

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	iv
---------------	----

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	20
1.7 (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server	20
1.8 (5%) Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền lautamquoc.com	20
1.8.1 Cài đặt dịch vụ DNS	20
1.8.2 Cấu hình máy chủ DNS trên server	21
1.8.3 Khởi động dịch vụ DNS	23
1.8.4 Kiểm tra trên máy desktop	23
1.9 (5%) Cài đặt và cấu hình tường lửa trên server	24
1.9.1 Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP	25

1.9.2	Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server .	26
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	27
1.10.1	Tạo thư mục sao lưu dữ liệu	27
1.10.2	Viết shell script backup	27
1.10.3	Cấu hình cron	29

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	Nội dung file /etc/named.conf	21
Hình 29	Nội dung file /etc/named/forward.lautamquoc.com	22
Hình 30	Nội dung file /etc/named/reverse.lautamquoc.com	23
Hình 31	Kiểm tra DNS trên máy desktop	24
Hình 32	Sử dụng trình duyệt để kiểm tra DNS server.....	24
Hình 33	Cấu hình tường lửa cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP ..	25
Hình 34	Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server	26
Hình 35	Script backup mỗi ngày	28

Hình 36	Script backup mỗi tuần.....	28
Hình 37	Script backup mỗi tháng	29
Hình 38	Cấu hình cron	30

DANH MỤC CODE

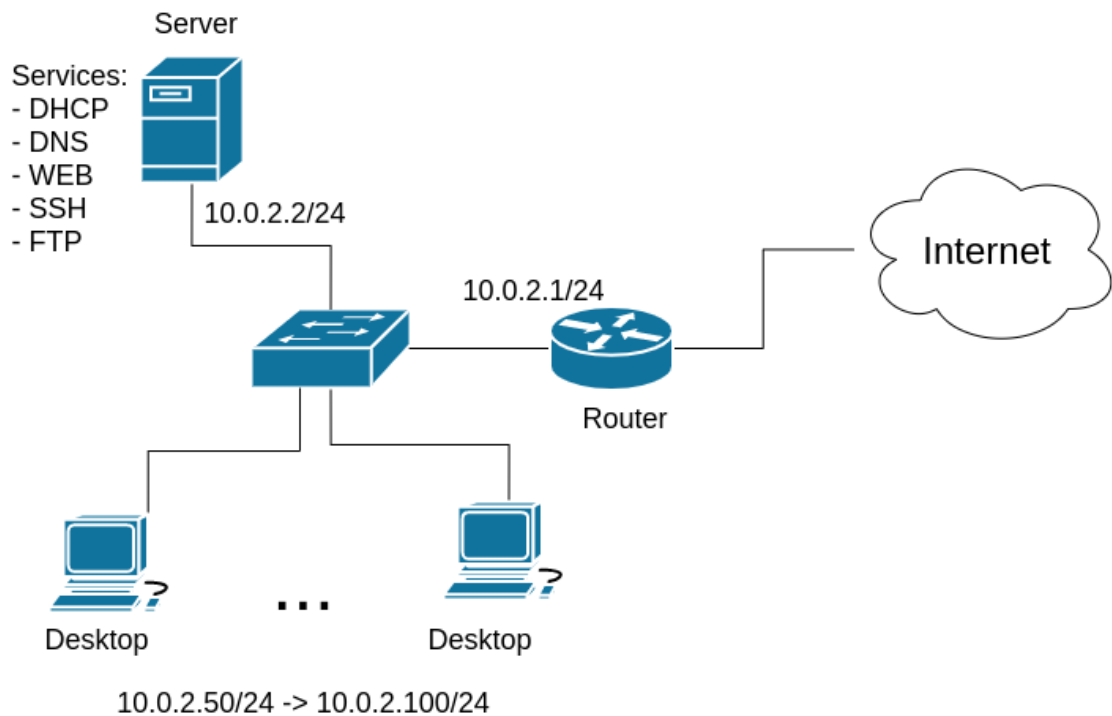
Code 1	Tạo và đặt mật khẩu cho tài khoản Lưu Bị	9
Code 2	Tạo và đặt mật khẩu cho các tài khoản còn lại	10
Code 3	Tạo nhóm bangiamdoc và thêm người dùng vào	11
Code 4	Tạo nhóm còn lại và thêm người dùng vào	11
Code 5	Cấp quyền sudo cho người dùng Gia Cát Lượng	12
Code 6	Tạo nhóm truongphong và thêm người 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 dhcp-server	14
Code 13	Cài đặt dịch vụ dhcp-server	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 /etc/named.conf	21
Code 19	Nội dung file /etc/named/forward.lautamquoc.com	22
Code 20	Nội dung file /etc/named/reverse.lautamquoc.com	23
Code 21	Khởi động dịch vụ DNS	23
Code 22	Tạo zone mới có tên là services	25
Code 23	Tạo zone mới có tên là services	25
Code 24	Thêm các dịch vụ DNS, DHCP, SSH, Web, FTP vào zone services	26
Code 25	Khởi động lại firewalld sau khi đổi zone mới	26
Code 26	Thêm một rule mới cho phép desktop (10.0.2.50) vào zone có port 22 (port của SSH)	27
Code 27	Xóa dịch vụ SSH ra khỏi zone	27
Code 28	Khởi động lại firewalld sau khi thêm rule mới	27
Code 29	Ta sẽ tạo thư mục /mnt/backup để lưu trữ dữ liệu sao lưu.	27
Code 30	Script backup mỗi ngày	28
Code 31	Script backup mỗi tuần	28
Code 32	Script backup mỗi tháng	29
Code 33	Cấu hình cron	30

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

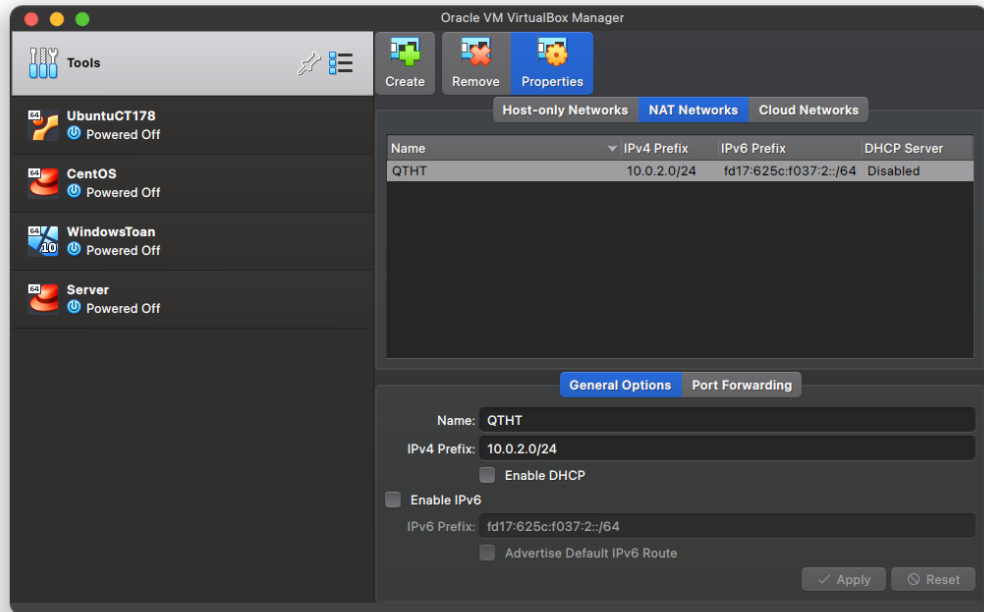
Bảng 2: Cấu hình máy Desktop

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	Cấu hình tự động sử dụng dịch vụ DHCP
Subnet mask	
Gateway	
DNS	

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 Tạo 1 NAT Network tên "QTHT"

