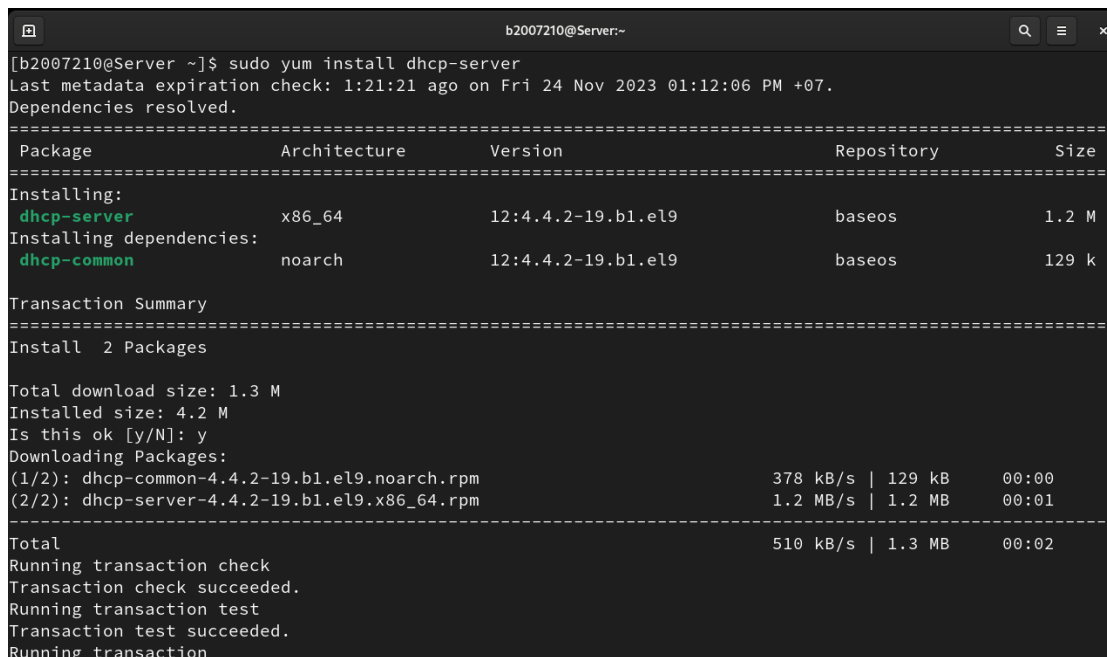
3. Khởi động lại dịch vụ tường lửa để áp dụng những thay đổi này

```
1 sudo systemctl restart firewalld
```

1.6 (5%) Cài đặt và cấu hình dịch vụ DHCP trên Server để cấu hình mạng tự động cho các máy Desktop trong nhánh mạng

- Địa chỉ IP của desktop: trong dãy 192.168.1.100/24 đến 192.168.1.254/24
- Địa chỉ gateway: 192.168.1.1
- DNS server: 192.168.1.2 và 8.8.8.8

1.6.1 Cài đặt dịch vụ DHCP



```
[b2007210@Server ~]$ sudo yum install dhcp-server
Last metadata expiration check: 1:21:21 ago on Fri 24 Nov 2023 01:12:06 PM +07.
Dependencies resolved.
=====
Package                        Architecture      Version           Repository        Size
=====
Installing:
  dhcp-server                  x86_64            12:4.4.2-19.b1.el9    baseos            1.2 M
Installing dependencies:
  dhcp-common                  noarch            12:4.4.2-19.b1.el9    baseos            129 k
=====
Transaction Summary
=====
Install 2 Packages

Total download size: 1.3 M
Installed size: 4.2 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): dhcp-common-4.4.2-19.b1.el9.noarch.rpm        378 kB/s | 129 kB    00:00
(2/2): dhcp-server-4.4.2-19.b1.el9.x86_64.rpm       1.2 MB/s | 1.2 MB    00:01
-----
Total                                               510 kB/s | 1.3 MB    00:02
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
```

