

TRƯỜNG ĐẠI HỌC CẦN THƠ
TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG



QUẢN TRỊ HỆ THỐNG

Mã Học Phần: CT179

Nhóm học phần: 04

BÁO CÁO
BÀI TẬP TỔNG HỢP CUỐI KỲ

Giáo viên hướng dẫn

ThS.GV Lê Huỳnh Quốc Bảo

Sinh viên thực hiện

Tên: Trần Thái Toàn

MSSV: B2203534

Học Kỳ II, 2023 - 2024

MỤC LỤC

DANH MỤC HÌNH	i
DANH MỤC CODE	iii
DANH MỤC BẢNG	v
1. Cài đặt và cấu hình Server/Desktop	1
1.1 (10%) Sử dụng phần mềm VirtualBox/VMware/UTM/Parallels	1
1.1.1 Tạo 1 NAT Network tên "QTHT"	3
1.1.2 Tạo 2 máy ảo Server và Desktop	3
1.2 (10%) Tạo các nhóm người dùng và người dùng	8
1.2.1 Tạo người dùng	9
1.2.2 Tạo nhóm người dùng và thêm người dùng vào nhóm	10
1.2.3 Cấp quyền sudo cho người dùng Gia Cát Lượng	12
1.3 (10%) Tạo và phân quyền cho thư mục /data	12
1.4 (10%) Cài đặt và cấu hình dịch vụ DHCP trên server để cấu hình mạng tự động cho các máy desktop trong nhánh mạng	14
1.4.1 Cài đặt dịch vụ DHCP	14
1.4.2 Cấu hình dịch vụ DHCP	14
1.4.3 Khởi động dịch vụ DHCP	16
1.4.4 Kiểm tra dịch vụ DHCP	16
1.5 (10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa server	17
1.5.1 Cài đặt dịch vụ SSH	17
1.5.2 Cấu hình chỉ cho phép thành viên trong ban giám đốc và các trưởng phòng mới có quyền điều khiển từ xa	18
1.5.3 Chỉ cho phép chứng thực bằng private key	18
1.6 (10%) Cài đặt và cấu hình dịch vụ máy chủ Web trên server sử dụng Docker	20
1.6.1 Xây dựng trang web	20
1.6.2 Cấu hình cho Docker và nginx	21
1.6.3 Khởi chạy trang web trên máy server	24
1.7 (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server	27
1.7.1 Cài đặt dịch vụ FTP	27
1.7.2 Cấu hình dịch vụ FTP	27
1.7.3 Sử dụng máy desktop để kiểm tra kết nối tới dịch vụ FTP	28
1.8 (5%) Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền lautamquoc.com	29
1.8.1 Cài đặt dịch vụ DNS	30

1.8.2	Cấu hình máy chủ DNS trên server	30
1.8.3	Khởi động dịch vụ DNS	32
1.8.4	Kiểm tra trên máy desktop	32
1.9	(5%) Cài đặt và cấu hình tường lửa trên server	33
1.9.1	Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP	34
1.9.2	Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server .	35
1.10	(5%) Sử dụng dịch vụ cron và shell script tự động thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng trên server	36
1.10.1	Tạo thư mục sao lưu dữ liệu	36
1.10.2	Viết shell script backup	36
1.10.3	Cấu hình cron	38

DANH MỤC HÌNH

Hình 1	Sơ đồ hệ thống mạng của công ty Tam Quốc	1
Hình 2	Cấu hình NAT Network QTHT	3
Hình 3	Số Core CPU của Server	4
Hình 4	Dung lượng Ram của Server.....	4
Hình 5	Dung lượng ổ cứng của Server.....	5
Hình 6	Cấu hình mạng máy tính Server	5
Hình 7	Cấu hình mạng máy tính Server	6
Hình 8	Số Core CPU của Desktop	7
Hình 9	Dung lượng Ram của Desktop	7
Hình 10	Dung lượng ổ cứng của Desktop	8
Hình 11	Cấu hình mạng máy tính Desktop.....	8
Hình 12	Tạo và đặt mật khẩu cho tài khoản Lưu Bị.....	9
Hình 13	Tạo và đặt mật khẩu cho các tài khoản còn lại	10
Hình 14	Tạo nhóm bangiamdoc và thêm người dùng vào.....	11
Hình 15	Tạo nhóm còn lại và thêm người dùng vào.....	11
Hình 16	Cấp quyền sudo cho người dùng Gia Cát Lượng	12
Hình 17	Tạo và phân quyền cho thư mục /data	13
Hình 18	Cài đặt dịch vụ dhcp-server	14
Hình 19	Cấu hình dịch vụ DHCP	15
Hình 20	Khởi động dịch vụ DHCP	16
Hình 21	Truy cập vào internet bằng máy desktop	16
Hình 22	Kiểm tra địa chỉ IP của máy desktop (10.0.2.50)	17
Hình 23	Cài đặt và kích hoạt dịch vụ openssh-server	17
Hình 24	Cấu hình chỉ cho phép bangiamdoc và truongphong sử dụng dịch vụ SSH để điều khiển từ xa.....	18
Hình 25	Cấu hình chỉ cho phép chứng thực bằng private key	19
Hình 26	Tạo public/private key bằng ssh-keygen	19
Hình 27	Đổi tên và phân quyền cho file public key	20
Hình 28	Cấu trúc trang web lautamquoc.com	21
Hình 29	Khởi chạy trang web bằng docker compose up	25
Hình 30	Giao diện trang web lautamquoc.com	25
Hình 31	Chỉnh sửa file /etc/hosts để trả tên miền lautamquoc.com về địa chỉ localhost	26
Hình 32	Truy cập vào trang web từ server qua địa chỉ http://lautamquoc.com .	26
Hình 33	Nội dung file /etc/vsftpd/vsftpd.conf	27
Hình 34	Tạo file /data/test.txt trên máy server	29

Hình 35	Kiểm tra kết nối tới dịch vụ FTP trên máy desktop	29
Hình 36	Nội dung file /etc/named.conf	30
Hình 37	Nội dung file /etc/named/forward.lautamquoc.com	31
Hình 38	Nội dung file /etc/named/reverse.lautamquoc.com	32
Hình 39	Kiểm tra DNS trên máy desktop	33
Hình 40	Sử dụng trình duyệt để kiểm tra DNS server.....	33
Hình 41	Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP .	34
Hình 42	Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server	35
Hình 43	Script backup mỗi ngày	37
Hình 44	Script backup mỗi tuần.....	37
Hình 45	Script backup mỗi tháng	38
Hình 46	Cấu hình cron	39

DANH MỤC CODE

Code 1	Tạo và đặt mật khẩu cho tài khoản Lưu Bị	9
Code 2	Tạo và đặt mật khẩu cho các tài khoản còn lại	10
Code 3	Tạo nhóm bangiamdoc và thêm người dùng vào	11
Code 4	Tạo nhóm còn lại và thêm người dùng vào	11
Code 5	Cấp quyền sudo cho người dùng Gia Cát Lượng	12
Code 6	Tạo nhóm truongphong và thêm người dùng vào	13
Code 7	Tạo thư mục /data.....	13
Code 8	Phân quyền cho ban giám đốc	13
Code 9	Phân quyền cho trưởng phòng	13
Code 10	Phân quyền cho nhân viên	13
Code 11	Phân quyền cho chủ sở hữu	13
Code 12	Cài đặt dịch vụ dchp-server	14
Code 13	Nội dung file /etc/dhcp/dhcpd.conf	15
Code 14	Khởi động dịch vụ DHCP	16
Code 15	Cài đặt và kích hoạt dịch vụ openssh-server.....	18
Code 16	Đổi tên tập tin public key thành authorized_key cho người dùng Gia Cát Lượng	20
Code 17	Cho phép Gia Cát Lượng đọc và ghi vào tập tin authorized_key	20
Code 18	Nội dung file /Dockerfile	22
Code 19	Nội dung file /docker-compose.yml.....	23
Code 20	Nội dung file /.nginx/nginx.conf	24
Code 21	Nội dung file /etc/vsftpd/vsftpd.conf	27
Code 22	Khởi chạy dịch vụ FTP	28
Code 23	Nội dung file /etc/named.conf.....	30
Code 24	Nội dung file /etc/named/forward.lautamquoc.com	31
Code 25	Nội dung file /etc/named/reverse.lautamquoc.com.....	32
Code 26	Khởi động dịch vụ DNS	32
Code 27	Tạo zone mới có tên là services	34
Code 28	Tạo zone mới có tên là services	34
Code 29	Thêm các dịch vụ DNS, DHCP, SSH, Web, FTP vào zone services	35
Code 30	Khởi động lại firewalld sau khi đổi zone mới	35
Code 31	Thêm một rule mới cho phép desktop (10.0.2.50) vào zone có port 22 (port của SSH)	36
Code 32	Xóa dịch vụ SSH ra khỏi zone	36
Code 33	Khởi động lại firewalld sau khi thêm rule mới	36
Code 34	Ta sẽ tạo thư mục /mnt/backup để lưu trữ dữ liệu sao lưu.	36

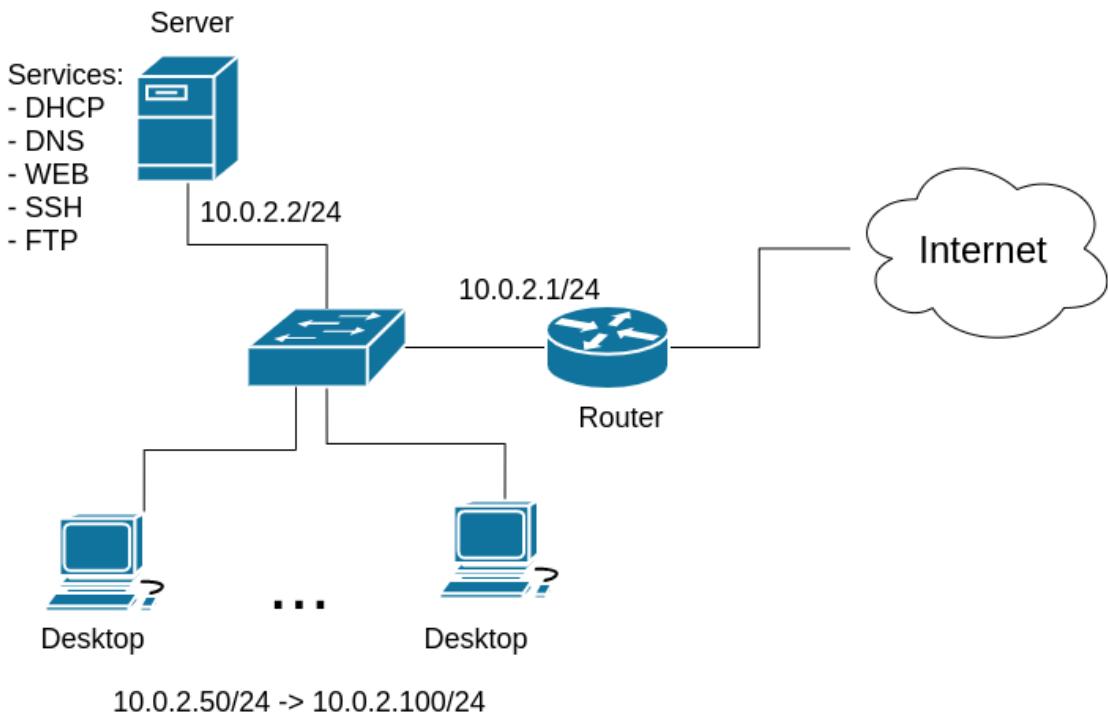
Code 35	Script backup mỗi ngày	37
Code 36	Script backup mỗi tuần	37
Code 37	Script backup mỗi tháng	38
Code 38	Cấu hình cron	39

DANH MỤC BẢNG

Bảng 1	Cấu hình máy Server	2
Bảng 2	Cấu hình máy Desktop	2
Bảng 3	Danh sách người dùng và nhóm người dùng	9

Mô tả bài tập

Công ty Tam Quốc chuyên kinh doanh buffet lẩu cay Tứ Xuyên có nhu cầu cài đặt các dịch vụ mạng phục vụ cho công việc của công ty như sau:



Hình 1: Sơ đồ hệ thống mạng của công ty Tam Quốc

1. Cài đặt và cấu hình Server/Desktop

1.1 (10%) Sử dụng phần mềm VirtualBox/VMware/UTM/Parallels

- Tạo 1 Nat Network tên "QTHT" có địa chỉ mạng là 10.0.2.0/24. Tắt dịch vụ DHCP có sẵn trên NAT Network "QTHT".
- 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	10.0.2.2
Subnet mask	255.255.255.0
Gateway	10.0.2.1
DNS	10.0.2.1