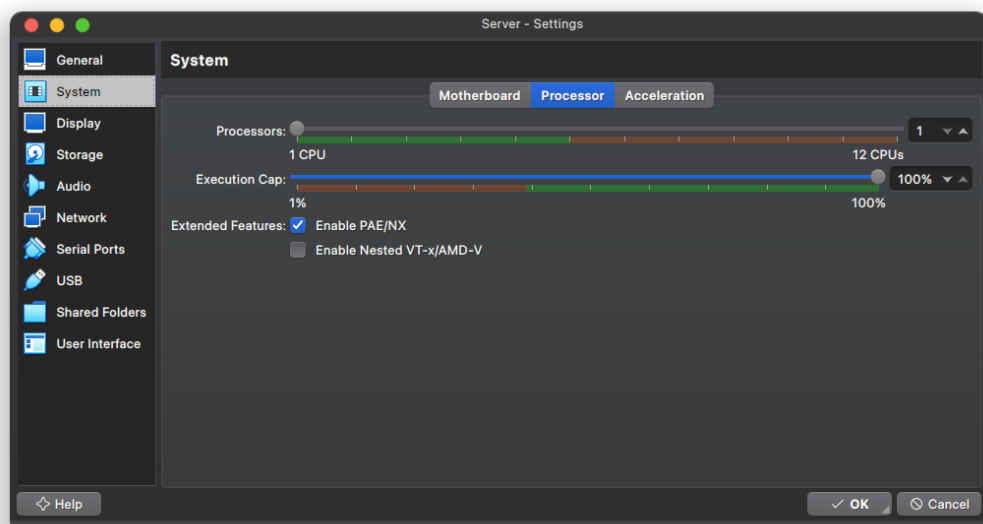


Hình 2: Cấu hình NAT Network QTHT

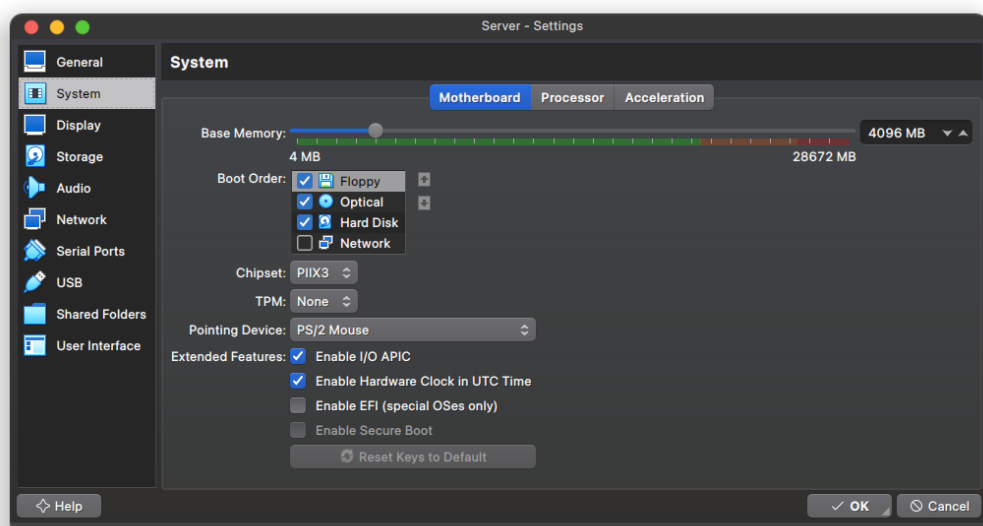
1.1.2 Tạo 2 máy ảo Server và Desktop

1.1.2.1 Server có cấu hình như sau:

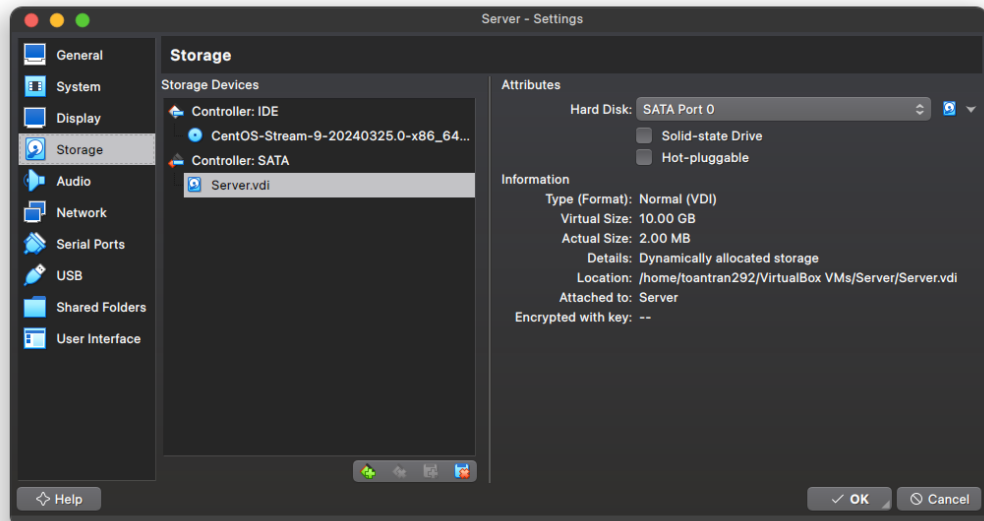
- Hệ điều hành: CentOS 9
- CPU: 1 Core (**Hình 3**)
- Ram: 4GB (**Hình 4**)
- Disk: 10GB (**Hình 5**)
- Network: NAT Network "QTHT" (**Hình 6**)
- IPv4: 10.0.2.2 (**Hình 7**)
- Subnet mask: 255.255.255.0 (**Hình 7**)
- Gateway: 10.0.2.1 (**Hình 7**)
- DNS: 10.0.2.1 (**Hình 7**)