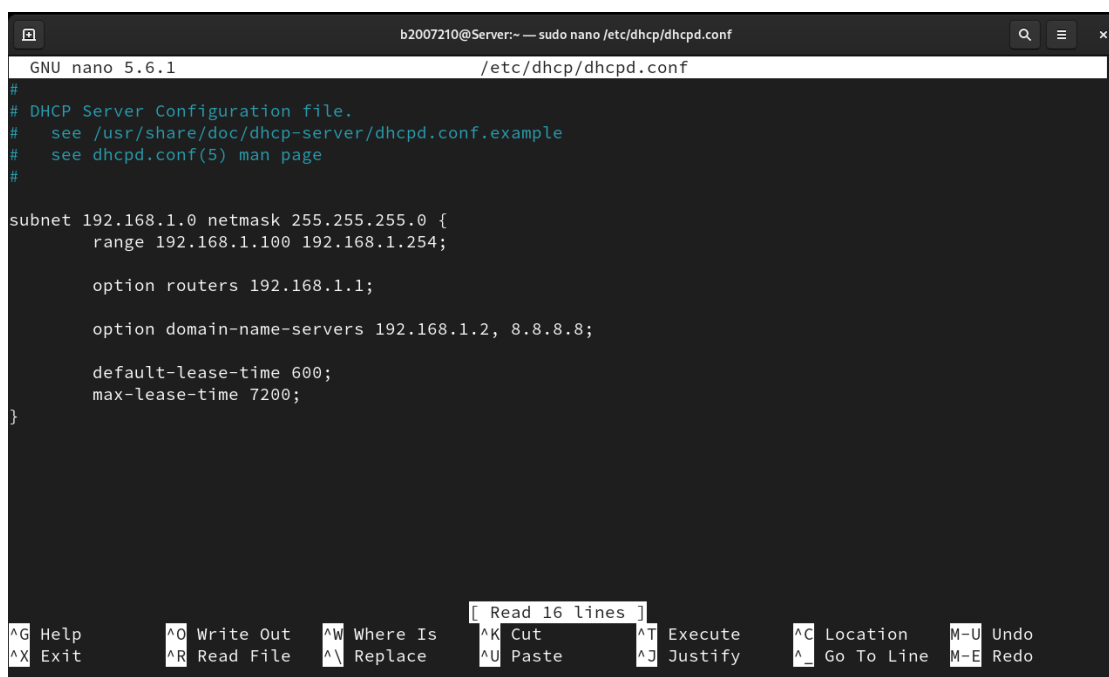
Hình 26: Cài đặt dhcp-server

```
1 sudo yum install dhcp-server
```

Listing 17: Cài đặt dịch vụ DHCP

1.6.2 Cấu hình dịch vụ dhcp

Ta có thể cấu hình dịch vụ dhcp bằng cách chỉnh sửa nội dung file `/etc/dhcp/dhcpd.conf`



```
GNU nano 5.6.1 /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.254;

    option routers 192.168.1.1;

    option domain-name-servers 192.168.1.2, 8.8.8.8;

    default-lease-time 600;
    max-lease-time 7200;
}
```

Hình 27: Cấu hình dịch vụ dhcp

Nội dung file `/etc/dhcp/dhcpd.conf` như sau:

```
1 subnet 192.168.1.0 netmask 255.255.255.0 {
2 range 192.168.1.100 192.168.1.254;
3
4 option routers 192.168.1.1;
5
6 option domain-name-servers 192.168.1.2, 8.8.8.8;
7
8 default-lease-time 600;
9 max-lease-time 7200;
10 }
```

Listing 18: Nội dung file `/etc/dhcp/dhcpd.conf`

Dòng 1 Cấu hình subnet là 255.255.255.0 với địa chỉ mạng là 192.168.1.0.

Dòng 2 Cấu hình range địa chỉ IP cho các máy desktop là từ 192.168.1.100 đến 192.168.1.254.