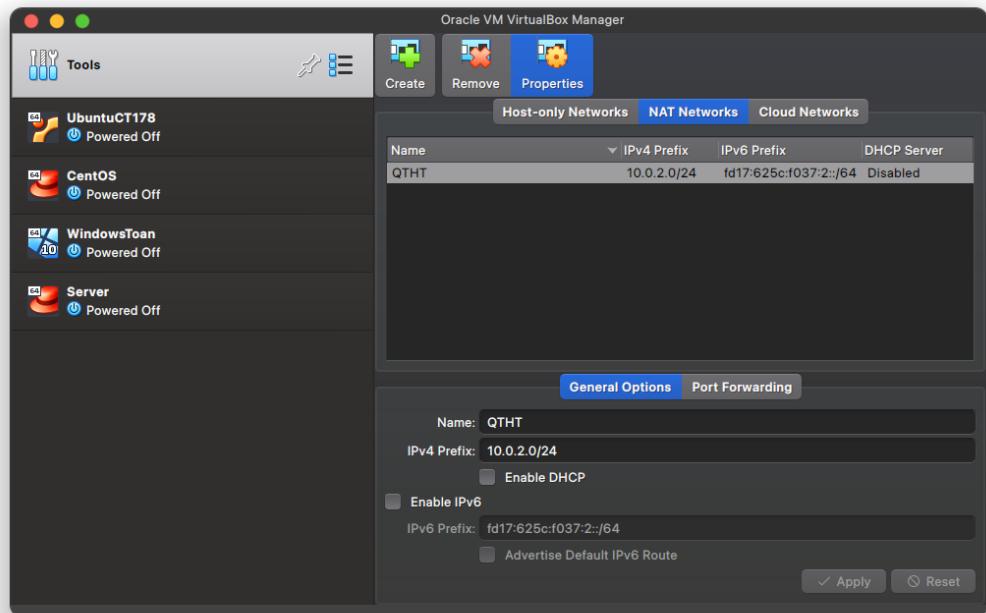
Bảng 2: Cấu hình máy Desktop

Hostname	Desktop
Hệ điều hành	Lubuntu 22.04, hoặc bất kỳ hệ điều hành khác
CPU / RAM / DISK	1core/2G/20G 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

Lưu ý:

- + 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).

1.1.1 Tao 1 NAT Network tên "QTHT"

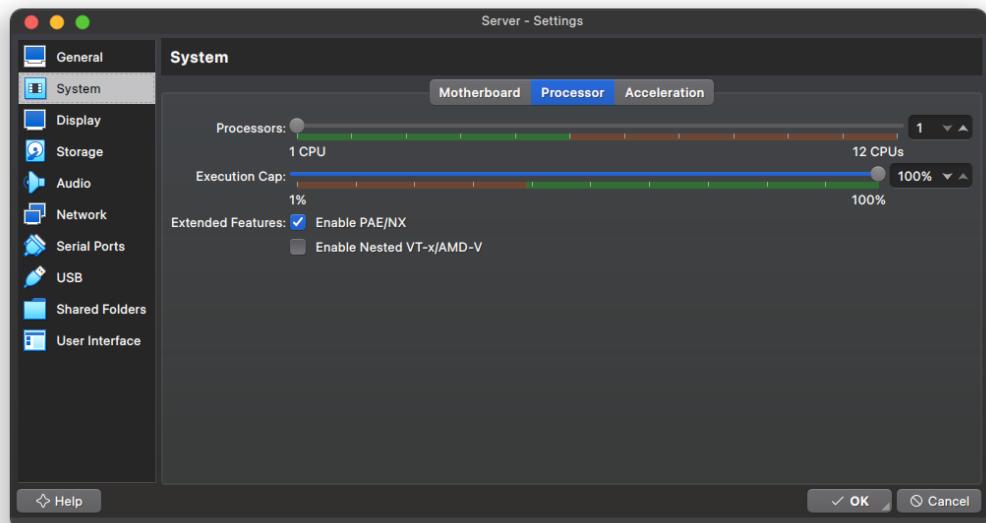


Hình 2: Cấu hình NAT Network QTHT

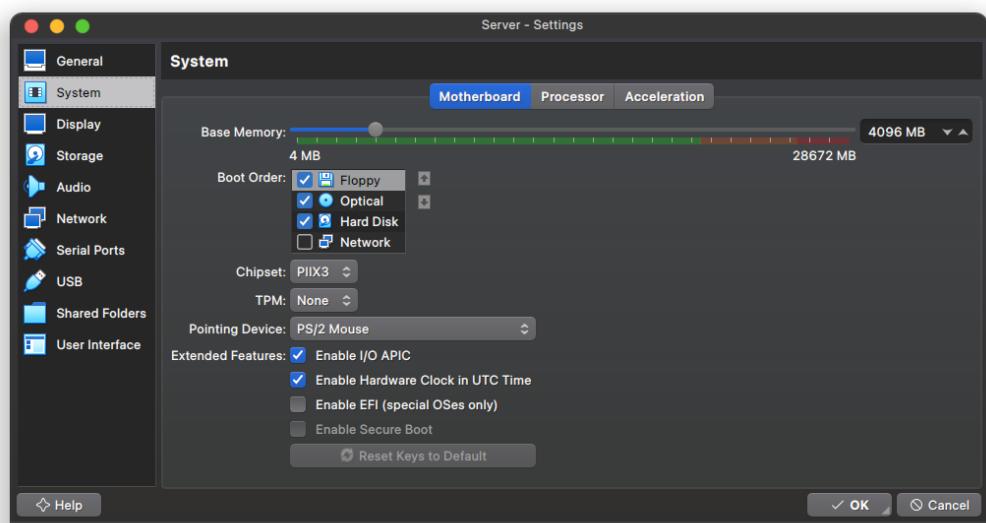
1.1.2 Tao 2 máy ảo Server và Desktop

1.1.2.1 Server có cấu hình như sau:

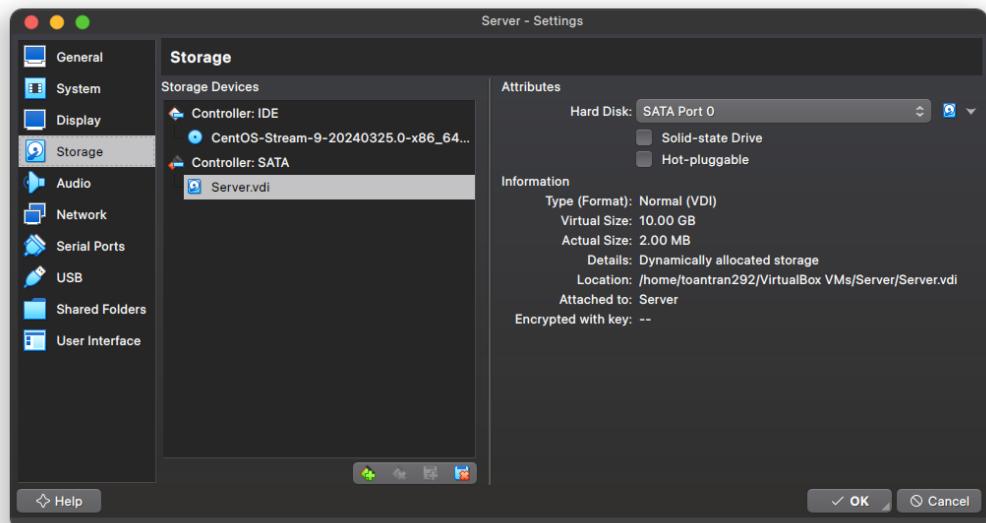
- Hệ điều hành: CentOS 9
- CPU: 1 Core (**Hình 3**)
- Ram: 4GB (**Hình 4**)
- Disk: 10GB (**Hình 5**)
- Network: NAT Network "QTHT" (**Hình 6**)
- IPv4: 10.0.2.2 (**Hình 7**)
- Subnet mask: 255.255.255.0 (**Hình 7**)
- Gateway: 10.0.2.1 (**Hình 7**)
- DNS: 10.0.2.1 (**Hình 7**)