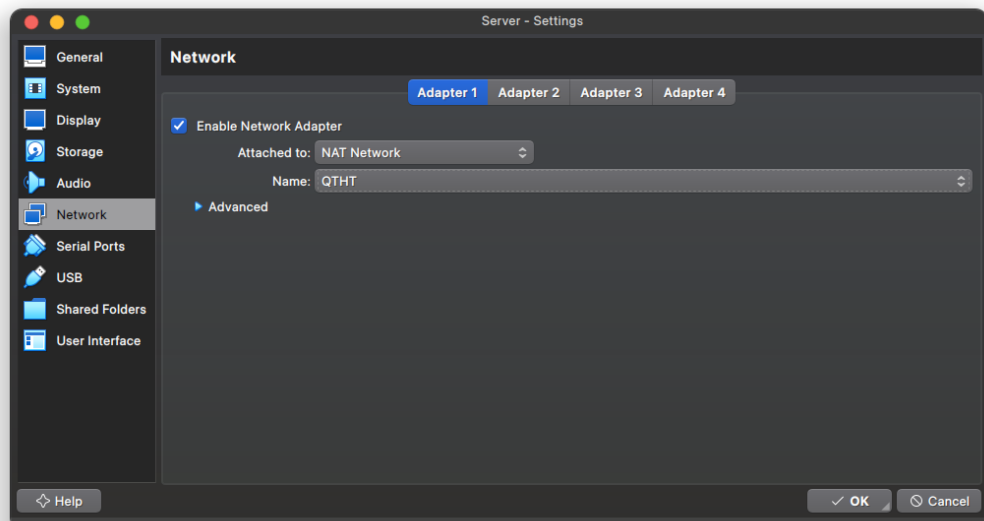
Hình 3: Số Core CPU của Server



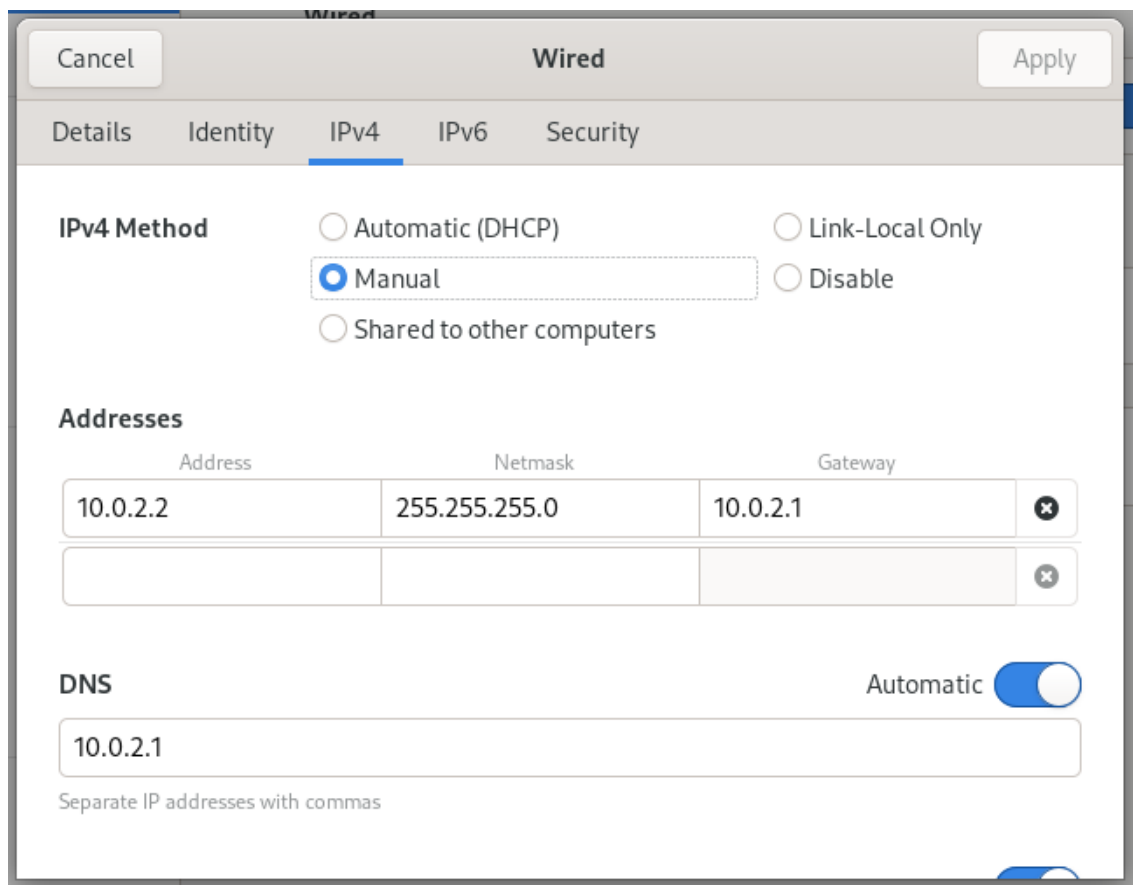
Hình 4: Dung lượng Ram của Server



Hình 5: Dung lượng ổ cứng của Server



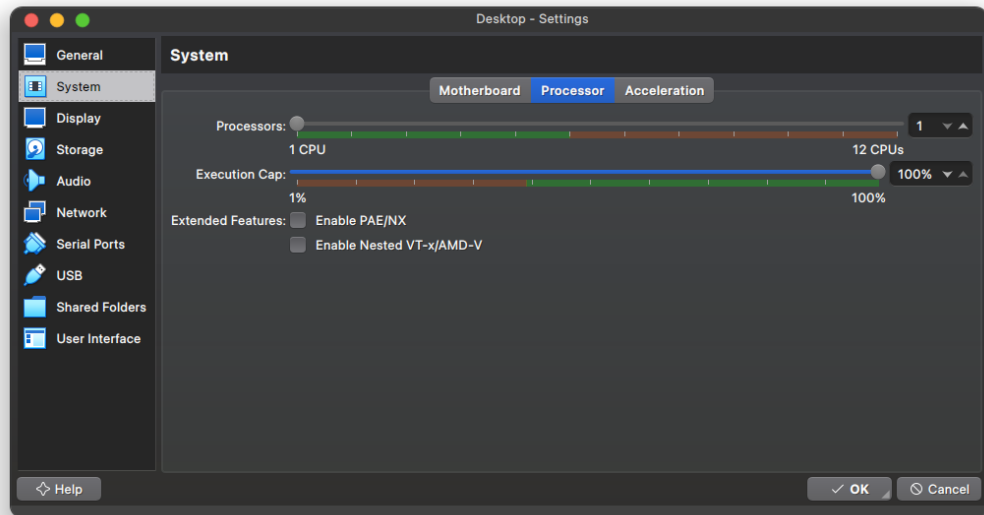
Hình 6: Cấu hình mạng máy tính Server



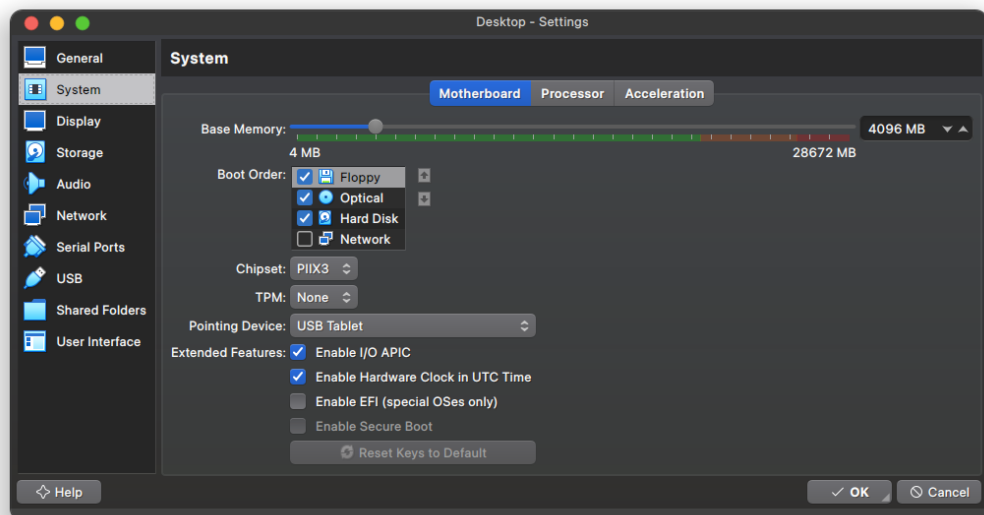
Hình 7: Cấu hình mạng máy tính Server

1.1.2.2 Desktop có cấu hình như sau:

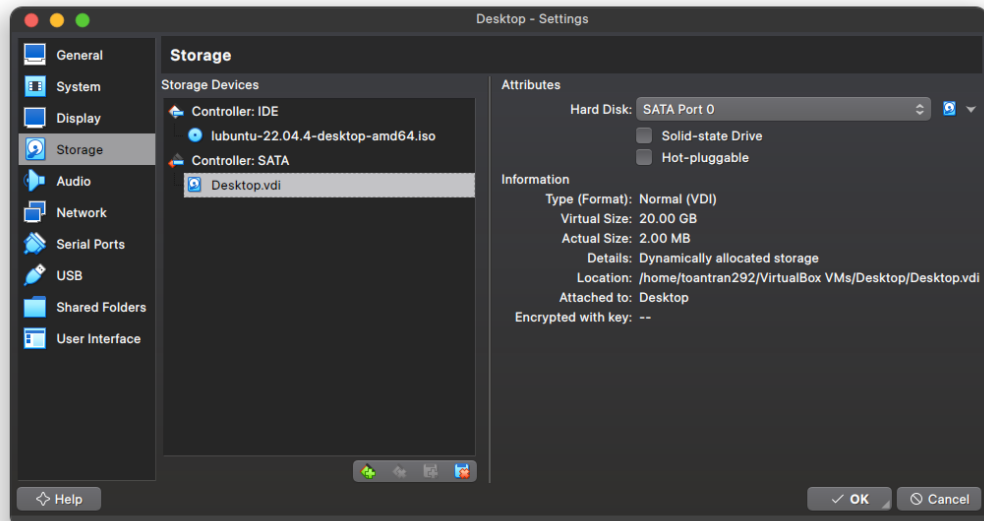
- Hệ điều hành: CentOS 9
- CPU: 1 Core (**Hình 8**)
- Ram: 4GB (**Hình 9**)
- Disk: 20GB (**Hình 10**)
- Network: NAT Network "QTHT" (**Hình 11**)



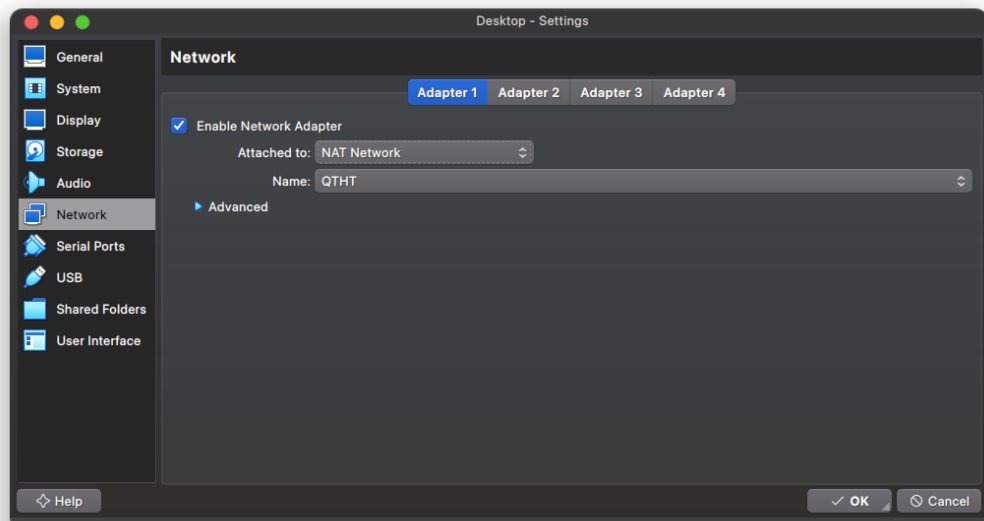
Hình 8: Số Core CPU của Desktop



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

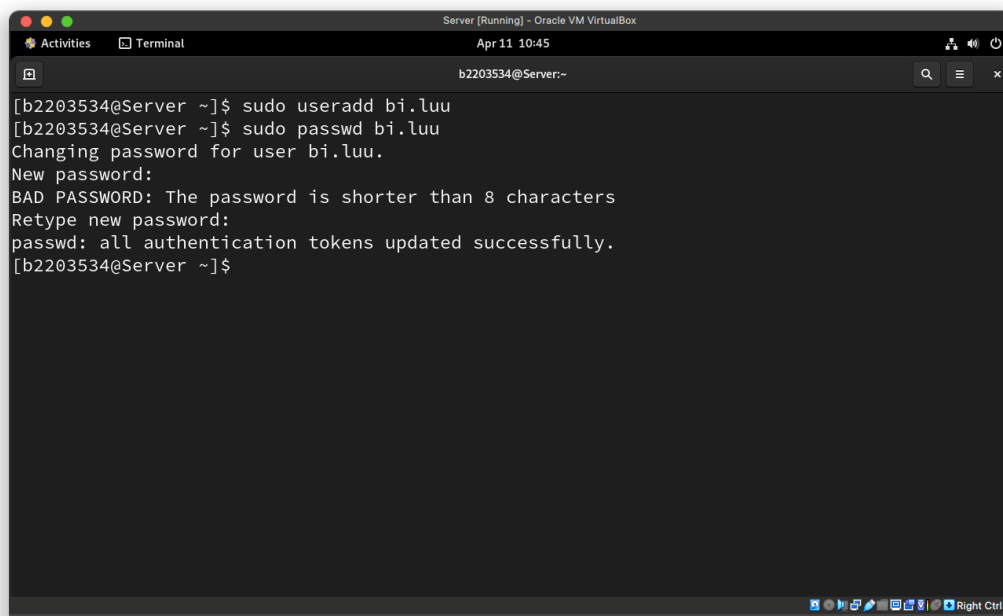
Để quản lý các bộ phận và người dùng trong công ty, hãy tạo các nhóm người dùng (group) và người dùng (user) trên server như sau. Cấp quyền sudo cho người dùng Gia Cát Lượng.

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**).



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

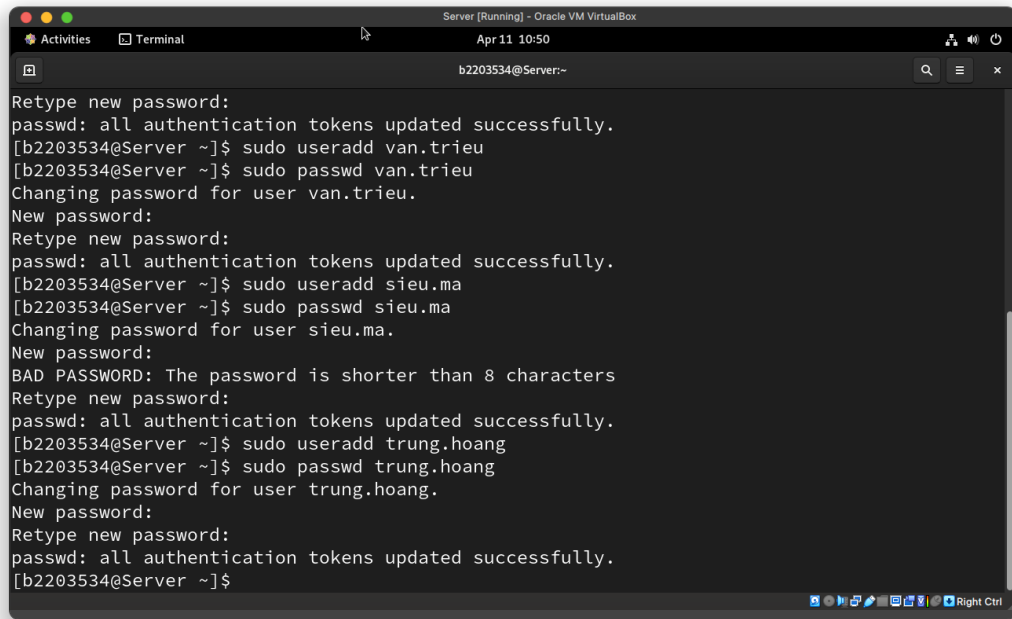
```

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**).



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

```

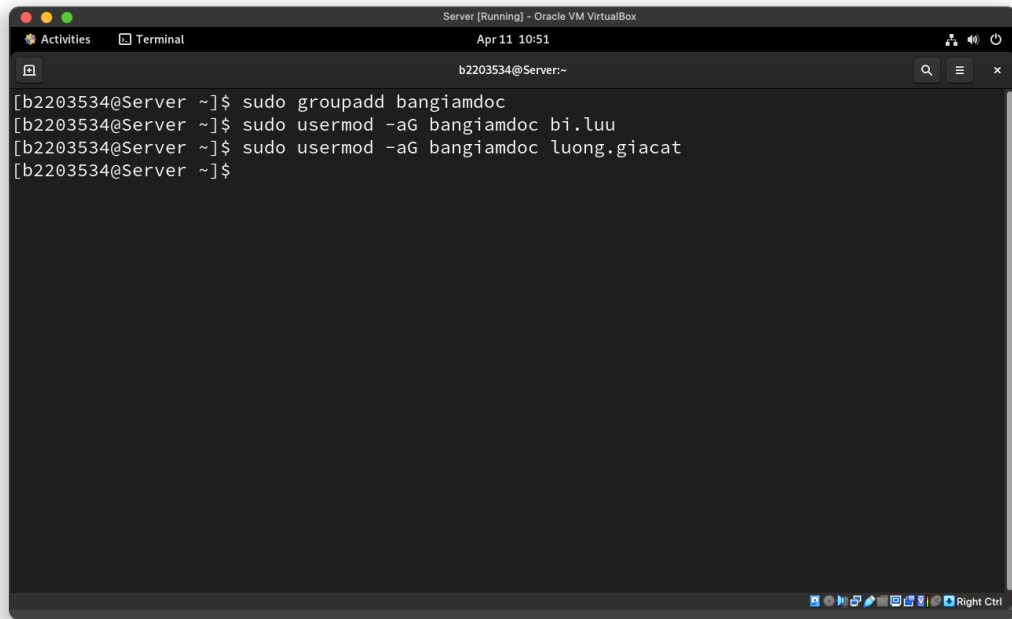
1 sudo useradd bi.luu
2 sudo passwd bi.luu
3 sudo useradd luong.giacat
4 sudo passwd luong.giacat
5 sudo useradd vu.quan
6 sudo passwd vu.quan
7 sudo useradd phi.truong
8 sudo passwd phi.truong
9 sudo useradd van.trieu
10 sudo passwd van.trieu
11 sudo useradd sieu.ma
12 sudo passwd sieu.ma
13 sudo useradd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