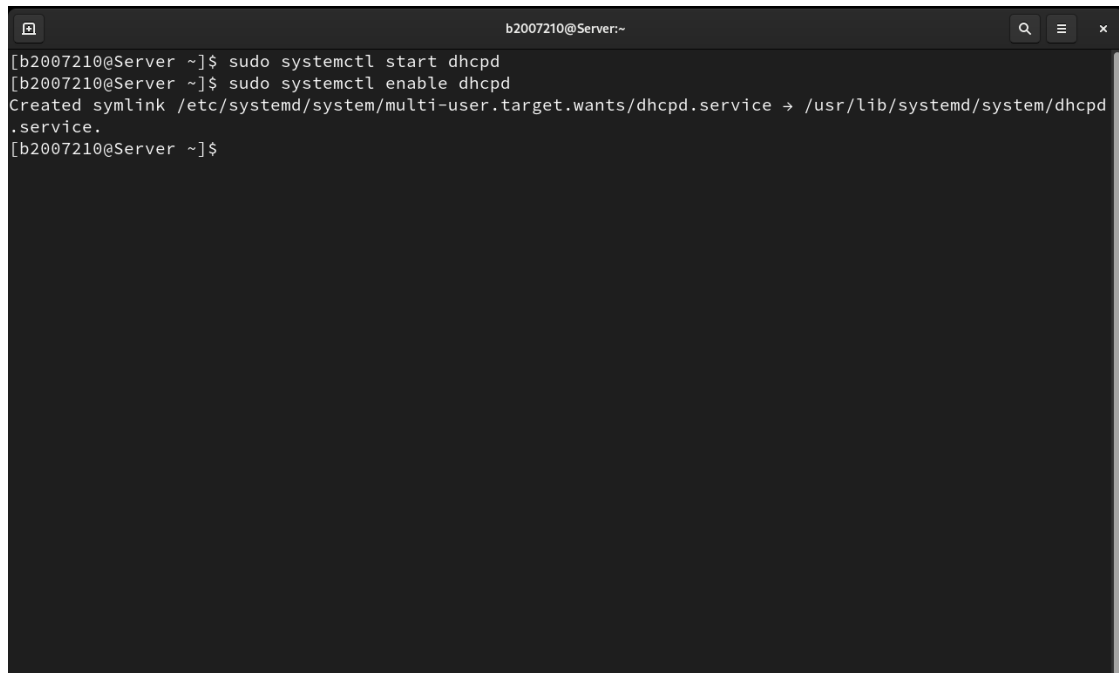
Dòng 4 Cấu hình địa chỉ gateway là 192.168.1.1.

Dòng 6 Cấu hình địa chỉ DNS server là

Dòng 8 Cấu hình thời gian mặc định mà một thiết bị sẽ được cấp phát địa chỉ IP là 600s.

Dòng 9 Cấu hình thời gian tối đa mà một thiết bị được cấp địa chỉ IP là 7200s (2h).

1.6.3 Khởi động dịch vụ dhcp



```
b2007210@Server:~  
[b2007210@Server ~]$ sudo systemctl start dhcpd  
[b2007210@Server ~]$ sudo systemctl enable dhcpd  
Created symlink /etc/systemd/system/multi-user.target.wants/dhcpd.service → /usr/lib/systemd/system/dhcpd.service.  
[b2007210@Server ~]$
```

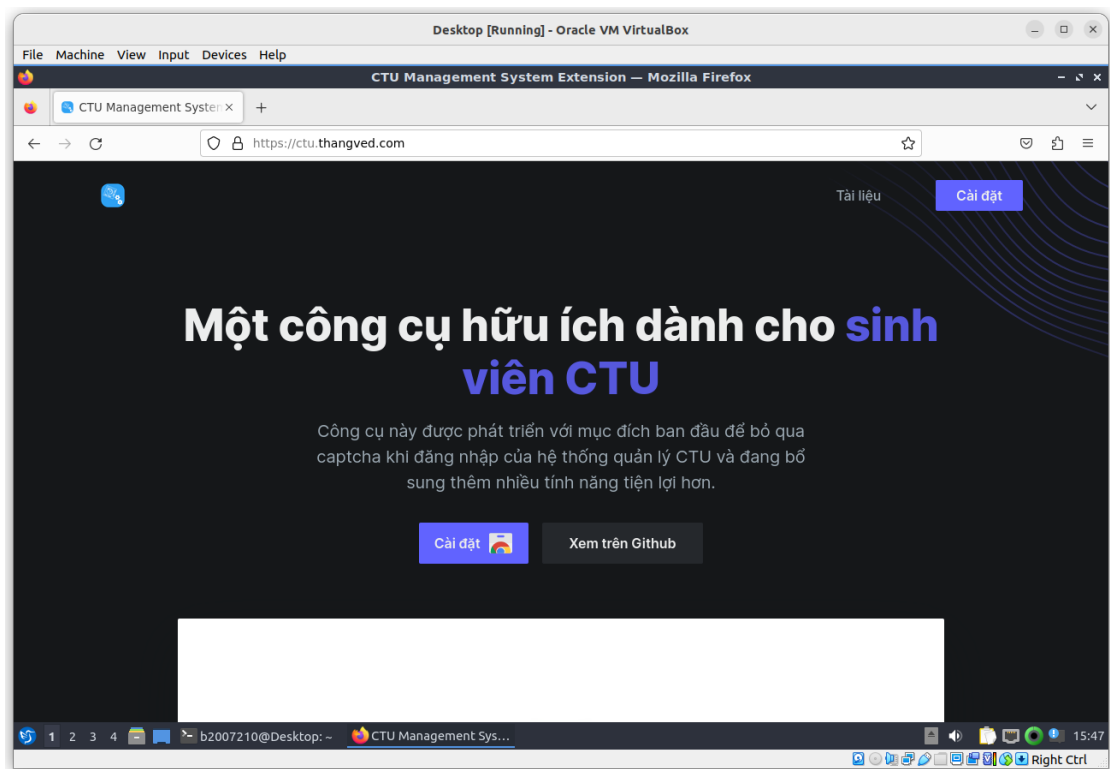
Hình 28: Khởi động dịch vụ dhcp

```
1 sudo systemctl start dhcpd  
2 sudo systemctl enable dhcpd
```