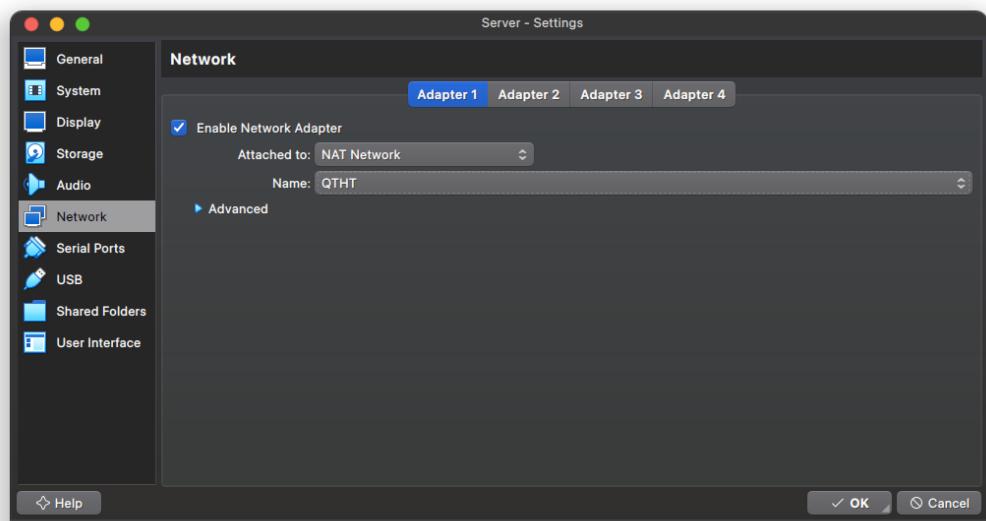
Hình 3: Số Core CPU của Server



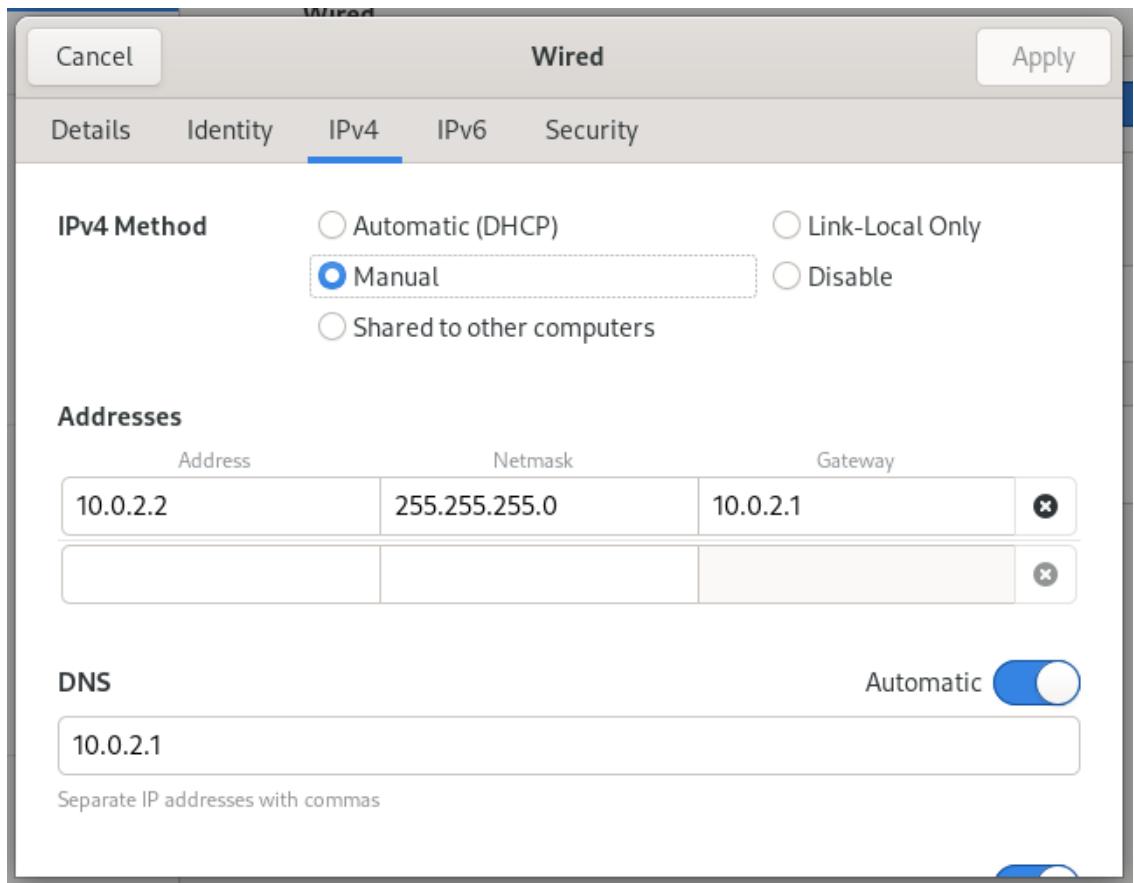
Hình 4: Dung lượng Ram của Server



Hình 5: Dung lượng ổ cứng của Server



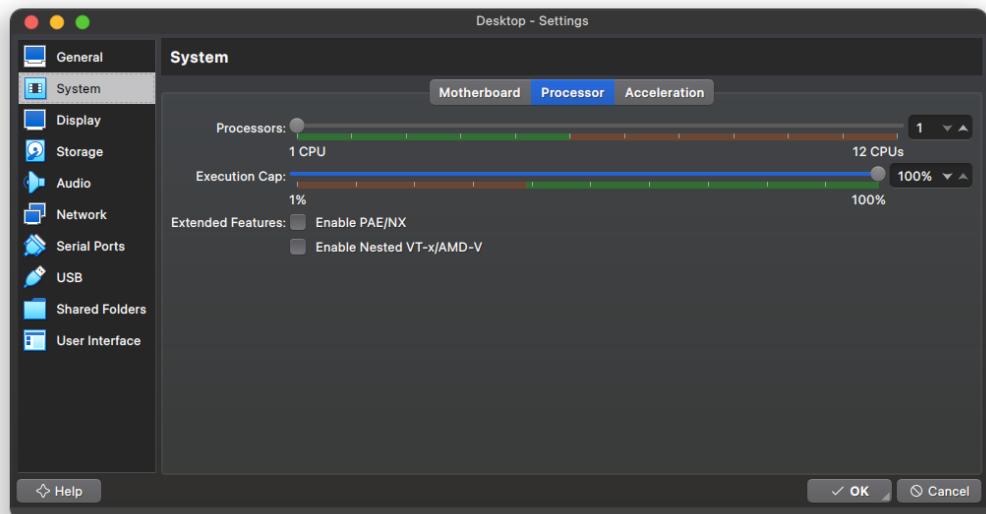
Hình 6: Cấu hình mạng máy tính Server



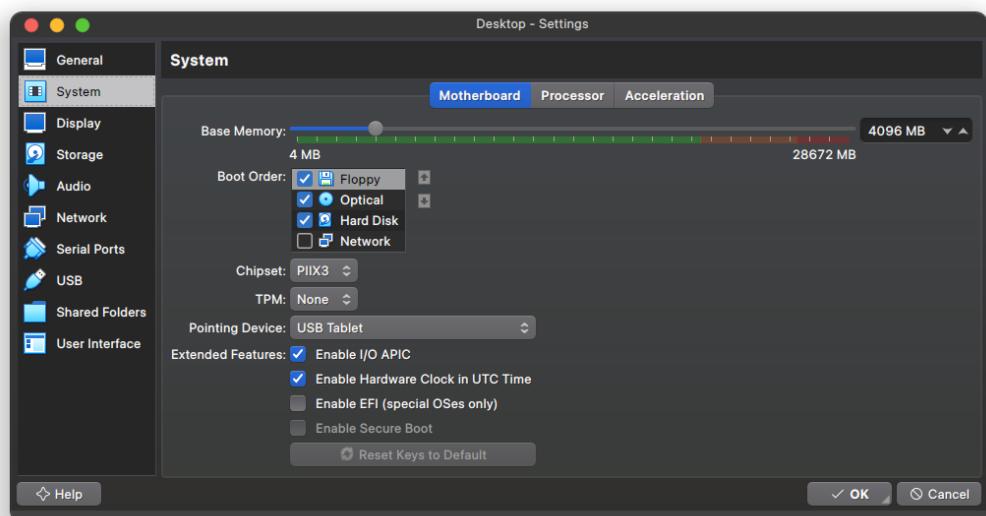
Hình 7: Cấu hình mạng máy tính Server

1.1.2.2 Desktop có cấu hình như sau:

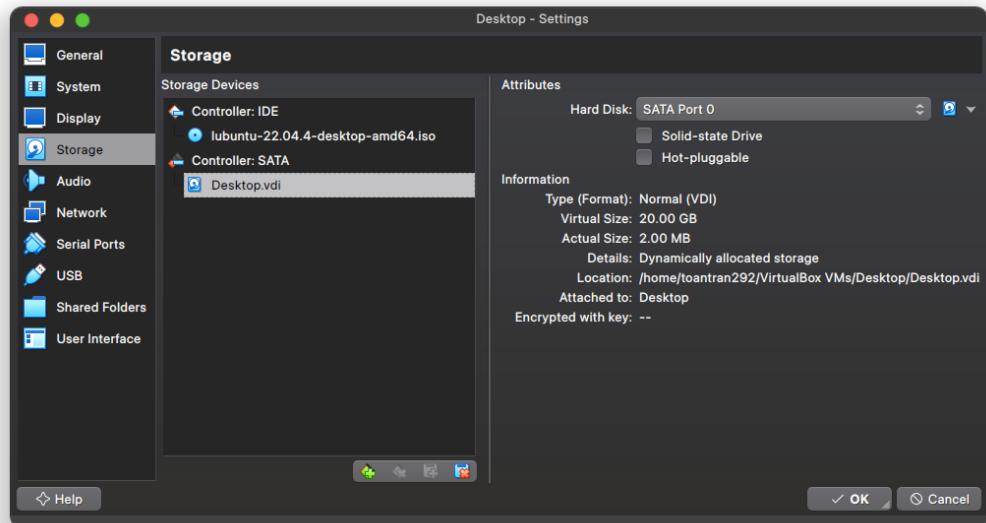
- Hệ điều hành: CentOS 9
- CPU: 1 Core (**Hình 8**)
- Ram: 4GB (**Hình 9**)
- Disk: 20GB (**Hình 10**)
- Network: NAT Network "QTHT" (**Hình 11**)



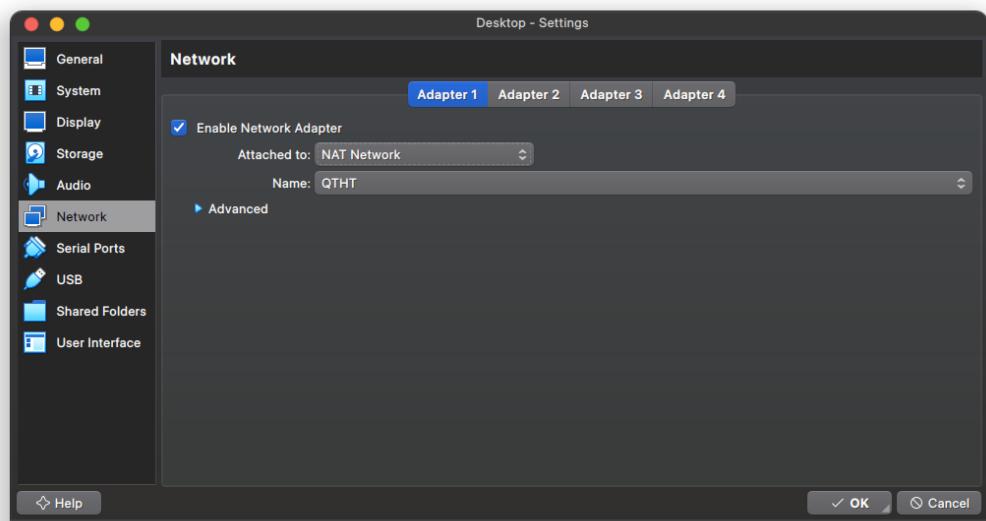
Hình 8: Số Core CPU của Desktop



Hình 9: Dung lượng Ram của Desktop



Hình 10: Dung lượng ổ cứng của Desktop



Hình 11: Cấu hình mạng máy tính Desktop

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

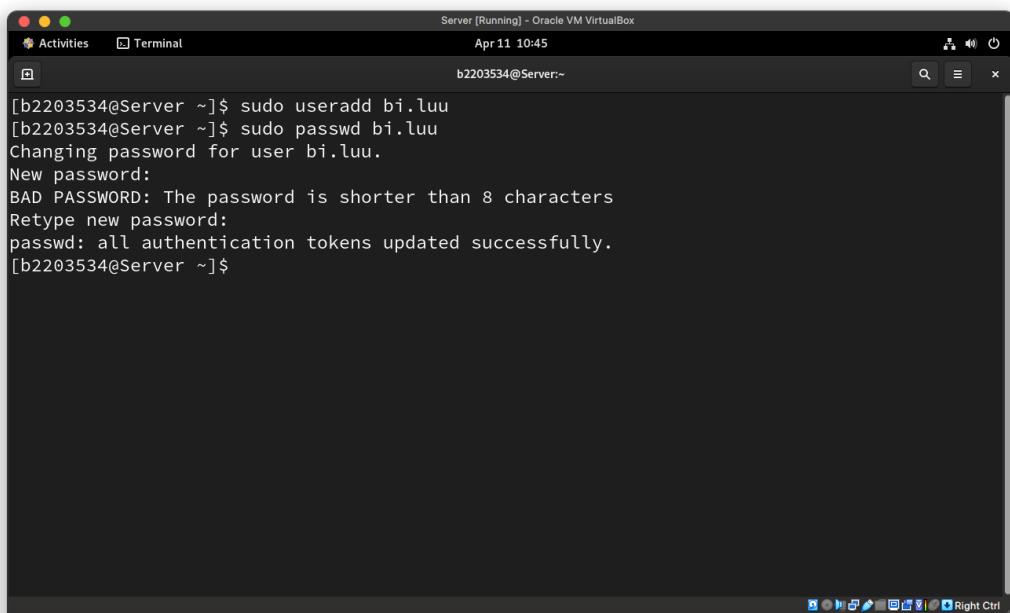
Để quản lý các bộ phận và người dùng trong công ty, hãy tạo các nhóm người dùng (group) và người dùng (user) trên server như sau. Cấp quyền sudo cho người dùng Gia Cát Lượng.

Bảng 3: Danh sách người dùng và nhóm người dùng

STT	Họ tên	Nhóm	Username	Password	Mô tả
1	Lưu Bị	bangiamdoc	bi.luu	luubi	Giám đốc
2	Gia Cát Lượng	bangiamdoc	luong.giacat	giacatluong	Phó giám đốc
3	Quan Vũ	hanhchanh	vu.quan	quanvu	Trưởng phòng
4	Trương Phi	hanhchanh	phi.truong	truongphi	Nhân viên
5	Triệu Vân	banhang	van.trieu	trieuvan	Trưởng phòng
6	Mã Siêu	banhang	sieu.ma	masieu	Nhân viên
7	Hoàng Trung	banhang	trung.hoang	hoangtrung	Nhân viên

1.2.1 Tạo người dùng

Trong CentOS để tạo người dùng ta có thể sử dụng lệnh `useradd <username>` và dùng lệnh `passwd <username>` để đặt mật khẩu cho người dùng. Dưới đây là ví dụ về việc tạo tài khoản và đặt mật khẩu cho tài khoản Lưu Bị (**Hình 12**).