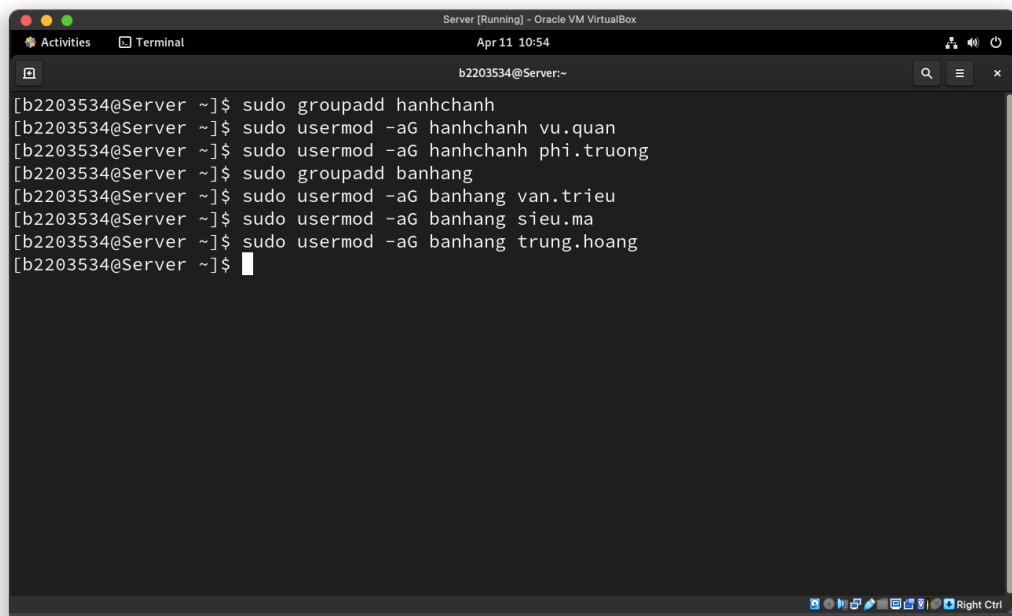
Ta sử dụng lệnh `groupadd <group-name>` để thêm nhóm người dùng và thêm người dùng vào nhóm bằng lệnh `usermod -aG <group-name> <username>`. Dưới đây là ví dụ tạo nhóm `bangiamdoc` và thêm `luu.bi` và `luong.giacat` vào nhóm này (Hình 14).



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

```

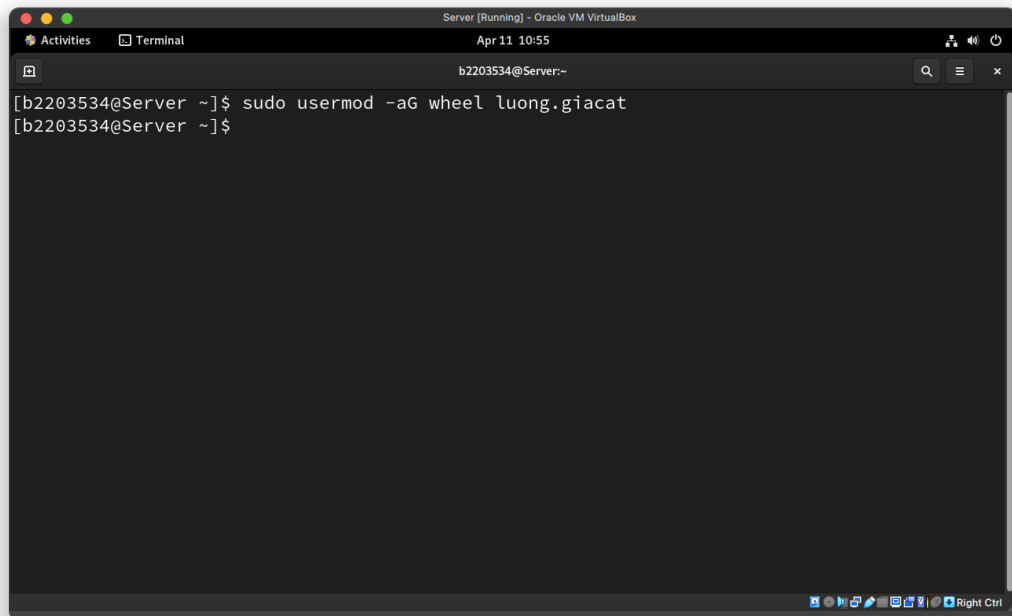
1 sudo groupadd hanhchanh
2 sudo usermod -aG hanhchanh vu.quan
3 sudo usermod -aG hanhchanh phi.truong
4 sudo groupadd banhang
5 sudo usermod -aG banhang van.trieu
6 sudo usermod -aG banhang sieu.ma
7 sudo usermod -aG banhang trung.hoang

```

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

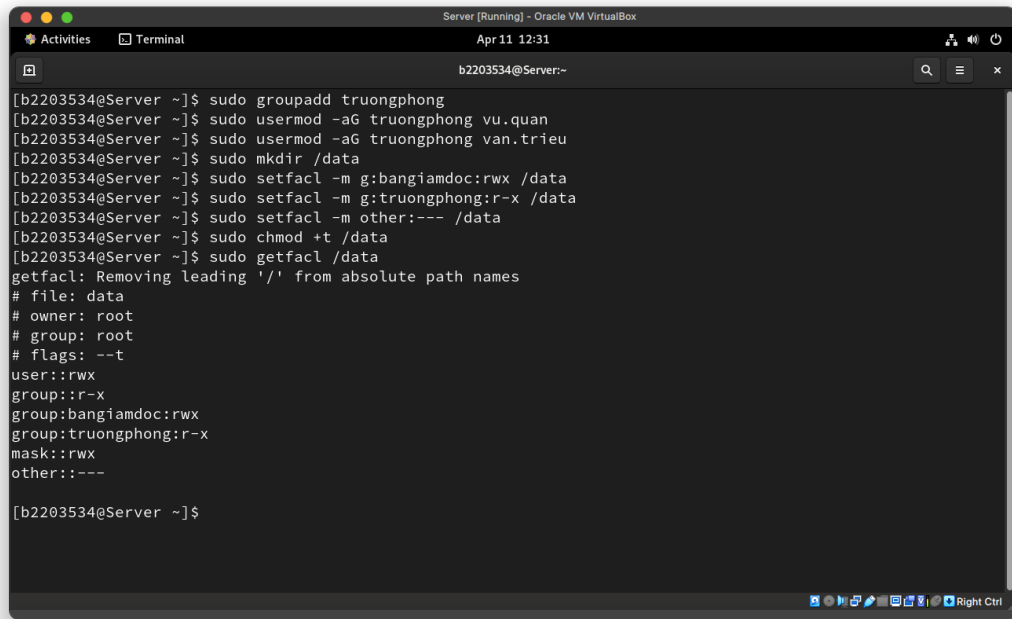
```

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*).



```
[b2203534@Server ~]$ sudo groupadd truongphong
[b2203534@Server ~]$ sudo usermod -aG truongphong vu.quan
[b2203534@Server ~]$ sudo usermod -aG truongphong van.trieu
[b2203534@Server ~]$ sudo mkdir /data
[b2203534@Server ~]$ sudo setfacl -m g:bangiamdoc:rwX /data
[b2203534@Server ~]$ sudo setfacl -m g:truongphong:r-X /data
[b2203534@Server ~]$ sudo setfacl -m other:--- /data
[b2203534@Server ~]$ sudo chmod +t /data
[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:---
[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.

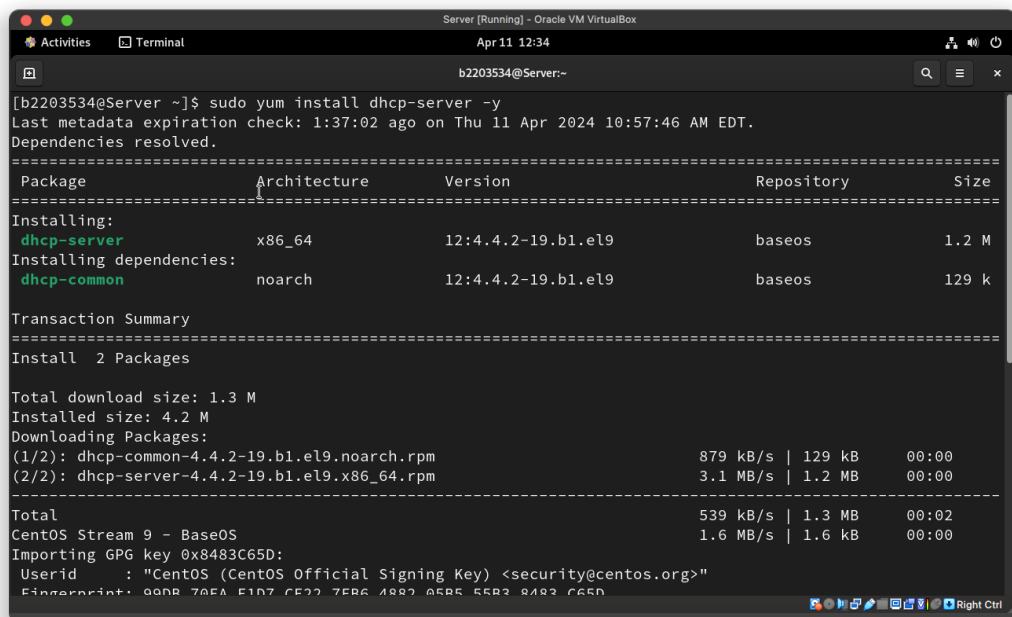
```
1 sudo chmod +t /data
```

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



```
[b2203534@Server ~]$ sudo yum install dhcp-server -y
Last metadata expiration check: 1:37:02 ago on Thu 11 Apr 2024 10:57:46 AM EDT.
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
Downloading Packages:
(1/2): dhcp-common-4.4.2-19.b1.el9.noarch.rpm      879 kB/s | 129 kB    00:00
(2/2): dhcp-server-4.4.2-19.b1.el9.x86_64.rpm     3.1 MB/s | 1.2 MB    00:00
-----
Total                                           539 kB/s | 1.3 MB    00:02
CentOS Stream 9 - BaseOS                       1.6 MB/s | 1.6 kB    00:00
Importing GPG key 0x8483C65D:
  Userid : "CentOS (CentOS Official Signing Key) <security@centos.org>"
  Fingerprint: 0906 78FA F1D7 CE22 7EB6 4BB2 05BE 55B2 2A82 C65D
```