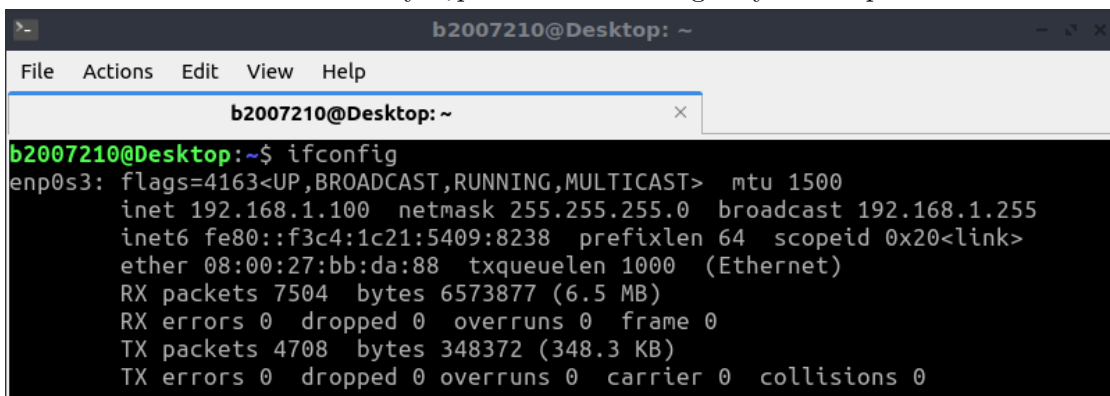
Listing 19: Khởi động dịch vụ dhcp

1.6.4 Kiểm tra lại dịch vụ dhcp

Sau khi cấu hình xong, ta sẽ kiểm tra lại bằng cách sử dụng máy desktop (*Hình 29*) để kết nối vào mạng QHTT và kiểm tra địa chỉ IP của máy Desktop (*Hình 30*).



Hình 29: Truy cập vào internet bằng máy Desktop




Hình 30: Kiểm tra địa chỉ IP của máy desktop (192.168.1.100)

1.7 (5%) Cài đặt và cấu hình dịch vụ máy chủ Web trên Server sử dụng Docker

Tạo một trang web cho công ty có tên miền strawhat.com với nội dung trang chủ giới thiệu về các thành viên trong công ty.

1.7.1 Xây dựng trang web

Có khá nhiều framework/thư viện hỗ trợ tạo trang web, ở đây ta sẽ sử dụng Vitejs để tạo một trang web đơn giản với thư viện Reactjs. Mã nguồn trang web: <https://github.com/thangved/strawhat.com>



thangved

Merge pull request #3 from thangved/thangved-patch-1

✓



















7eadeb4

3 hours ago

🕒

23 commits

▼

	.github/workflows	Merge pull request #3 from thangved/thangved-patch-1	3 hours ago
	.husky	test: test database	5 hours ago
	.nginx	chore: update nginx.conf	3 hours ago
	public	chore: init project	6 hours ago
	src	chore: add logo	3 hours ago
	.dockerignore	fix: fix Dockerfile	3 hours ago
	.eslintrc.cjs	chore: config prettier and husky	6 hours ago
	.gitignore	test: test database	5 hours ago
	.prettierrc	chore: config prettier and husky	6 hours ago
	Dockerfile	fix: fix Dockerfile	3 hours ago
	README.md	chore: config prettier and husky	6 hours ago
	docker-compose.yml	fix: fix Dockerfile	4 hours ago
	index.html	chore: config prettier and husky	6 hours ago
	package-lock.json	chore: add copy right	3 hours ago
	package.json	chore: add copy right	3 hours ago
	tsconfig.json	chore: config prettier and husky	6 hours ago
	tsconfig.node.json	feat: add models	6 hours ago
	vite.config.ts	chore: image optimized	4 hours ago
	vitest.config.ts	test: test database	5 hours ago