The screenshot shows a terminal window titled "Server [Running] - Oracle VM VirtualBox". The window displays the following command sequence:

```
[b2203534@Server ~]$ sudo useradd bi.luu
[b2203534@Server ~]$ sudo passwd bi.luu
Changing password for user bi.luu.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[b2203534@Server ~]$
```

Hình 12: Tạo và đặt mật khẩu cho tài khoản Lưu Bị

```
1 sudo useradd bi.luu
2 sudo passwd bi.luu
```

Code 1: Tạo và đặt mật khẩu cho tài khoản Lưu Bị

Các tài khoản còn lại thực hiện tương tự (**Hình 13**).

```

Retype new password:
passwd: all authentication tokens updated successfully.
[b2203534@Server ~]$ sudo useradd van.trieu
[b2203534@Server ~]$ sudo passwd van.trieu
Changing password for user van.trieu.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[b2203534@Server ~]$ sudo useradd sieu.ma
[b2203534@Server ~]$ sudo passwd sieu.ma
Changing password for user sieu.ma.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[b2203534@Server ~]$ sudo useradd trung.hoang
[b2203534@Server ~]$ sudo passwd trung.hoang
Changing password for user trung.hoang.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[b2203534@Server ~]$ 

```

Hình 13: Tạo và đặt mật khẩu cho các tài khoản còn lại

```

1 sudo useradd bi.luu
2 sudo passwd bi.luu
3 sudo useradd luong.giacat
4 sudo passwd luong.giacat
5 sudo useradd vu.quan
6 sudo passwd vu.quan
7 sudo useradd phi.truong
8 sudo passwd phi.truong
9 sudo useradd van.trieu
10 sudo passwd van.trieu
11 sudo useradd sieu.ma
12 sudo passwd sieu.ma
13 sudo useradd trung.hoang
14 sudo passwd trung.hoang

```

Code 2: Tạo và đặt mật khẩu cho các tài khoản còn lại

1.2.2 Tạo nhóm người dùng và thêm người dùng vào nhóm

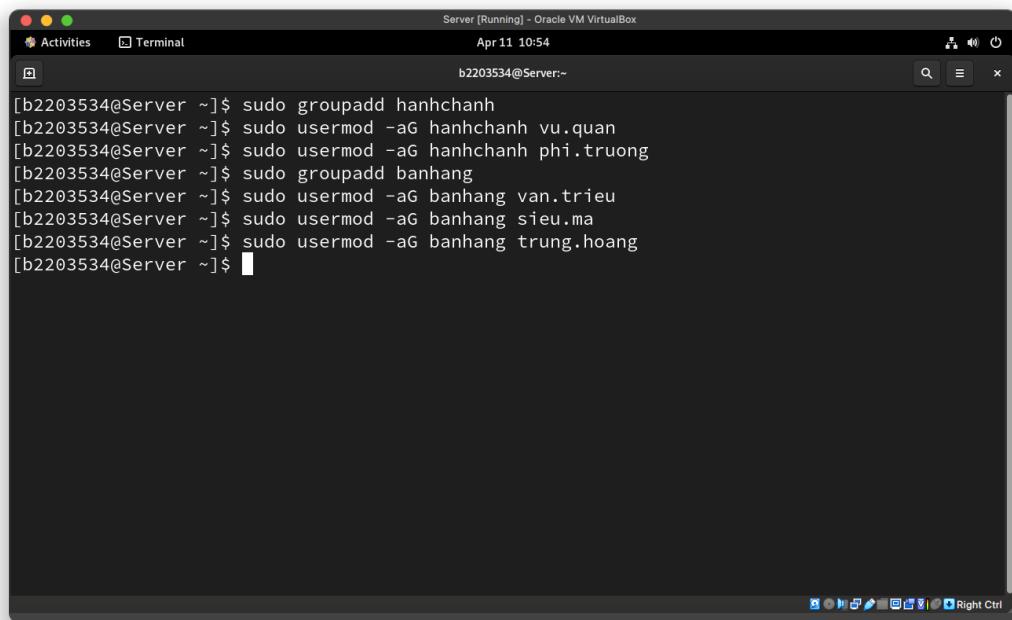
Ta sử dụng lệnh groupadd <group-name> để thêm nhóm người dùng và thêm người dùng vào nhóm bằng lệnh usermod -aG <group-name> <username>. Dưới đây là ví dụ tạo nhóm bangiamdoc và thêm luu.bi và luong.giacat vào nhóm này (**Hình 14**).



Hình 14: Tạo nhóm bangiamdoc và thêm người dùng vào

```
1 sudo groupadd bangiamdoc
2 sudo usermod -aG bangiamdoc bi.luu
3 sudo usermod -aG bangiamdoc luong.giacat
```

Code 3: Tạo nhóm bangiamdoc và thêm người dùng vào
Các nhóm còn lại thực hiện tương tự (**Hình 15**).



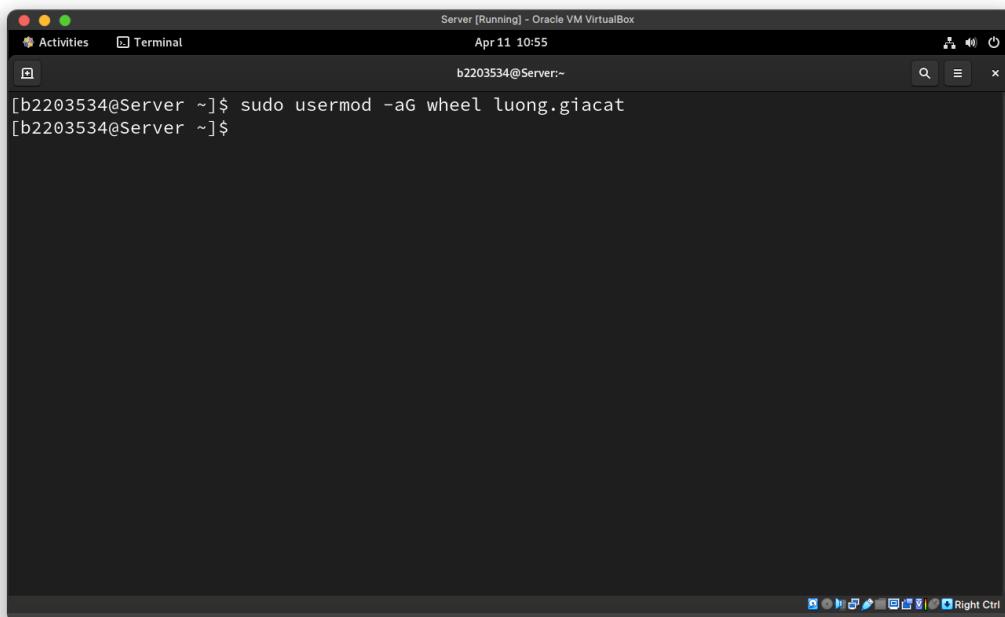
Hình 15: Tạo nhóm còn lại và thêm người dùng vào

```
1 sudo groupadd hanhchanh
2 sudo usermod -aG hanhchanh vu.quan
3 sudo usermod -aG hanhchanh phi.truong
4 sudo groupadd banhang
5 sudo usermod -aG banhang van.trieu
6 sudo usermod -aG banhang sieu.ma
7 sudo usermod -aG banhang trung.hoang
```

Code 4: Tạo nhóm còn lại và thêm người dùng vào

1.2.3 Cấp quyền sudo cho người dùng Gia Cát Lượng

Để cấp quyền sudo cho một người dùng, ta thêm người dùng đó nhóm sudo hoặc nhóm wheel. Bên dưới là minh họa việc thêm người dùng luong.giacat vào nhóm wheel (**Hình 16**).



Hình 16: Cấp quyền sudo cho người dùng Gia Cát Lượng

```
1 sudo usermod -aG wheel luong.giacat
```

Code 5: Cấp quyền sudo cho người dùng Gia Cát Lượng

1.3 (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.

Để tạo và phân quyền cho thư mục /data, ta thực theo các bước như (**Hình 17**).

```

[1] b2203534@Server ~]$ sudo groupadd truongphong
[2] b2203534@Server ~]$ sudo usermod -aG truongphong vu.quan
[3] b2203534@Server ~]$ sudo usermod -aG truongphong phi.truong
[4] b2203534@Server ~]$ sudo mkdir /data
[5] b2203534@Server ~]$ sudo setfacl -m g:bangiamdoc:rwx /data
[6] b2203534@Server ~]$ sudo setfacl -m g:truongphong:r-x /data
[7] b2203534@Server ~]$ sudo setfacl -m other::--- /data
[8] b2203534@Server ~]$ sudo chmod +t /data
[9] b2203534@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::---

[10] b2203534@Server ~]$
```

Hình 17: Tạo và phân quyền cho thư mục /data

Cụ thể các bước như sau:

1. Tạo nhóm **truongphong** và thêm người dùng vào.

```

1 sudo groupadd truongphong
2 sudo usermod -aG truongphong vu.quan
3 sudo usermod -aG truongphong phi.truong
```

Code 6: Tạo nhóm truongphong và thêm người dùng vào

2. Tạo thư mục **/data**.

```
1 sudo mkdir /data
```

Code 7: Tạo thư mục /data

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

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

Code 8: Phân quyền cho ban giám đốc

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

```
1 sudo setfacl -m g:truongphong:r-x /data
```

Code 9: Phân quyền cho trưởng phòng

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

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

Code 10: Phân quyền cho nhân viên

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

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

Code 11: Phân quyền cho chủ sở hữu

1.4 (10%) 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 10.0.2.50/24 đến 10.0.2.100/24
- Địa chỉ gateway: 10.0.2.1
- DNS server: 10.0.2.2 và 8.8.8.8

1.4.1 Cài đặt dịch vụ DHCP



Hình 18: Cài đặt dịch vụ dhcp-server

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

Code 12: Cài đặt dịch vụ dhcp-server

1.4.2 Cấu hình dịch vụ DHCP

Ta chỉnh sửa nội dung file /etc/dhcp/dhcpd.conf để cấu hình dịch vụ DHCP (**Hình 19**).

```

# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
subnet 10.0.2.0 netmask 255.255.255.0 {
    range 10.0.2.50 10.0.2.100;
    option routers 10.0.2.1;
    option domain-name-servers 10.0.2.2, 8.8.8.8;
    default-lease-time 600;
    max-lease-time 7200;
}

```

[Wrote 16 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo Right Ctrl

Hình 19: Cấu hình dịch vụ DHCP

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

```

1 subnet 10.0.2.0 netmask 255.255.255.0 {
2     range 10.0.2.50 10.0.2.100;
3
4     option routers 10.0.2.1;
5
6     option domain-name-servers 10.0.2.2, 8.8.8.8;
7
8     default-lease-time 600;
9     max-lease-time 7200;
10 }

```

Code 13: Nội dung file /etc/dhcp/dhcpd.conf

Dòng 1 Cấu hình subnet là 255.255.255.0 với địa chỉ mạng là 10.0.2.0.

Dòng 2 Cấu hình range địa chỉ IP cho các máy desktop là từ 10.0.2.50 đến 10.0.2.100.

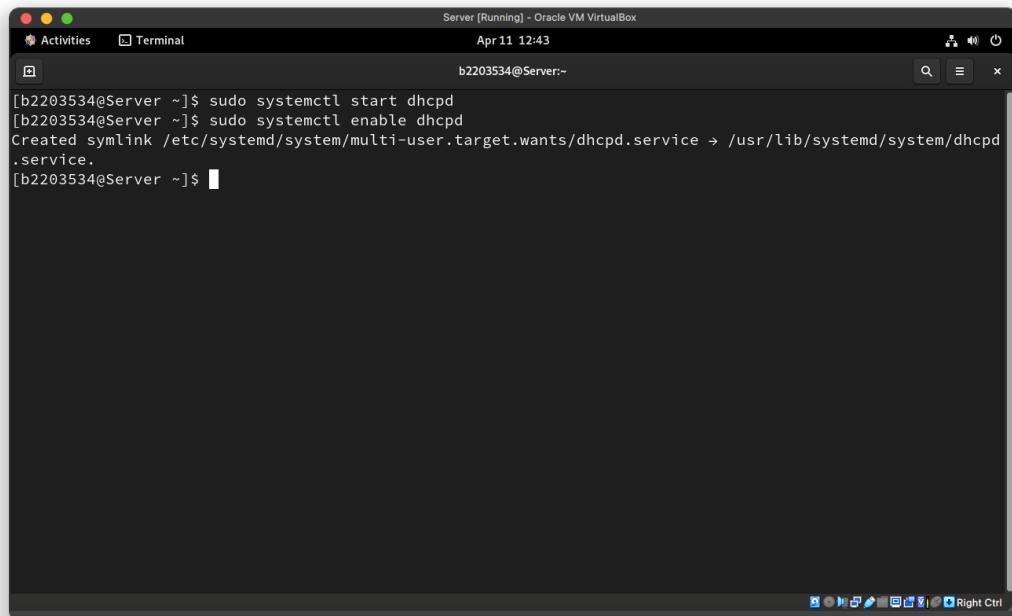
Dòng 4 Cấu hình địa chỉ gateway là 10.0.2.1.

Dòng 6 Cấu hình địa chỉ DNS server là 10.0.2.2, 8.8.8.8.

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).