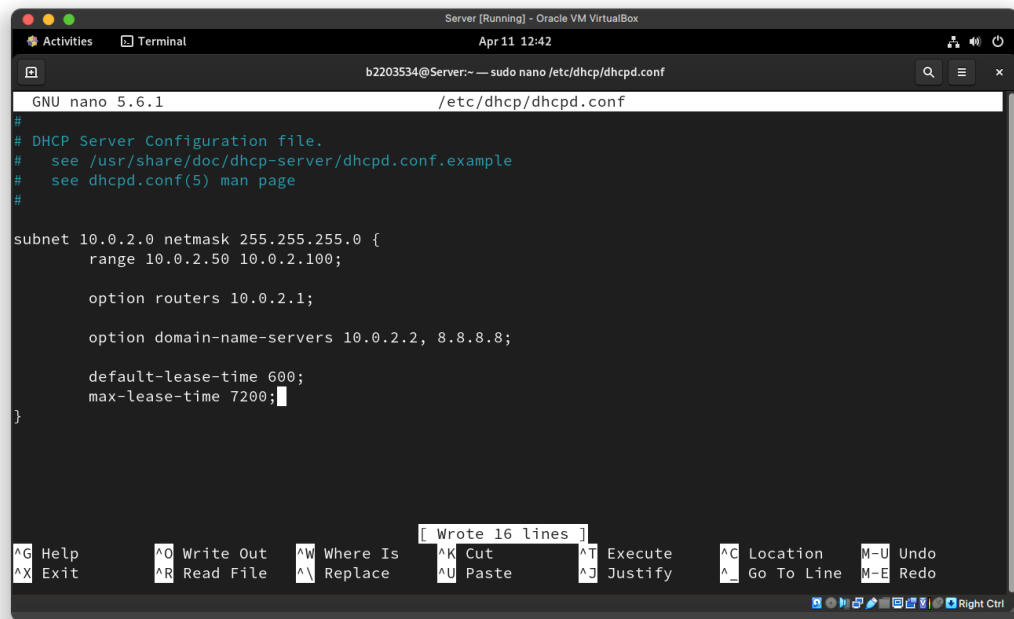
Hình 18: Cài đặt dịch vụ dhcp-server

```
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).



```
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 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;
}
```

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: Cài đặt dịch vụ dhcp-server

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.

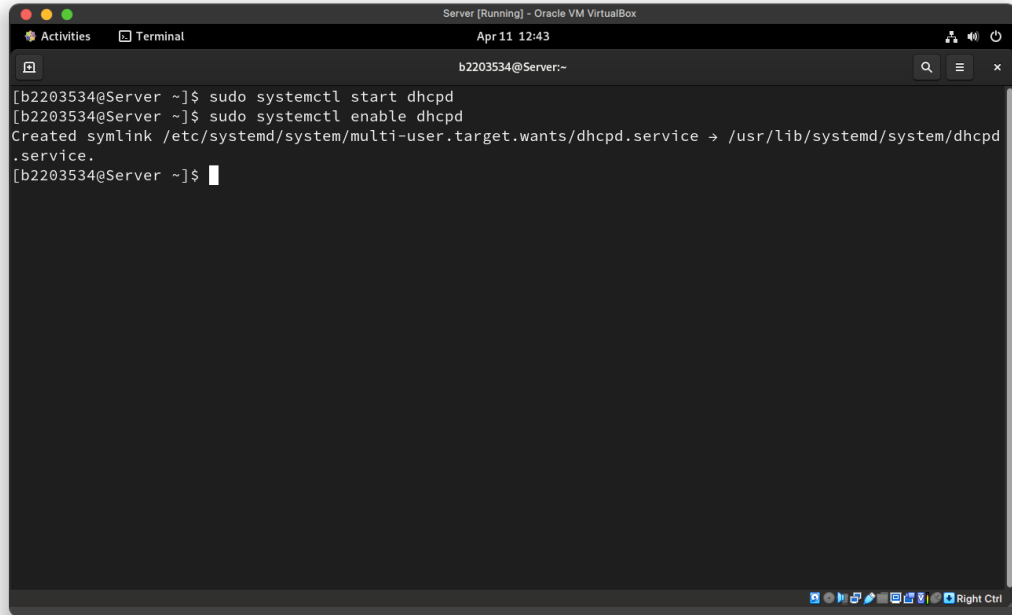
Dòng 4 Cấu hình địa chỉ gateway là 10.0.2.1.

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



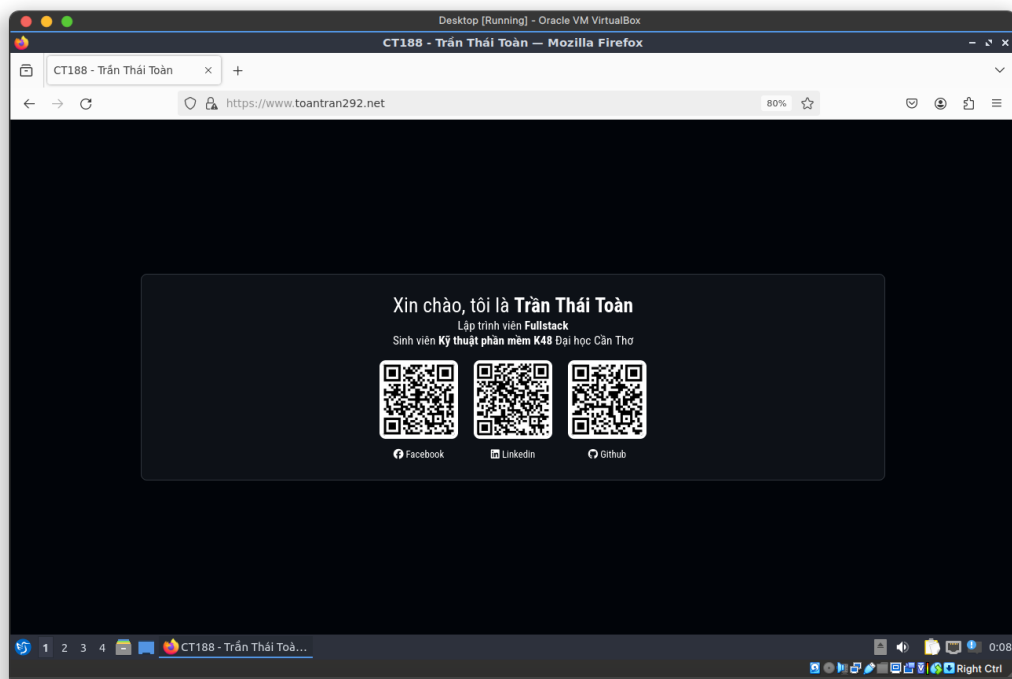
Hình 20: Khởi động dịch vụ DHCP

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

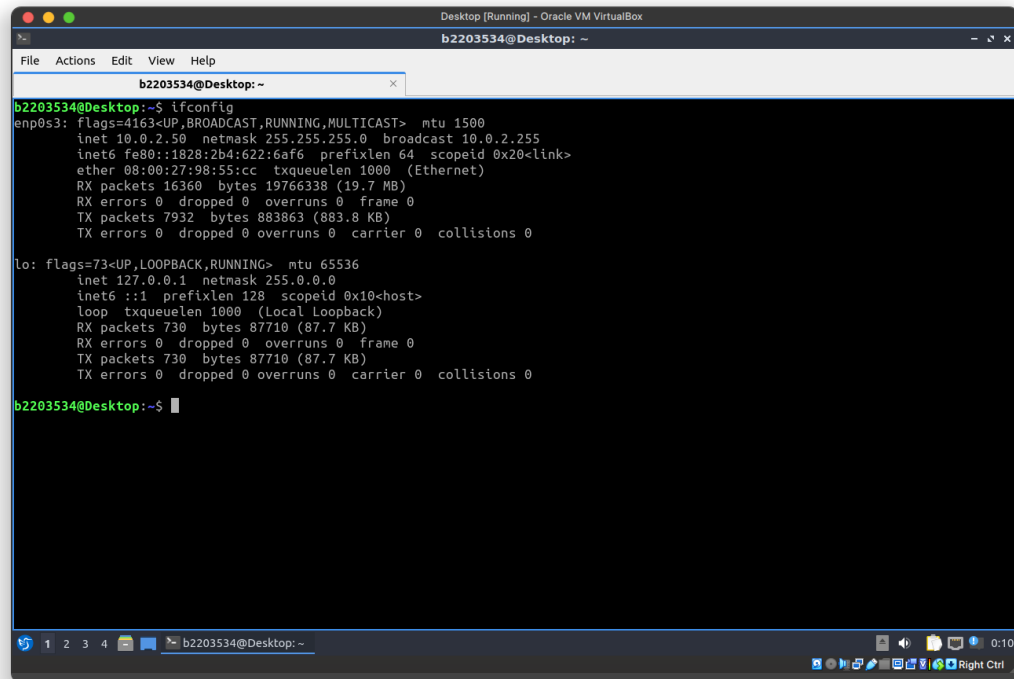
Code 14: Khởi động dịch vụ DHCP

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 QHTT và kiểm tra địa chỉ IP của máy desktop (**Hình 22**).



Hình 21: Truy cập vào internet bằng máy desktop

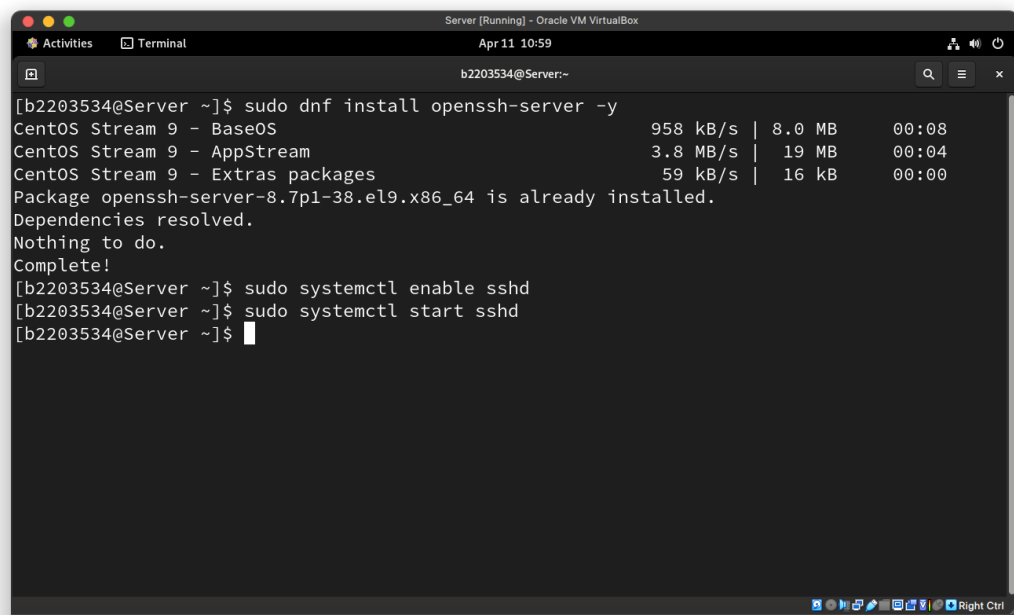


Hình 22: Kiểm tra địa chỉ IP của máy desktop (10.0.2.50)

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



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