Hình 31: Cấu trúc trang web strawhat.com

1.7.2 Cấu hình Docker và nginx

Ta cần quan tâm đến các file sau đây:

- /Dockerfile file này sẽ được sử dụng để build image cho container.

```
1 FROM node:20-alpine as development
2
3 WORKDIR /app
4
5 COPY package*.json .
6
7 RUN npm ci
```

```

8
9 COPY . .
10
11 CMD [ "npm", "run", "dev" ]
12
13 FROM development as production
14
15 RUN npm run build
16
17 FROM nginx:alpine
18
19 COPY --from=production /app/.nginx/nginx.conf /etc/nginx/conf.d/
    default.conf
20
21 WORKDIR /usr/share/nginx/html
22
23 RUN rm -rf ./*
24
25 COPY --from=production /app/dist .
26
27 ENTRYPOINT ["nginx", "-g", "daemon off;"]

```

Listing 20: Nội dung file /Dockerfile

Dòng 1 - 11 Tạo môi trường phát triển bên trong docker container

- 1 Sử dụng image `node:20-alpine` làm base image.
- 3 Chỉ định thư mục làm việc bên trong image là `/app`.
- 5 Sao chép tập tin `package.json` và `package-lock.json` vào bên trong image.
- 7 Cài đặt các thư viện của dự án.
- 9 Sao chép mã nguồn của dự án vào image.
- 11 Lệnh `npm run dev` dùng để chạy dev server do Vitejs cấu hình.

Dòng 13 - 15 Build bản production để triển khai

- 13 Sử dụng image từ image `development` làm base image
- 15 Lệnh `npm run dev` sẽ tạo một bản build của dự án này vào trong thư mục `dist`

Dòng 17 - 27 Cấu hình nginx

- 17 Sử dụng image `nginx:alpine` làm base image.
- 19 Sao chép file cấu hình từ image `production` vào image và đổi tên thành `/etc/nginx/conf.d/default.conf`, đây là file config mặc định của nginx.
- 23 Chỉ định thư mục làm việc.
- 23 Xóa trang web mặc định của nginx.
- 25 Sao chép bản dựng từ image `production`.
- 27 Lệnh `nginx -g daemon off;` sẽ chạy nginx và không thoát ra.

– /docker-compose.yml.

```

1 version: '3.7'
2
3 services:
4   strawhat.com:
5     build: .
6     container_name: strawhat.com
7     ports:
8       - '80:80'

```

Listing 21: Nội dung file `/docker-compose.up`

Dòng 1 Sử dụng phiên bản 3.7 của docker-compose.

Dòng 3 Tạo một service có tên là `strawhat.com`.

Dòng 4 Sử dụng Dockerfile để build image cho service này.

Dòng 5 Đặt tên cho container là `strawhat.com`.

Dòng 6 Chỉ định cổng 80 của máy host sẽ được map vào cổng 80 của container.

– `/.nginx/nginx.conf` file này sẽ được sử dụng để cấu hình nginx.

```

1 server {
2   server_name strawhat.com www.strawhat.com;
3
4   listen 80;
5
6   location / {
7     root /usr/share/nginx/html;
8     index index.html index.htm;
9     try_files $uri /index.html =404;
10  }
11
12  error_page 500 502 503 504 /50x.html;
13
14  location = /50x.html {
15    root /usr/share/nginx/html;
16  }
17 }

```

Listing 22: Nội dung file `/.nginx/nginx.conf`

Dòng 2 Cấu hình server name là `strawhat.com` và `www.strawhat.com`, khi một request có domain là `strawhat.com` hoặc `www.strawhat.com` được gửi đến server này, nginx sẽ xử lý request này.

Dòng 4 Cấu hình nginx lắng nghe trên cổng 80.

Dòng 6 Cấu hình thư mục root là `/usr/share/nginx/html`.

Dòng 7 Cấu hình file index mặc định là `index.html`.

Dòng 8 Cấu hình thử các file tĩnh nếu không tìm thấy file `index.html`, do đây là trang web SPA nên ta sẽ thử các file tĩnh trước khi trả về trang `index.html`.