1.4.3 Khởi động dịch vụ DHCP



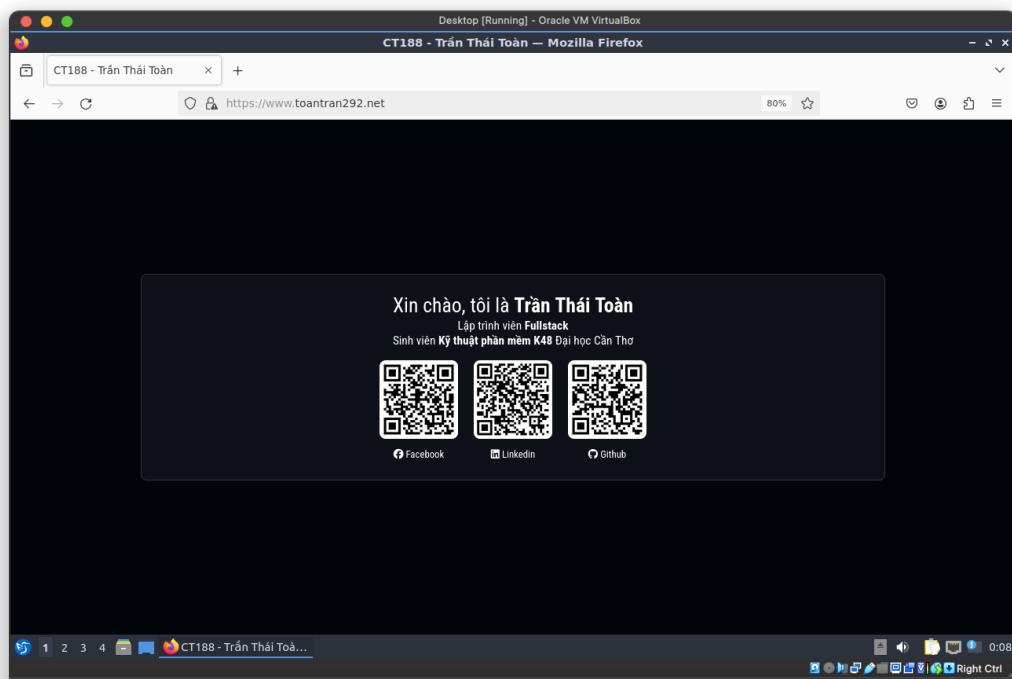
Hình 20: Khởi động dịch vụ DHCP

```
1 sudo systemctl start dhcpcd
2 sudo systemctl enable dhcpcd
```

Code 14: Khởi động dịch vụ DHCP

1.4.4 Kiểm tra dịch vụ DHCP

Sau khi cấu hình xong DHCP, ta sẽ dùng máy desktop (**Hình 21**) để kiểm tra bằng cách kết nối vào mạng QTHT và kiểm tra địa chỉ IP của máy desktop (**Hình 22**).



Hình 21: Truy cập vào internet bằng máy desktop

```

b2203534@Desktop:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.50 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::1828:2b4:622:6af6 prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:98:55:cc txqueuelen 1000 (Ethernet)
                    RX packets 16360 bytes 19766338 (19.7 MB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 7932 bytes 883863 (883.8 KB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 730 bytes 87710 (87.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 730 bytes 87710 (87.7 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

b2203534@Desktop:~$ 

```

Hình 22: Kiểm tra địa chỉ IP của máy desktop (10.0.2.50)

1.5 (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 các trưởng phòng 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 Gia Cát Lượng để có SSH tới server.

1.5.1 Cài đặt dịch vụ SSH

```

[b2203534@Server ~]$ sudo dnf install openssh-server -y
CentOS Stream 9 - BaseOS                               958 kB/s | 8.0 MB   00:08
CentOS Stream 9 - AppStream                            3.8 MB/s | 19 MB   00:04
CentOS Stream 9 - Extras packages                     59 kB/s | 16 kB   00:00
Package openssh-server-8.7p1-38.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[b2203534@Server ~]$ sudo systemctl enable sshd
[b2203534@Server ~]$ sudo systemctl start sshd
[b2203534@Server ~]$ 

```

Hình 23: Cài đặt và kích hoạt dịch vụ openssh-server

```

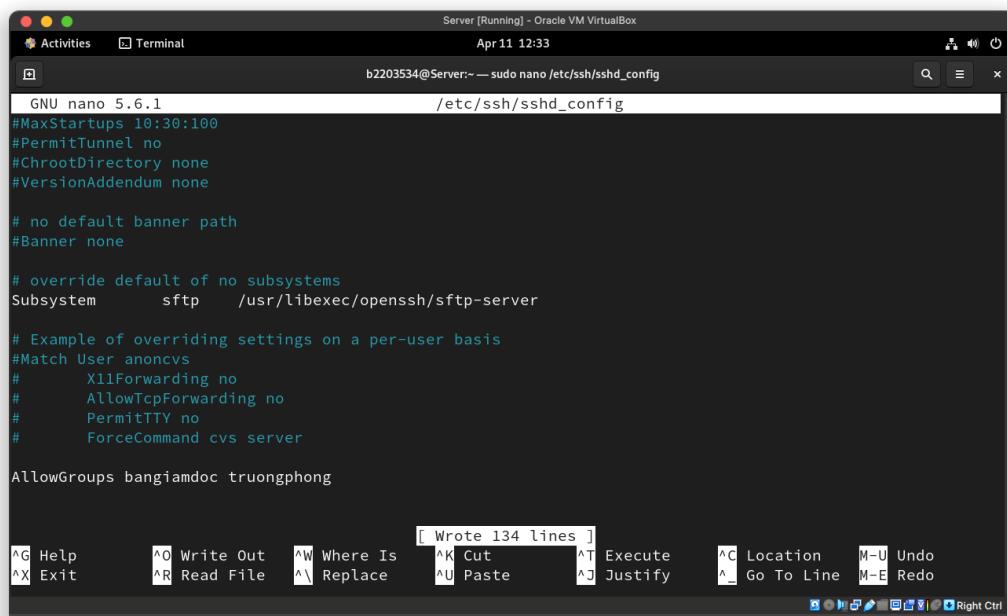
1 sudo dnf install openssh-server -y
2 sudo systemctl start sshd
3 sudo systemctl enable sshd

```

Code 15: Cài đặt và kích hoạt dịch vụ openssh-server

1.5.2 Cấu hình chỉ cho phép thành viên trong ban giám đốc và các trưởng phòng mới có quyền điều khiển từ xa

Ta sẽ cấu hình file `/etc/ssh/sshd_config` (**Hình 24**) để cấu hình chỉ cho phép một nhóm người dùng hoặc người dùng có thể sử dụng dịch vụ SSH.



```

#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 truongphong

```

[Wrote 134 lines]

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

Hình 24: Cấu hình chỉ cho phép bangiamdoc và truongphong sử dụng dịch vụ SSH để điều khiển từ xa

- `AllowGroups bangiamdoc truongnhom`: Cho phép nhóm bangiamdoc và nhóm truongnhom 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`).

1.5.3 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 25**)

```

GNU nano 5.6.1          /etc/ssh/sshd_config          Modified
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
PasswordAuthentication no

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
[ Wrote 136 lines ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File   ^V Replace     ^U Paste      ^J Justify   ^L Go To Line
^_             ^_             ^_             ^_             ^_             ^_

```

Hình 25: Cấu hình chỉ cho phép chứng thực bằng private key

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

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

Ta sử dụng lệnh ssh-keygen để tạo private/public key.

```

[b2203534@Server ~]$ sudo -u luong.giacat ssh-keygen
[sudo] password for b2203534:
Generating public/private rsa key pair.
Enter file in which to save the key (/home/luong.giacat/.ssh/id_rsa):
Created directory '/home/luong.giacat/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/luong.giacat/.ssh/id_rsa
Your public key has been saved in /home/luong.giacat/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:N1NjBU+VoFx/pgtbr/b+9S+mFD0a2TjfBPW86lwgAGI luong.giacat@Server
The key's randomart image is:
+---[RSA 3072]---+
|   E . .+++.o|
|   . . . o+... |
|   . o+ o.o|
|   .o o =.|
|   S +.*.o.o|
|   . 0.0.o.|
|   * + ooo|
|   +.o*.o|
|   +Bo+o|
+---[SHA256]---+
[b2203534@Server ~]$ 

```

Hình 26: Tạo public/private key bằng ssh-keygen

Tiếp theo, ta cần đổi tên của public key thành authenized_keys và phân lại quyền cho file này (**Hình 27**).

```
[b2203534@Server ~]$ sudo -u luong.giacat mv /home/luong.giacat/.ssh/id_rsa.pub \
> /home/luong.giacat/.ssh/authorized_keys
[b2203534@Server ~]$ sudo -u luong.giacat ls -l /home/luong.giacat/.ssh/authorized_keys
-rw-r--r--. 1 luong.giacat luong.giacat 573 Apr 11 11:40 /home/luong.giacat/.ssh/authorized_keys
[b2203534@Server ~]$ sudo -u luong.giacat chmod 600 /home/luong.giacat/.ssh/authorized_keys
[b2203534@Server ~]$ sudo -u luong.giacat ls -l /home/luong.giacat/.ssh/authorized_keys
-rw-----. 1 luong.giacat luong.giacat 573 Apr 11 11:40 /home/luong.giacat/.ssh/authorized_keys
[b2203534@Server ~]$
```

Hình 27: Đổi tên và phân quyền cho file public key

- Đổi tên tập tin public key thành authorized_key cho người dùng Gia Cát Lượng.

```
1 sudo -u luong.giacat mv \
/home/luong.giacat/.ssh/id_rsa.pub \
/home/luong.giacat/.ssh/authorized_keys
```

Code 16: Đổi tên tập tin public key thành authorized_key cho người dùng Gia
Cát Lượng

- Cho phép Gia Cát Lượng đọc và ghi vào tập tin authorized_key.

```
1 sudo -u luong.giacat chmod 600 \
/home/luong.giacat/.ssh/authorized_keys
```

Code 17: Cho phép Gia Cát Lượng đọc và ghi vào tập tin authorized_key

1.6 (10%) Cài đặt và cấu hình dịch vụ máy chủ Web trên server sử dụng Docker

Cài đặt và cấu hình dịch vụ máy chủ Web trên server. Tạo một trang web cho công ty có tên miền lautamquoc.com với nội dung trang chủ giới thiệu về các thành viên trong công ty.

1.6.1 Xây dựng trang web

Ta sẽ sử dụng mã nguồn trang web (sử dụng thư viện ReactJS và Vitejs): <https://github.com/toantran292/lautamquoc.com>

	toantran292	fix name file	1392df7 · 5 days ago	7 Commits
	.nginx	fix name file	5 days ago	
	public	init	last week	
	src	complete	last week	
	.eslintrc.cjs	init	last week	
	.gitignore	init	last week	
	Dockerfile	fix Dockerfile	5 days ago	
	README.md	first commit	last week	
	docker-compose.yml	adding dockerfile	last week	
	index.html	init	last week	
	package-lock.json	init	last week	
	package.json	init	last week	
	tsconfig.json	init	last week	
	tsconfig.node.json	init	last week	
	vite.config.ts	init	last week	

Hình 28: Cấu trúc trang web lautamquoc.com

1.6.2 *Cấu hình cho Docker và nginx*

Ta cần quan tâm đến các file sau:

- /Dockerfile: dùng 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;"]

```

Code 18: Nội dung file /Dockerfile

Có ý nghĩa cụ thể như sau:

Dòng 01 - 11: Tạo môi trường phát triển bên trong docker container

- 1 Sử dụng image node:20-alpine làm base image.
- 3 Đặt /app làm thư mục làm việc bên trong image.
- 5 Sao chép tập tin package.json và package-lock.json vào bên trong image.
- 7 Cài đặt các thư viện.
- 9 Sao chép toàn bộ mã nguồn dự án vào image.
- 11 Câu lệnh npm run dev được dùng để chạy dev server (do Vitejs cấu hình).

Dòng 13 - 15: Build production

- 13 Sử dụng image từ image development làm base image.

15 Câu lệnh `npm run build` sẽ tạo ra bản build của dự án nằm ở thư mục `/dist`

Dòng 17 - 27: Cấu hình cho nginx

17 Sử dụng image `nginx:alpine` làm base image.

19 Sao chép file cấu hình `/nginx.conf` từ image production vào image và đồng thời đổi tên thành `/default.conf`

21 Đặt `/usr/share/nginx/html` làm thư mục làm việc.

23 Xóa trang web mặc định của nginx.

25 Sao chép bản build từ image production.

27 Lệnh `nginx -g daemon off;` sẽ chạy nginx và không thoát ra.

– `/docker-compose.yml`: dùng để build và run các container.

```
1 version: '3.8'  
2  
3 services:  
4   lautamquoc.com:  
5     build: .  
6     container_name: lautamquoc.com  
7     ports:  
8       - '80:80'
```

Code 19: Nội dung file `/docker-compose.yml`

Có ý nghĩa cụ thể như sau:

Dòng 1 Sử dụng phiên bản 3.8 của docker-compose.

Dòng 4 Tạo một service có tên `lautamquoc.com`.

Dòng 5 Sử dụng Dockerfile để build image cho services này.

Dòng 6 Đặt tên cho container là `lautamquoc.com`.

Dòng 8 Chỉ định cổng 80 của máy hót sẽ được map vào cổng 80 của container.

– `./nginx/nginx.conf`: dùng để cấu hình cho nginx.