```

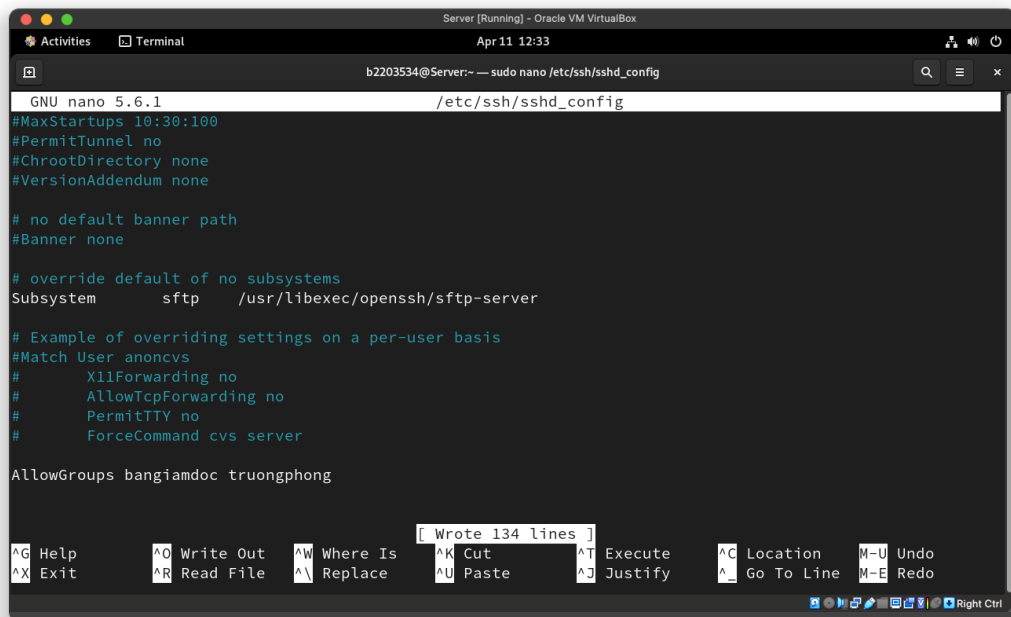
1 sudo dnf install openssh-server -y
2 sudo systemctl start sshd
3 sudo systemctl enable sshd

```

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.



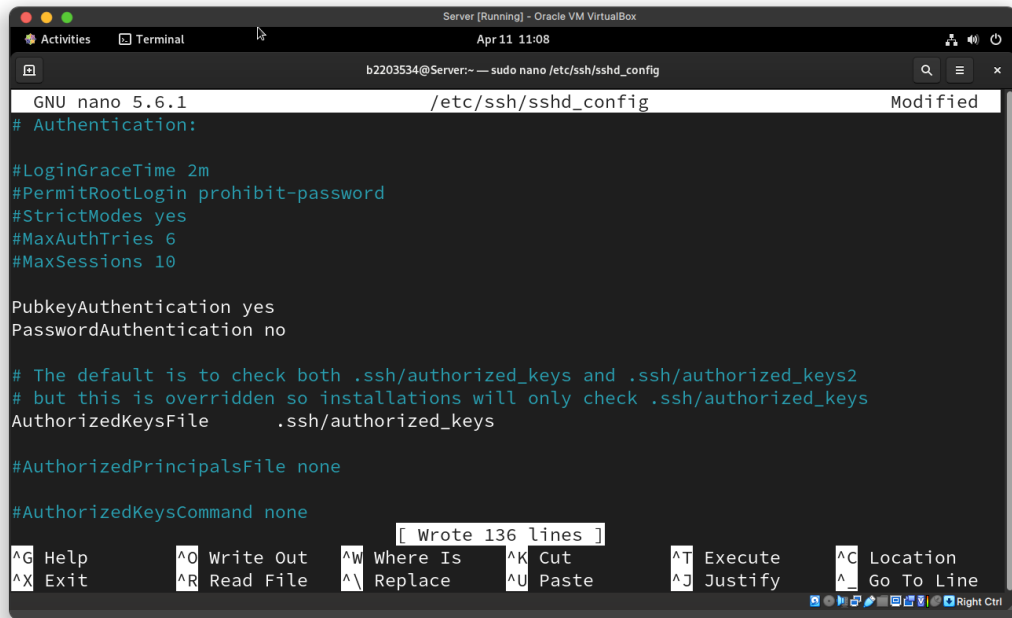
Hình 24: Cấu hình chỉ cho phép bangiamdoc và truongphong sử dụng dịch vụ SSH để điều khiển từ xa

- `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

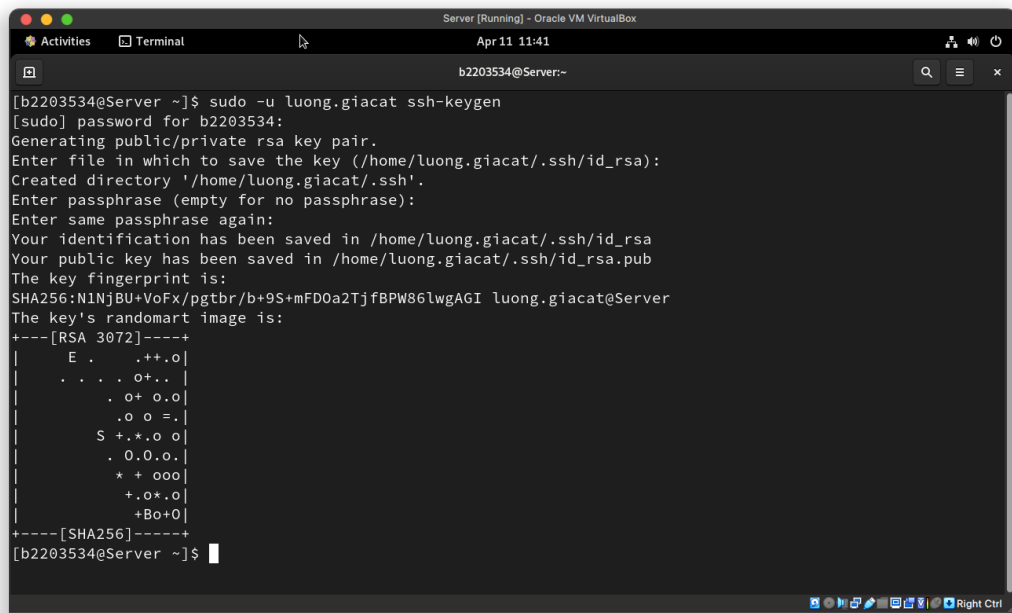
#AuthorizedKeysCommand none
[ Wrote 136 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

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`).

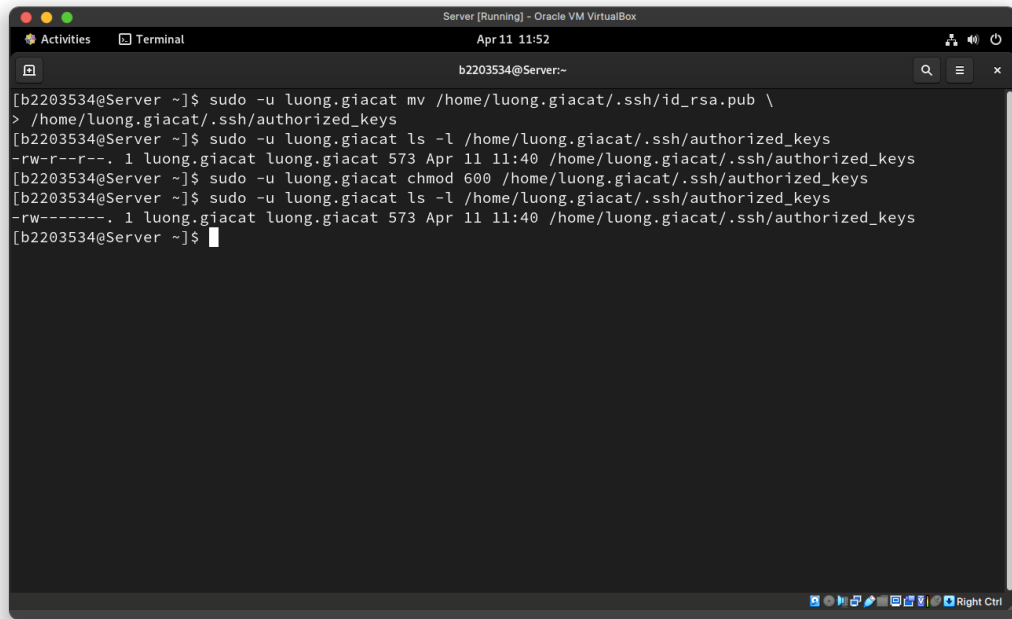
Ta sử dụng lệnh `ssh-keygen` để tạo private/public key.



```
[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:NINjBU+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 `authenrized_keys` và phân lại quyền cho file này (**Hình 27**).