Dòng 10 Cấu hình trang 50x.html.

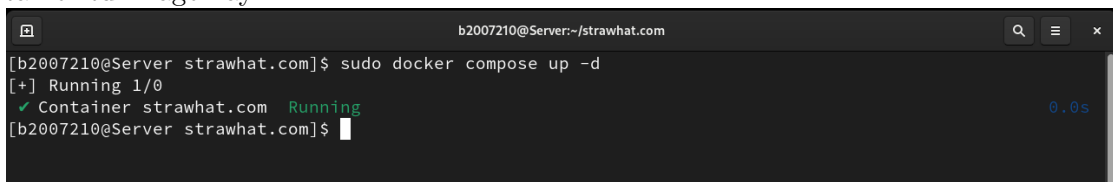
Dòng 12 Cấu hình thư mục root cho trang 50x.html.

Dòng 14 Cấu hình trang 50x.html.

Dòng 16 Cấu hình thư mục root cho trang 50x.html.

1.7.3 Chạy trang web trên máy host

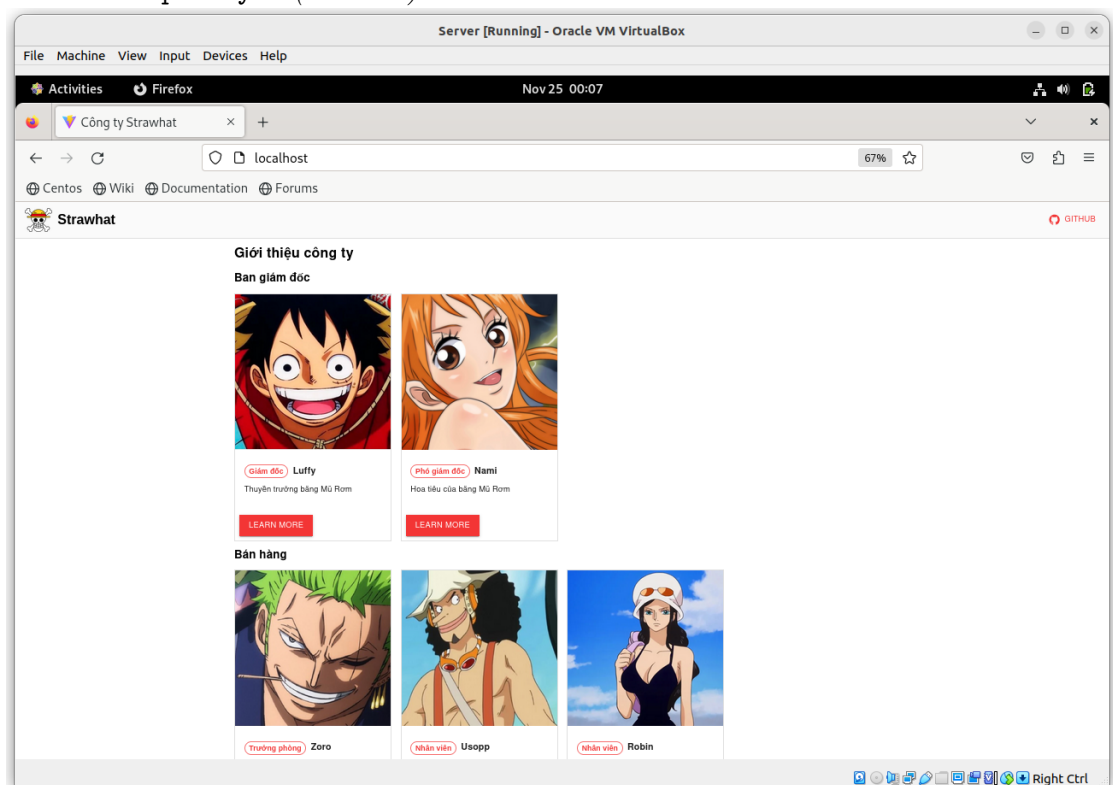
Để chạy thử web trên máy host, ta sẽ dùng lệnh `docker compose up` để docker sẽ tự động kéo các image trên cloud và build image cho service `strawhat.com` sau đó chạy container từ image này.



```
b2007210@Server:~/strawhat.com
[b2007210@Server strawhat.com]$ sudo docker compose up -d
[+] Running 1/0
✓ Container strawhat.com Running
[b2007210@Server strawhat.com]$
```

Hình 32: Chạy trang web bằng lệnh `docker compose up`

Lúc này, trang web sẽ được chạy trên cổng 80 của máy host như đã cấu hình trong file `docker-compose.yml` (Hình 32).