```

1 server {
2     server_name lautamquoc.com www.lautamquoc.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 }
```

Code 20: Nội dung file /.nginx/nginx.conf

Có ý nghĩa cụ thể như sau:

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

Dòng 4 Cấu hình nginx sẽ lắng nghe ở port 80.

Dòng 7 Cấu hình thư mục root là /usr/share/nginx/html.

Dòng 8 Cấu hình file index mặc định là index.html.

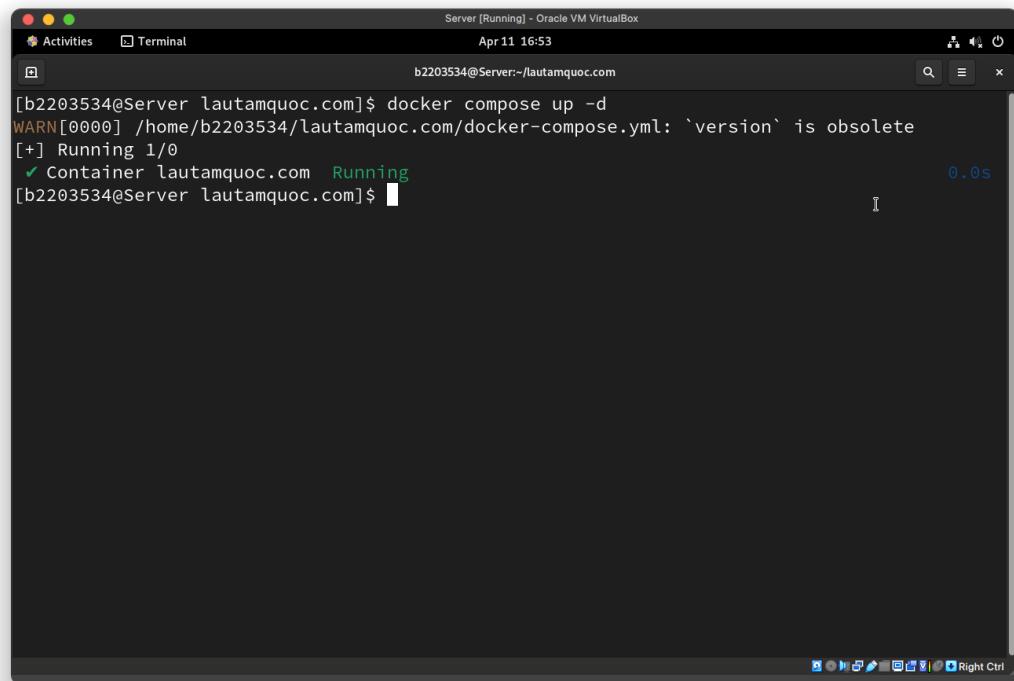
Dòng 9 Cấu hình thử các file tĩnh nếu không tìm thấy file index.html, do đây là trang web SPA (Single Page Application) nên ta sẽ thử các file tĩnh trước khi trả về trang index.html.

Dòng 12 Cấu hình trang 50x.html.

Dòng 15 Cấu hình thư mục root cho trang 50x.html là /usr/share/nginx/html.

1.6.3 Khởi chạy trang web trên máy server

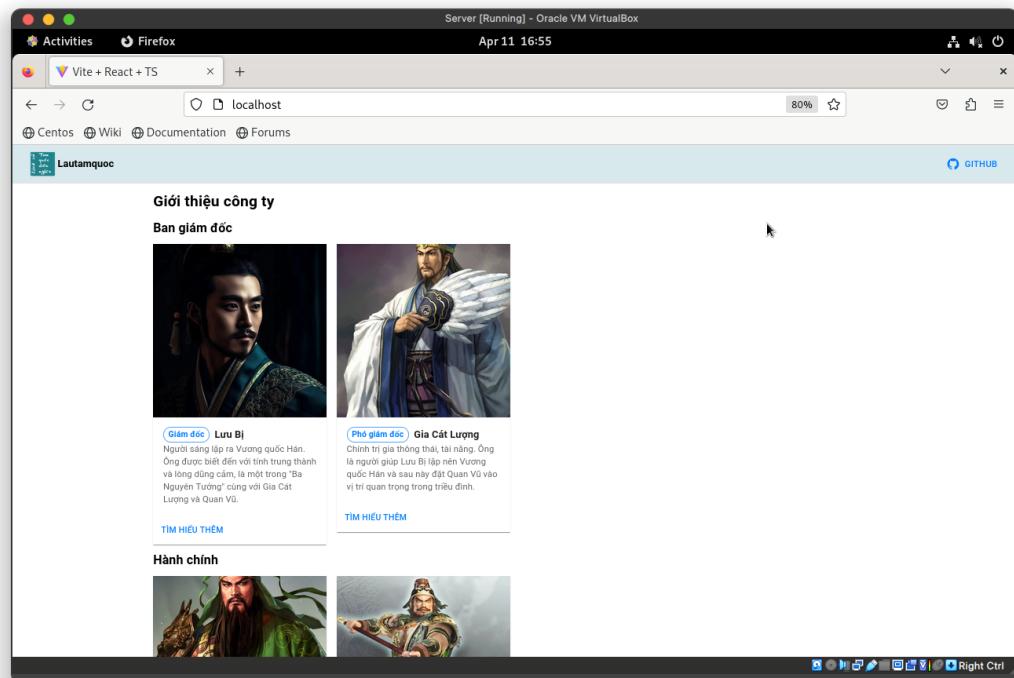
Để chạy thử web trên máy server, ta dùng lệnh docker compose up để docker sẽ tự động kéo các image từ cloud về và build image cho service lautamquoc.com sau đó khởi chạy container từ image này như (**Hình 29**).



```
[b2203534@Server lautamquoc.com]$ docker compose up -d
WARN[0000] /home/b2203534/lautamquoc.com/docker-compose.yml: `version` is obsolete
[+] Running 1/0
✓ Container lautamquoc.com  Running
[b2203534@Server lautamquoc.com]$
```

Hình 29: Khởi chạy trang web bằng docker compose up

Lúc này, trang web sẽ chạy trên cổng 80 của máy server như đã cấu hình trong file docker-compose.yml (**Hình 30**).



Hình 30: Giao diện trang web lautamquoc.com

Ta có thể chỉnh sửa DNS của máy server để trả tên miền lautamquoc.com về địa chỉ localhost để kiểm tra nginx đã hoạt động chính xác hay chưa (**Hình 31**).

```

GNU nano 5.6.1          /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

127.0.0.1 lautamquoc.com www.lautamquoc.com

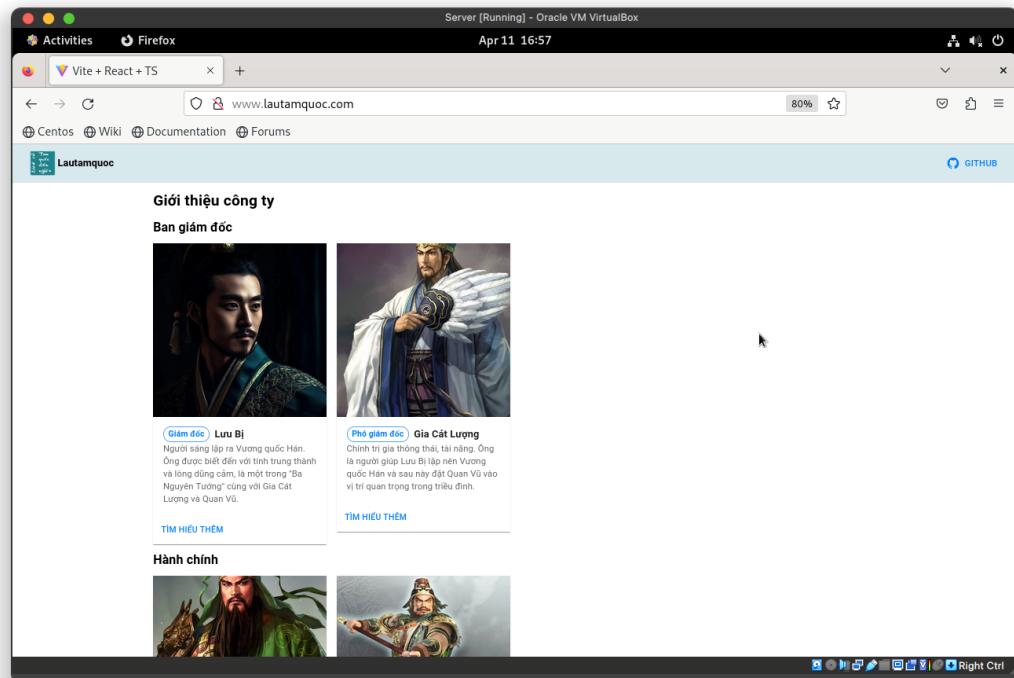
[ Wrote 4 lines ]

```

^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 31: Chỉnh sửa file /etc/hosts để trỏ tên miền lautamquoc.com về địa chỉ localhost

Sau khi cấu hình xong, ta có thể truy cập vào trang web theo địa chỉ như sau <http://lautamquoc.com> (**Hình 32**).



Hình 32: Truy cập vào trang web từ server qua địa chỉ <http://lautamquoc.com>

1.7 (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server

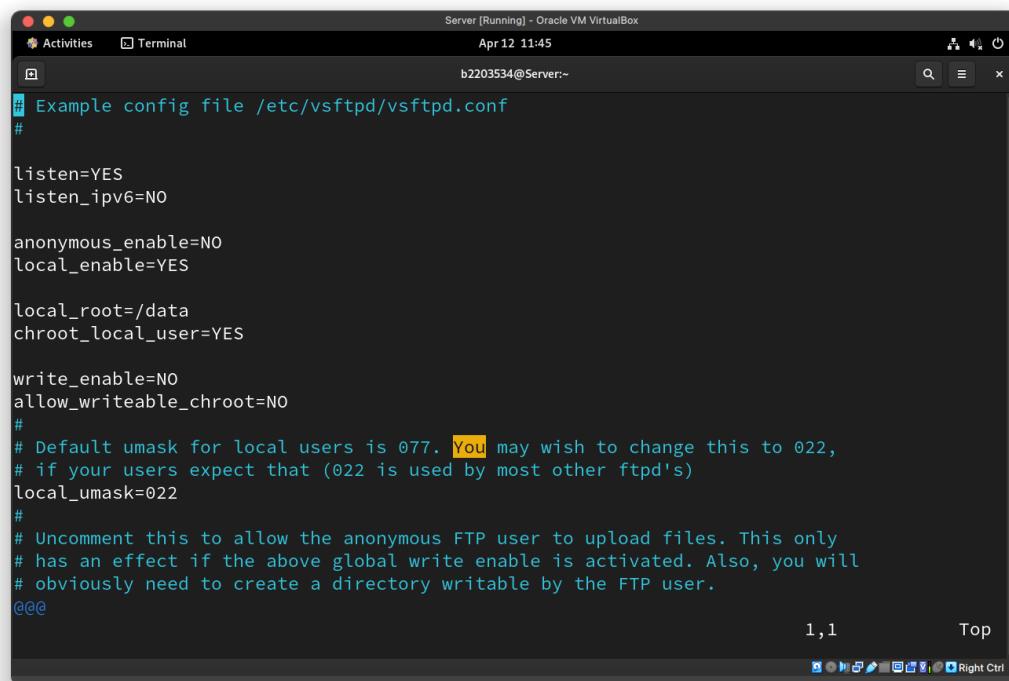
Cài đặt và cấu hình dịch vụ máy chủ FTP trên server. Cấu hình chỉ cho phép người dùng download (không được upload) dữ liệu từ thư mục /data trên server. Không cho phép người dùng chuyển sang thư mục khác, chỉ được làm việc trong thư mục /data.

1.7.1 Cài đặt dịch vụ FTP

Để cài đặt dịch vụ FTP, ta sử dụng lệnh sudo dnf install vsftpd. Sau đó ta tiến hành cấu hình dịch vụ trong file /etc/vsftpd/vsftpd.conf.

1.7.2 Cấu hình dịch vụ FTP

Ta thực hiện việc cấu hình cho dịch vụ FTP như (**Hình 33**).