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**
- 1.7 (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server**
- 1.8 (5%) Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền lautamquoc.com**

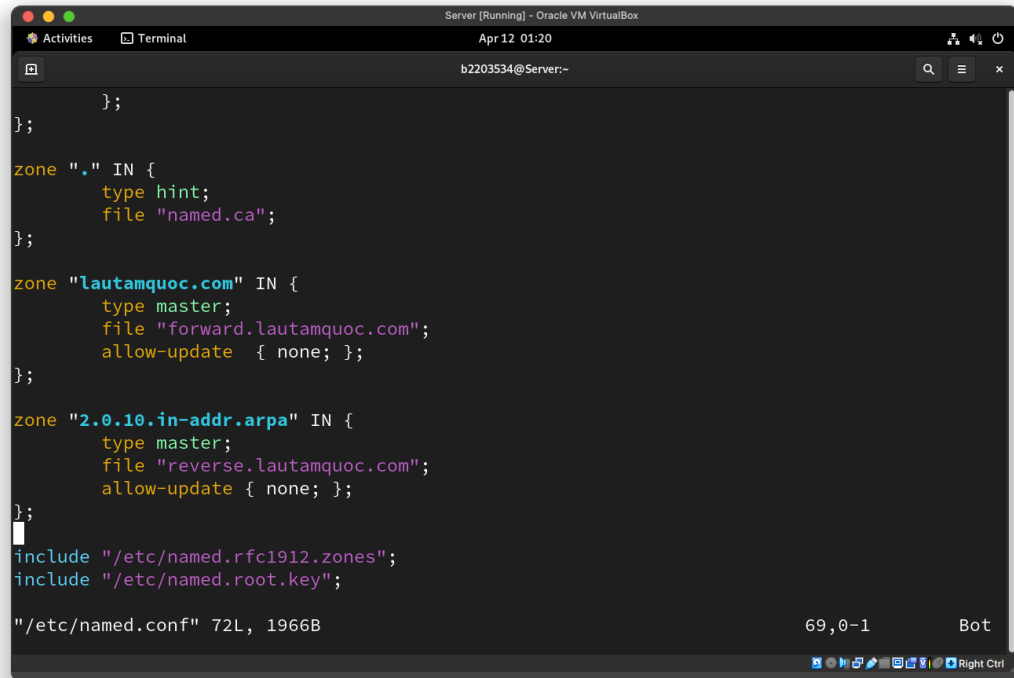
Tên miền: www.lautamquoc.com <—> IP: 10.0.2.2 (server IP)

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

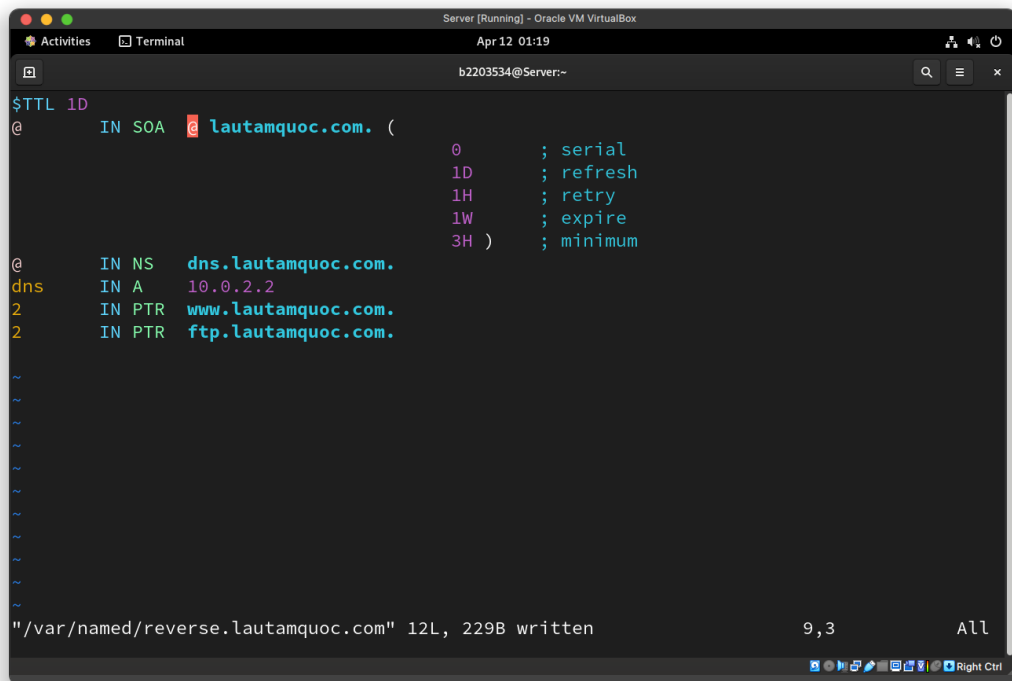


```
};  
};  
zone "." IN {  
    type hint;  
    file "named.ca";  
};  
zone "lautamquoc.com" IN {  
    type master;  
    file "forward.lautamquoc.com";  
    allow-update { none; };  
};  
zone "2.0.10.in-addr.arpa" IN {  
    type master;  
    file "reverse.lautamquoc.com";  
    allow-update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

Hình 28: 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 18: 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
2       IN PTR     www.lautamquoc.com.
2       IN PTR     ftp.lautamquoc.com.

~
~
~
~
~
~
~
~
~
~

"/var/named/reverse.lautamquoc.com" 12L, 229B written          9,3      All
```

Hình 30: 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 )
9 @      IN NS      dns.lautamquoc.com.
10 dns     IN A        10.0.2.2
11 2       IN A        www.lautamquoc.com.
12 2       IN A        ftp.lautamquoc.com.
```

Code 20: Nội dung file /etc/named/reverse.lautamquoc.com

1.8.3 Khởi động dịch vụ DNS

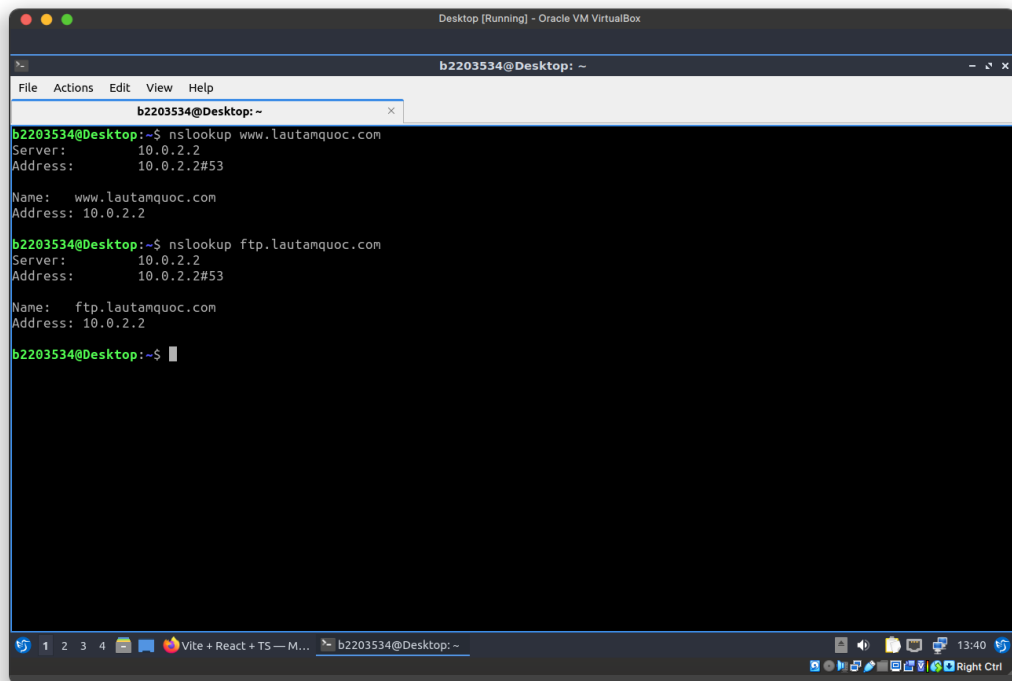
Ta khởi động dịch vụ DNS để áp dụng thay đổi.

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

Code 21: Khởi động dịch vụ DNS

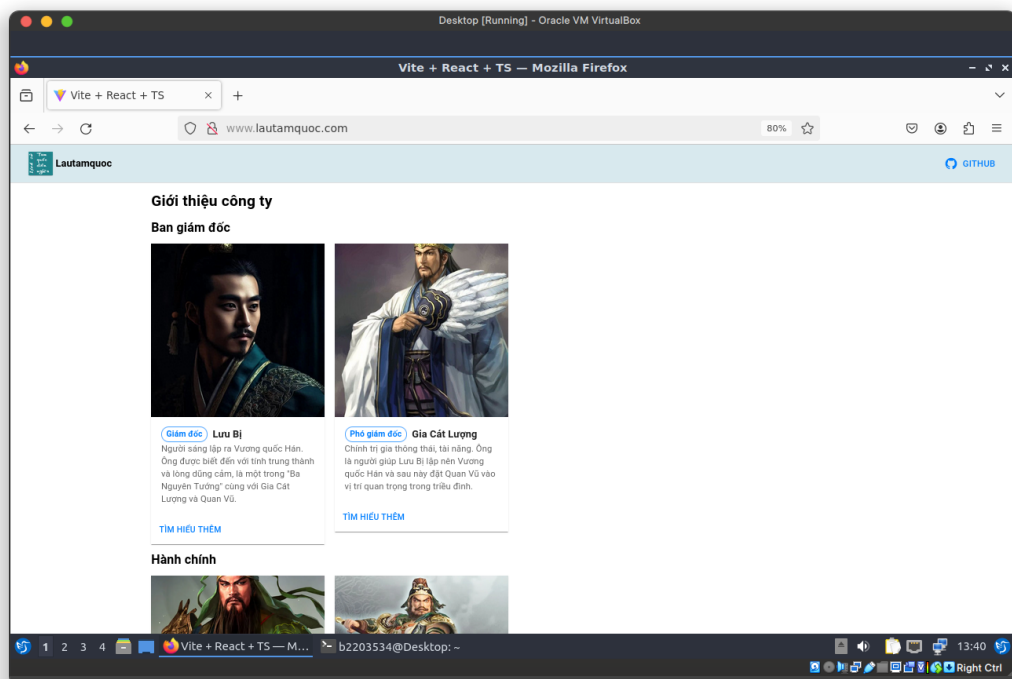
1.8.4 Kiểm tra trên máy desktop

Ta sử dụng máy desktop để kiểm tra máy chủ DNS đã cấu hình đúng hay chưa (Hình 31).



Hình 31: Kiểm tra DNS trên máy desktop

Kiểm tra trên trình duyệt web (*Hình 32*)



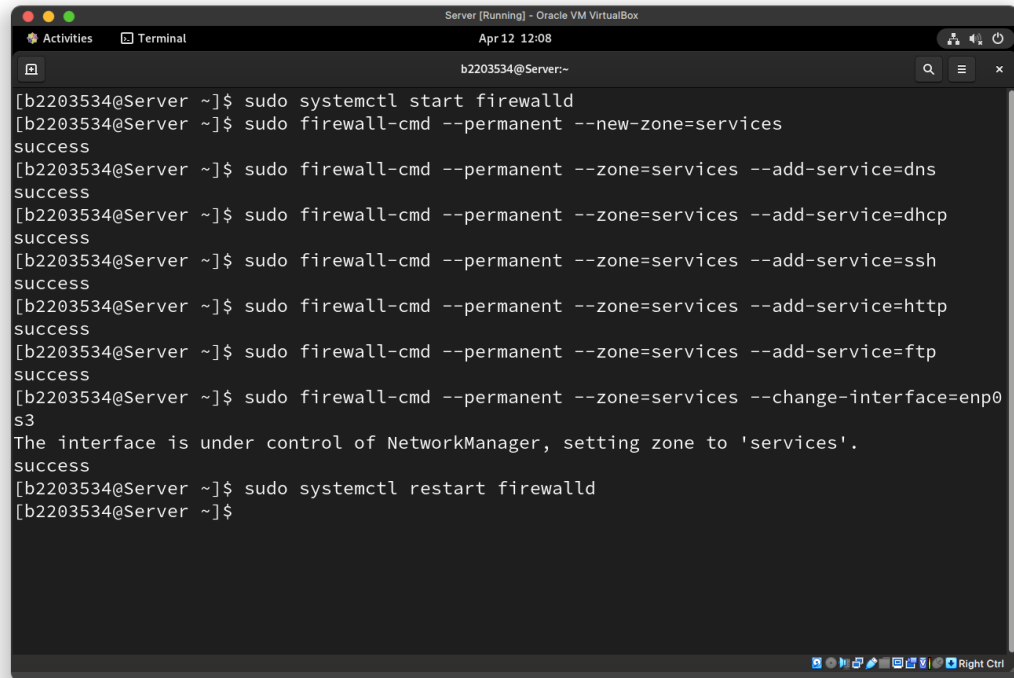
Hình 32: Sử dụng trình duyệt để kiểm tra DNS server

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 33*)