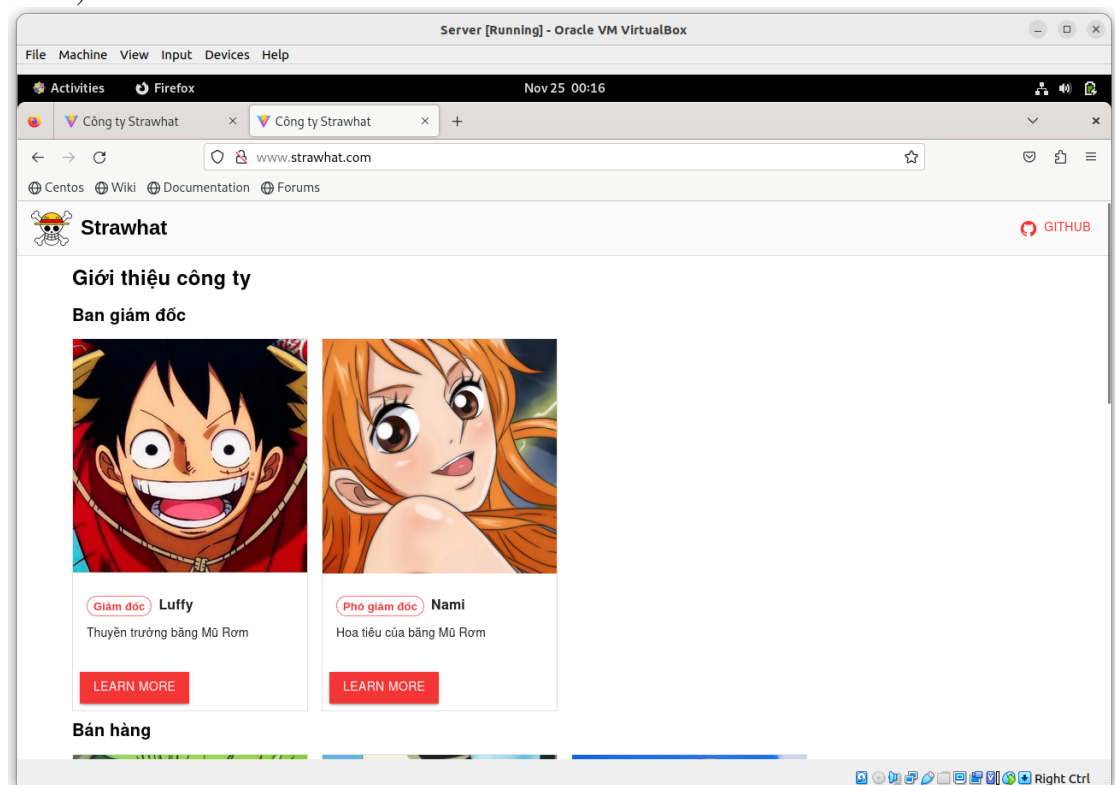


Hình 33: Giao diện trang web strawhat.com

Ta có thể thử chỉnh sửa DNS của máy host để trỏ tên miền strawhat.com về địa chỉ localhost để kiểm tra trang web đã hoạt động chính xác hay chưa.

```
b2007210@Server:~/strawhat.com — sudo nano /etc/hosts
GNU nano 5.6.1 /etc/hosts
127.0.0.1 Server localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 strawhat.com www.strawhat.com
```

Hình 34: Chỉnh sửa file `/etc/hosts` để trỏ tên miền strawhat.com về địa chỉ localhost. Sau khi cấu hình xong, ta có thể truy cập vào trang web theo địa chỉ `http://strawhat.com` (Hình 35).



Hình 35: Truy cập vào trang web từ server qua địa chỉ `http://strawhat.com`

1.8 (5%) Cài đặt và cấu hình dịch vụ SAMBA trên Server

- Thành viên ban giám đốc và trưởng phòng có thể truy cập vào thư mục `/data` trên Server.
- Tất cả người dùng có thể truy cập vào thư mục cá nhân của họ (`/home/<username>`) trên Server.
- Trên Desktop tạo ổ cứng ảo nối kết tới dịch vụ SAMBA trên Server.