```
# Example config file /etc/vsftpd/vsftpd.conf
#
listen=YES
listen_ipv6=NO

anonymous_enable=NO
local_enable=YES

local_root=/data
chroot_local_user=YES

write_enable=NO
allow_writeable_chroot=NO
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#@@

1,1          Top
```

Hình 33: Nội dung file /etc/vsftpd/vsftpd.conf

```

1 ...
2
3 listen=YES
4 listen_ipv6=NO
5
6 anonymous_enable=NO
7 local_enable=YES
8
9 local_root=/data
10 chroot_local_user=YES
11
12 write_enable=NO
13 allow_writeable_chroot=NO
14
15 ...

```

Code 21: Nội dung file /etc/vsftpd/vsftpd.conf

Dòng 3 Câu hình cho phép máy chủ FTP lắng nghe các kết nối từ máy khác.

Dòng 4 Câu hình vô hiệu hóa lắng nghe trên IPv6.

Dòng 6 Câu hình không cho phép người vô danh truy cập.

Dòng 7 Câu hình cho phép các tài khoản cục bộ truy cập.

Dòng 9 Câu hình xác định thư mục gốc là /data.

Dòng 10 Câu hình giới hạn hoạt động người dùng trong thư mục được xác định bởi local_root.

Dòng 12 Câu hình vô hiệu hóa quyền ghi cho người dùng (không cho phép upload).

Dòng 13 Câu hình vô hiệu hóa quyền ghi trong môi trường /chroot (không cho phép upload).

Sau đó, ta cần khởi chạy dịch vụ FTP .

```

1 sudo systemctl start vsftpd
2 sudo systemctl enable vsftpd

```

Code 22: Khởi chạy dịch vụ FTP

1.7.3 Sử dụng máy desktop để kiểm tra kết nối tới dịch vụ FTP

Trên máy server ta tạo ra một file test.txt trong thư mục /data như (**Hình 34**)

```
[b2203534@Server ~]$ sudo vi /data/test.txt
[b2203534@Server ~]$ sudo ls -l /data
total 4
-rw-r--r--. 1 root root 9 Apr 12 04:15 test.txt
[b2203534@Server ~]$ sudo cat /data/test.txt
B2203534
[b2203534@Server ~]$
```

Hình 34: Tạo file /data/test.txt trên máy server

Trên máy desktop ta kết nối tới dịch vụ FTP bằng cách sử dụng lệnh như sau `ftp <ftp-host>`, và dùng các lệnh `get <file-name>` và `put <file-name>` để download và upload file như (**Hình 35**).

```
b2203534@Desktop:~$ ftp 10.0.2.2
Connected to 10.0.2.2.
220 (vsFTPd 3.0.5)
Name (10.0.2.2:b2203534): vu.quan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||6946|).
150 Opening BINARY mode data connection for test.txt (9 bytes).
100% |*****| 9 266.33 Kib/s 00:00 ETA
226 Transfer complete.
9 bytes received in 00:00 (10.83 Kib/s)
ftp> put test.txt test2.txt
local: test.txt remote: test2.txt
229 Entering Extended Passive Mode (|||37214|).
550 Permission denied.
ftp> exit
221 Goodbye.
b2203534@Desktop:~$ cat test.txt
B2203534
b2203534@Desktop:~$
```

Hình 35: Kiểm tra kết nối tới dịch vụ FTP trên máy desktop

1.8 (5%) Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền lautamquoc.com

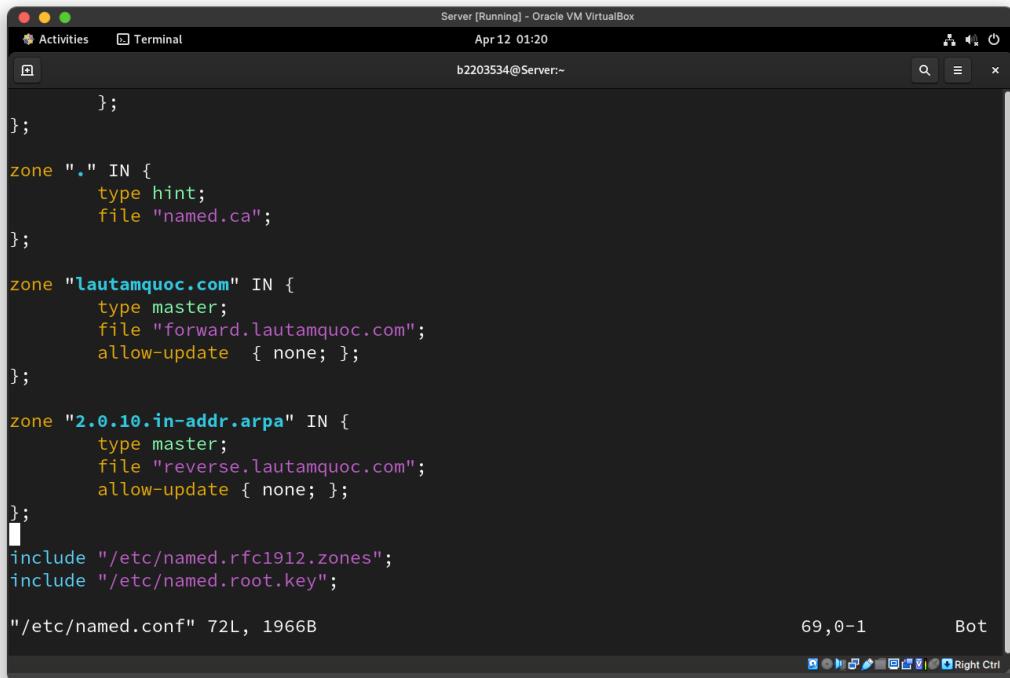
Tên miền: `www.lautamquoc.com <—> IP: 10.0.2.2 (server IP)`

Tên miền: ftp.lautamquoc.com <→ IP: 10.0.2.2 (server IP)

1.8.1 Cài đặt dịch vụ DNS

Để cài đặt dịch vụ DNS, ta dùng lệnh sudo dnf install bind bind-utils

1.8.2 Cấu hình máy chủ DNS trên server



The screenshot shows a terminal window titled "Server [Running] - Oracle VM VirtualBox". The window displays the contents of the /etc/named.conf file. The configuration includes several zones: a root zone ("."), a master zone for "lautamquoc.com" (IP 10.0.2.2), and a master zone for the reverse zone "2.0.10.in-addr.arpa". The file also includes standard include statements for RFC 1912 zones and a root key.

```
};  
};  
  
zone "." IN {  
    type hint;  
    file "named.ca";  
};  
  
zone "lautamquoc.com" IN {  
    type master;  
    file "forward.lautamquoc.com";  
    allow-update { none; };  
};  
  
zone "2.0.10.in-addr.arpa" IN {  
    type master;  
    file "reverse.lautamquoc.com";  
    allow-update { none; };  
};  
  
include "/etc/named.rfc1912.zones";  
include "/etc/named.root.key";  
  
"/etc/named.conf" 72L, 1966B  
69,0-1 Bot
```

Hình 36: Nội dung file /etc/named.conf

```
1 ...  
2  
3 zone "." IN {  
4     ...  
5 };  
6  
7 zone "lautamquoc.com" IN {  
8     type master;  
9     file "forward.lautamquoc.com";  
10    allow-update { none; };  
11};  
12  
13 zone "2.0.10.in-addr.arpa" IN {  
14     type master;  
15     file "reverse.lautamquoc.com";  
16     allow-update { none; };  
17};  
18  
19 ...
```

Code 23: Nội dung file /etc/named.conf

```
$TTL 1D
@ IN SOA @ lautamquoc.com. (
    0 ; serial
    1D ; refresh
    1H ; retry
    1W ; expire
    3H ) ; minimum
@ IN NS dns.lautamquoc.com.
dns IN A 10.0.2.2
www IN A 10.0.2.2
ftp IN A 10.0.2.2

~/var/named/forward.lautamquoc.com" 12L, 207B written
```

Hình 37: Nội dung file /etc/named/forward.lautamquoc.com

```
1 $TTL 1D
2 @ IN SOA @ lautamquoc.com. (
3                         0 ; serial
4                         1D ; refresh
5                         1H ; retry
6                         1W ; expire
7                         3H ) ; minimum
8 @ IN NS dns.lautamquoc.com.
9 dns IN A 10.0.2.2
10 www IN A 10.0.2.2
11 ftp IN A 10.0.2.1
```

Code 24: NỘI DUNG FILE /etc/named/forward.lautamquoc.com

Hình 38: Nội dung file /etc/named/reverse.lautamquoc.com

```
1 $TTL 1D
2 @ IN SOA @ lautamquoc.com. (
3                                     0 ; serial
4                                     1D ; refresh
5                                     1H ; retry
6                                     1W ; expire
7                                     3H ) ; minimum
8 @ IN NS dns.lautamquoc.com.
9 dns IN A 10.0.2.2
10 2 IN A www.lautamquoc.com.
11 2 IN A fpt.lautamquoc.com.
```

Code 25: NỘI DUNG FILE /etc/named/reverse.lautamquoc.com

1.8.3 Khởi động dịch vụ DNS

Ta khởi động dịch vụ DNS để áp dụng thay đổi.

```
1 sudo systemctl restart named  
2 sudo systemctl enable named
```

Code 26: Khởi động dịch vụ DNS

1.8.4 Kiểm tra trên máy desktop

Ta sử dụng máy desktop để kiểm tra máy chủ DNS đã cấu hình đúng hay chưa (**Hình 39**).

```

Desktop [Running] - Oracle VM VirtualBox
File Actions Edit View Help
b2203534@Desktop:~$ nslookup www.lautamquoc.com
Server: 10.0.2.2
Address: 10.0.2.2#53
Name: www.lautamquoc.com
Address: 10.0.2.2

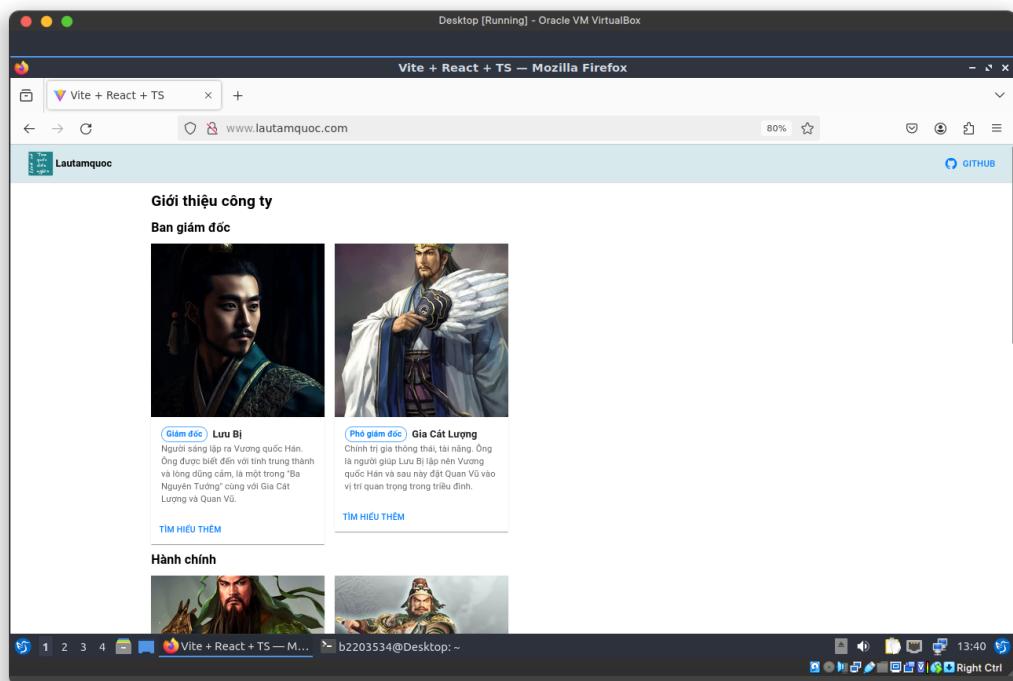
b2203534@Desktop:~$ nslookup ftp.lautamquoc.com
Server: 10.0.2.2
Address: 10.0.2.2#53