```
[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 33: 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 22: 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 23: 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 24: Thêm các dịch vụ DNS, DHCP, SSH, Web, FTP vào zone services

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

```

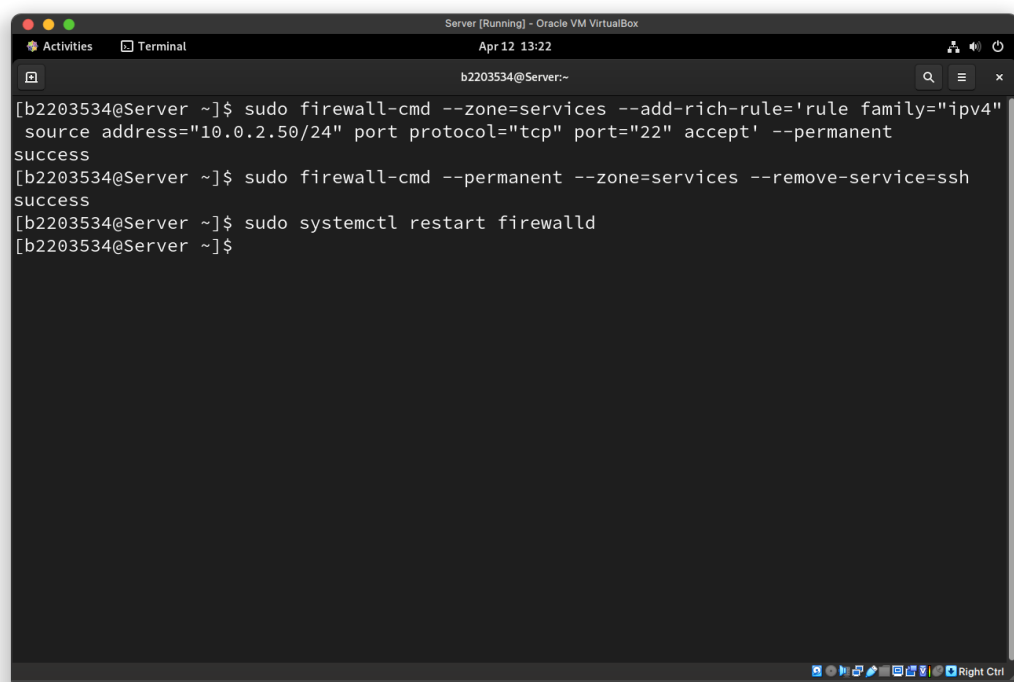
1 sudo systemctl restart firewalld

```

Code 25: 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 34**)



The screenshot shows a terminal window titled "Server [Running] - Oracle VM VirtualBox" with a timestamp of "Apr 12 13:22". The user is logged in as "b2203534@Server:~". The terminal displays the following commands and their outputs:

```

[b2203534@Server ~]$ 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
success
[b2203534@Server ~]$ sudo firewall-cmd --permanent --zone=services --remove-service=ssh
success
[b2203534@Server ~]$ sudo systemctl restart firewalld
[b2203534@Server ~]$

```

Hình 34: Cấu hình chỉ cho phép máy desktop mới có thể SSH tới server

Cụ thể các bước như sau

1. 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 26: 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 27: 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 28: 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 hằng 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 29: 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:

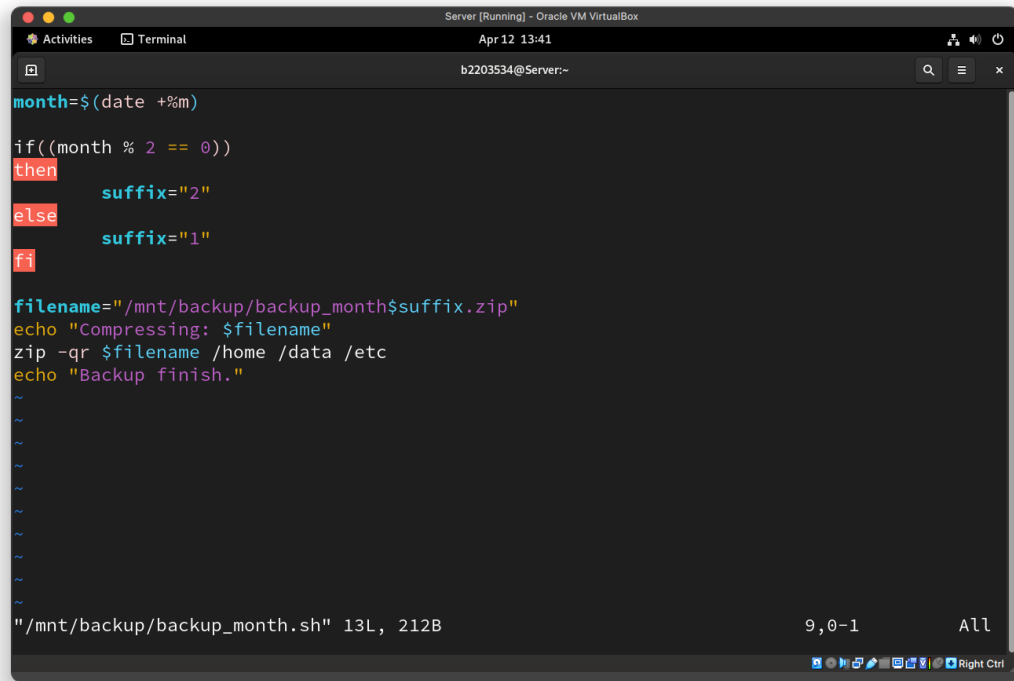
- Tạo một biến lưu trữ tên file
- Nén thư mục /home, /data, /etc


```

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 31: Script backup mỗi tuần



Hình 37: Script backup mỗi tháng

```

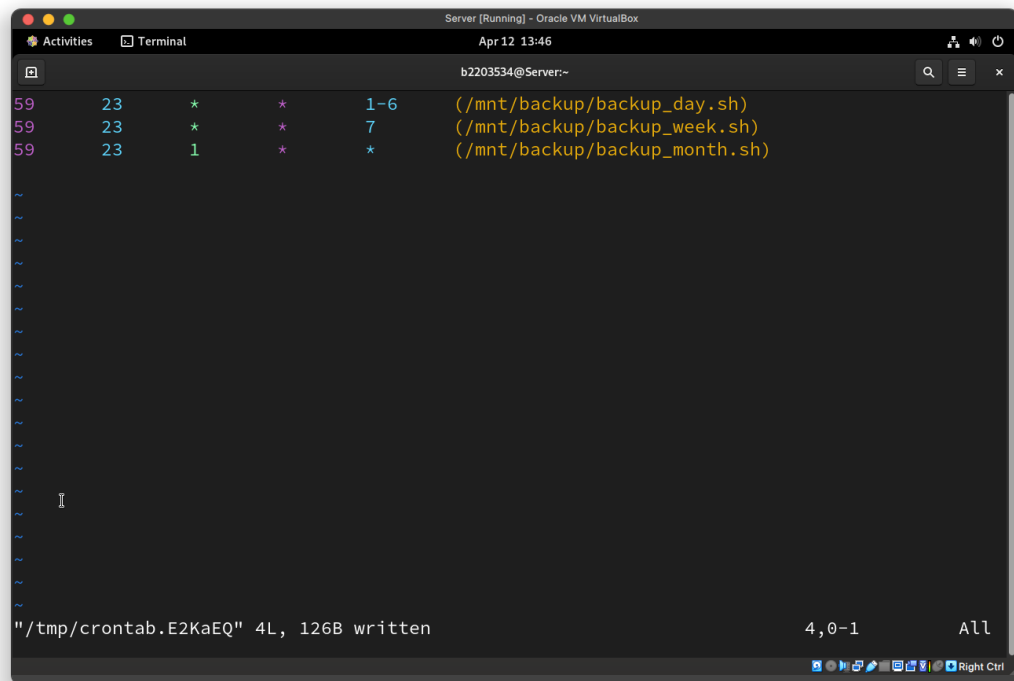
1 month=$(date + %m)
2
3 if ((month % 2 == 0))
4 then
5     suffix="2"
6 else
7     suffix="1"
8 fi
9
10 filename="/mnt/backup/backup_month$suffix.zip"
11 echo "Compressing: $filename"
12 zip -qr $filename /home /data /etc
13 echo "Backup finish."

```

Code 32: Script backup mỗi tháng

1.10.3 Cấu hình cron

Ta cấu hình cron thực thi script backup như sau



Hình 38: 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 33: Cấu hình cron