Name: ftp.lautamquoc.com
Address: 10.0.2.2
b2203534@Desktop:~$ 

```

Hình 39: Kiểm tra DNS trên máy desktop

Kiểm tra trên trình duyệt web (**Hình 40**)



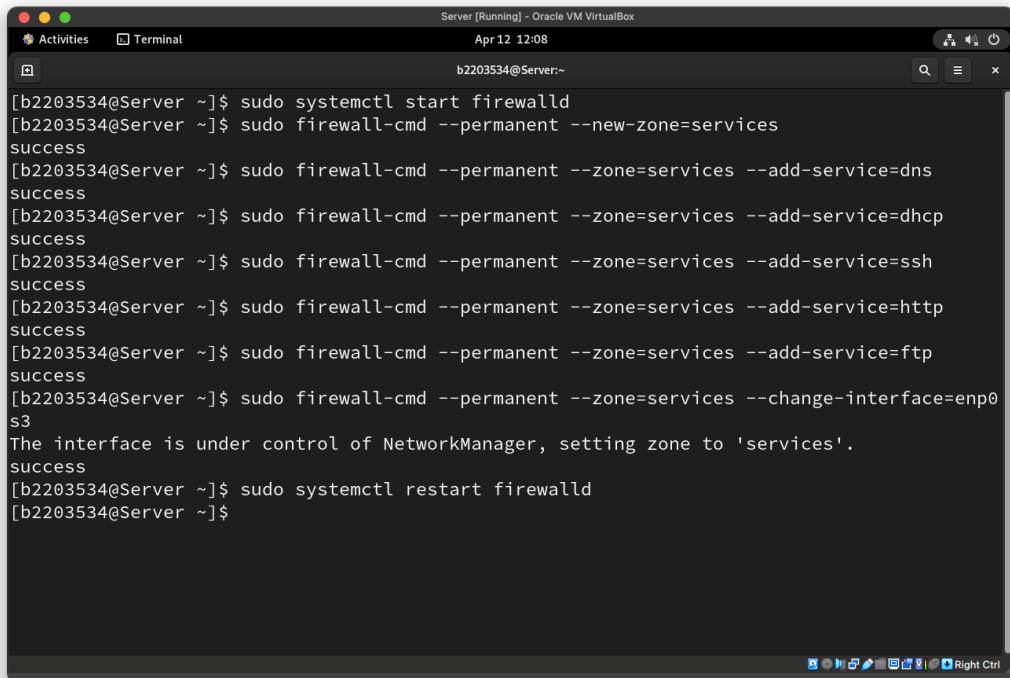
Hình 40: Sử dụng trình duyệt để kiểm tra DNS server

1.9 (5%) Cài đặt và cấu hình tường lửa trên server

- Có thể truy cập các dịch vụ DNS, DHCP, SSH, Web, FTP trên server. Các dịch vụ khác KHÔNG cập truy cập được.
- Chỉ máy desktop có thể SSH tới server, các máy khác KHÔNG SSH được.

1.9.1 Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP

Ta cấu hình như sau (**Hình 41**)



```
[b2203534@Server ~]$ sudo systemctl start firewalld
[b2203534@Server ~]$ sudo firewall-cmd --permanent --new-zone=services
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=dns
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=dhcp
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=ssh
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=http
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --add-service=ftp
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'services'.
success
[b2203534@Server ~]$ sudo systemctl restart firewalld
[b2203534@Server ~]$
```

Hình 41: Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP

Cụ thể các bước như sau

1. Khởi động dịch vụ firewalld

```
1 sudo systemctl start firewalld
```

Code 27: Tạo zone mới có tên là services

2. Tạo một zone mới có tên là services

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

Code 28: Tạo zone mới có tên là services

3. Thêm các dịch vụ DNS, DHCP, SSH, Web, FTP 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=ftp

```

Code 29: Thêm các dịch vụ DNS, DHCP, SSH, Web, FTP vào zone services

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

```

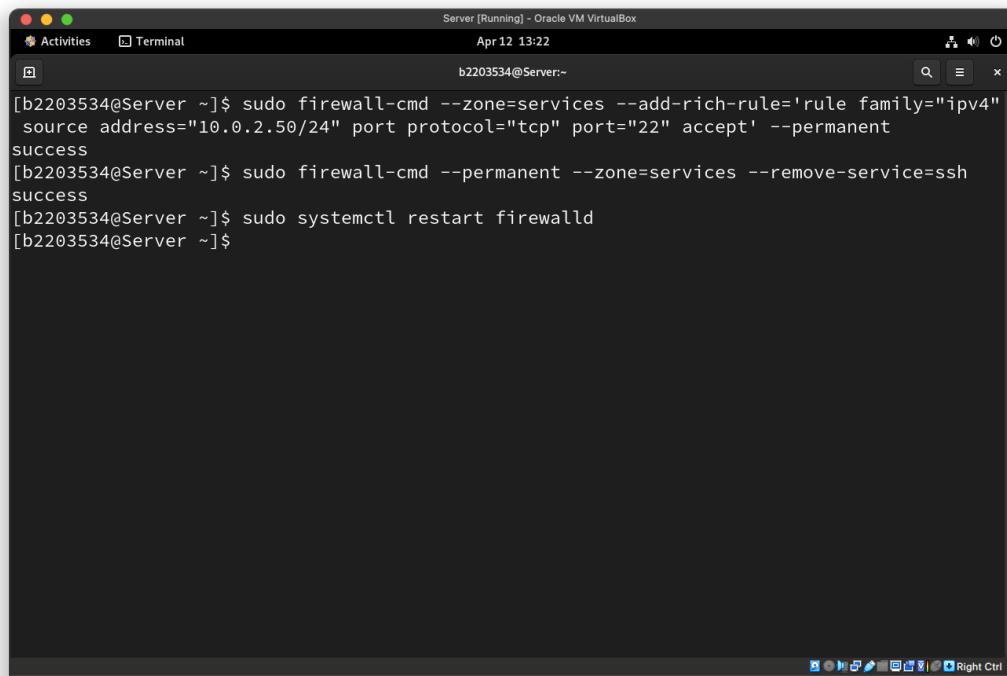
1 sudo systemctl restart firewalld

```

Code 30: Khởi động lại firewalld sau khi đổi zone mới

1.9.2 Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server

Ta cấu hình như sau (**Hình 42**)



Hình 42: Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server

Cụ thể các bước như sau

- Thêm một rule mới cho phép desktop (10.0.2.50) vào zone có port 22 (port của SSH)

```
1 sudo firewall-cmd --zone=services --add-rich-rule='rule
family="ipv4" source address="10.0.2.50/24" port
protocol="tcp" port="22" accept' --permanent
```

Code 31: Thêm một rule mới cho phép desktop (10.0.2.50) vào zone có port 22
(port của SSH)

2. Xóa dịch vụ SSH ra khỏi zone

```
1 sudo firewall-cmd --permanent --zone=services \
--remove-service=ssh
```

Code 32: Xóa dịch vụ SSH ra khỏi zone

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

```
1 sudo systemctl restart firewalld
```

Code 33: Khởi động lại firewalld sau khi thêm rule mới

1.10 (5%) Sử dụng dịch vụ cron và shell script tự động thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng trên server

- + Các thư mục cần sao lưu sao lưu: /home, /data, /etc.
- + Nơi lưu dữ liệu sao lưu: /mnt/backup.
 - Sao lưu mỗi ngày: thực hiện vào lúc 23:59 từ thứ 2 đến thứ 7, dữ liệu sẽ được nén lại và lưu với tên như sau: backup_<thứ> (ví dụ: backup_monday).
 - Sao lưu mỗi tuần: thực hiện vào lúc 23:59 ngày chủ nhật hàng tuần, dữ liệu sẽ được nén lại và lưu với tên như sau: backup_week<thứ tự tuần> (ví dụ: backup_week1).
 - Sao lưu mỗi tháng: thực hiện vào lúc 23:59 ngày 1 hàng tháng, dữ liệu sẽ được nén lại và lưu với tên backup_month1 nếu là tháng lẻ, backup_month2 nếu là tháng chẵn.

1.10.1 Tạo thư mục sao lưu dữ liệu

Ta sẽ tạo thư mục /mnt/backup để lưu trữ dữ liệu sao lưu.

```
1 sudo mkdir /mnt/backup
```

Code 34: Ta sẽ tạo thư mục /mnt/backup để lưu trữ dữ liệu sao lưu.

1.10.2 Viết shell script backup

Ta viết script thực hiện việc sao lưu dữ liệu theo các bước như sau:

- Tạo một biến lưu trữ tên file
- Nén thư mục /home, /data, /etc

A screenshot of a Linux desktop environment showing a terminal window titled "Server [Running] - Oracle VM VirtualBox". The terminal window has a dark background and contains the following text:

```
filename="/mnt/backup/backup_$(date + %A).zip"
echo "Compressing: $filename"
zip -qr $filename /home /data /etc
echo "Backup finish."
~/mnt/backup/backup_day.sh" 4L, 133B written
```

The terminal window also shows the date and time as "Apr 12 13:32" and the user as "b2203534@Server:~". The bottom right corner of the terminal window displays "4,21" and "All".

Hình 43: Script backup mỗi ngày

```
1 filename="/mnt/backup/backup_$(date + %A).zip"
2 echo "Compressing: $filename"
3 zip -qr $filename /home /data /etc
4 echo "Backup finish."
```

Code 35: Script backup mỗi ngày

A screenshot of a Linux desktop environment showing a terminal window titled "Server [Running] - Oracle VM VirtualBox". The terminal window has a dark background and contains the following text:

```
filename="/mnt/backup/backup_week$(date + %U).zip"
echo "Compressing: $filename"
zip -qr $filename /home /data /etc
echo "Backup finish."
~/mnt/backup/backup_week.sh" 4L, 137B written
```

The terminal window also shows the date and time as "Apr 12 13:33" and the user as "b2203534@Server:~". The bottom right corner of the terminal window displays "1,43" and "All".

Hình 44: Script backup mỗi tuần

```
1 filename="/mnt/backup/backup_week$(date + %U).zip"
2 echo "Compressing: $filename"
3 zip -qr $filename /home /data /etc
4 echo "Backup finish."
```

Code 36: Script backup mỗi tuần

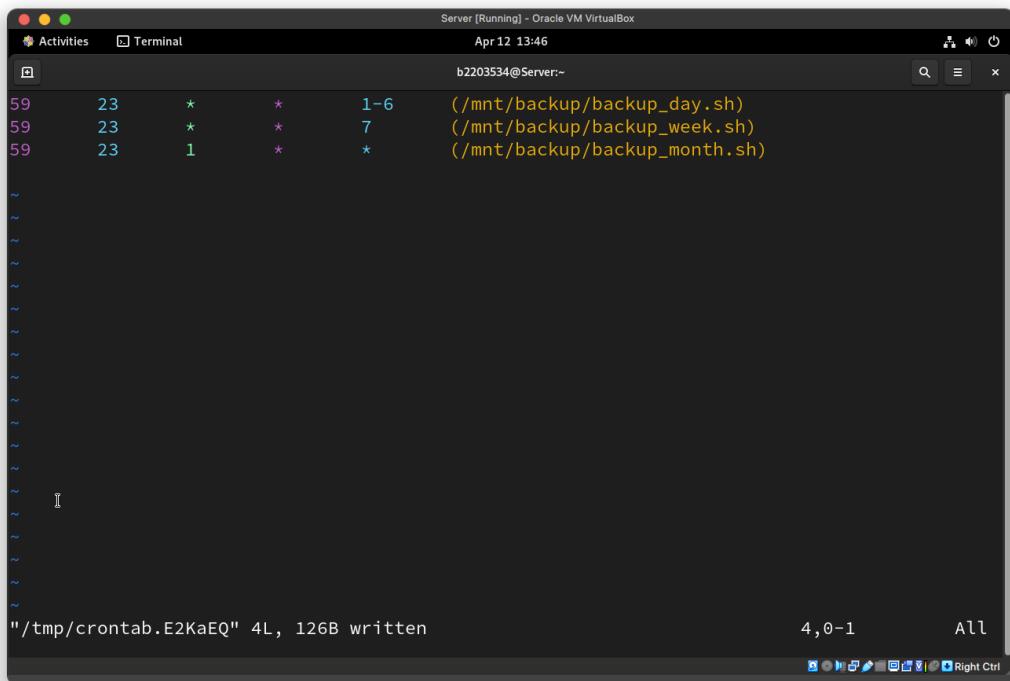
Hình 45: Script backup mỗi tháng

```
1 month=$(date + %m)
2
3 if ((month % 2 == 0))
4 then
5     suffix="2"
6 else
7     suffix="1"
8 fi
9
10 filename="/mnt/backup/backup_month$suffix.zip"
11 echo "Compressing: $filename"
12 zip -qr $filename /home /data /etc
13 echo "Backup finish."
```

Code 37: Script backup mỗi tháng

1.10.3 Cấu hình cron

Ta cấu hình cron thực thi script backup như sau



Hình 46: Cấu hình cron

```
1 59 23 * * 1-6 (/mnt/backup/backup_day.sh)
2 59 23 * * 0 (/mnt/backup/backup_week.sh)
3 59 23 1 * * (/mnt/backup/backup_month.sh)
```

Code 38: Cấu hình cron