

QUẢN TRỊ HỆ THỐNG

Lý Đại Phát – B1705292

Nhóm 05

GVBM: Thái Minh Tuấn

Nội dung bài tổng hợp:

1. Cài đặt và cấu hình server/desktop.	1
1.1. Sử dụng phần mềm VirtualBox/VMware/UTM/Parallels:	1
1.1.1. 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".	1
1.1.2. Cấu hình máy ảo CentOS 9 (Server).....	2
1.1.3. Cấu hình máy ảo Ubuntu (Desktop)	3
1.2. 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.	5
1.3. 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.	6
1.4. Cài đặt và cấu hình dịch vụ DHCP trên server để cấu hình mạng tự động cho các máy desktop trong nhánh mạng:	8
1.4.1. Cài đặt dịch vụ DHCP trên server CentOS 9:.....	8
1.4.2. Cấu hình DHCP	8
1.5. Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa server... ..	9
1.5.1. Cấu hình SSH cho phép (hoặc chặn) nhóm (hoặc người) dùng điều khiển server từ xa:.....	10
1.5.2. Chỉ cho chứng thực bằng private key, tạo private/public key cho người dùng luong.giatcat:	12

1.6. 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 lautamquoc.com với nội dung trang chủ giới thiệu về các thành viên trong công ty.	15
1.7. 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.	17
1.8. Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền lautamquoc.com	19
1.8.1. Cài đặt BIND và các công cụ cần thiết (đã cài trong lab5)	19
1.8.2. Cấu hình DNS server:	19
1.8.3. Tạo tập tin cấu hình phân giải xuôi:.....	20
1.8.4. Tạo tập tin cấu hình phân giải ngược:.....	21
1.8.5. Kiểm tra và sử dụng dịch vụ DNS:	21
1.9. Cài đặt và cấu hình tường lửa trên server để cho phép:	24
1.10. Sử dụng dịch vụ cron và shell script tự động thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng như sau:.....	29
1.10.1. Tạo shell script:	30
1.10.2. Lên lịch với Crontab.	32
1.10.3. Kiểm tra việc lên lịch Crontab và các file shell script.	33

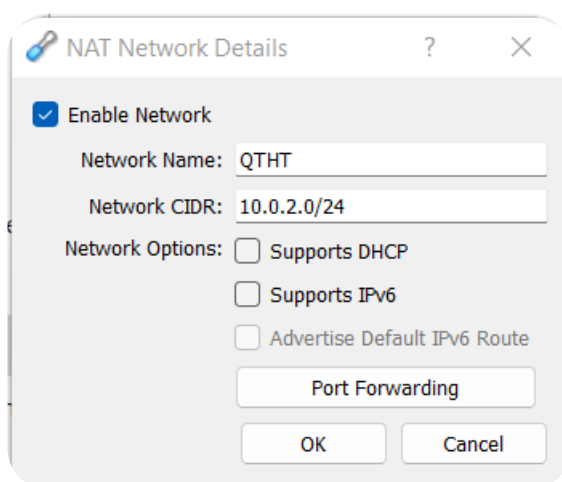
1. Cài đặt và cấu hình server/desktop.

1.1. Sử dụng phần mềm VirtualBox/VMware/UTM/Parallels:

1.1.1. 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".

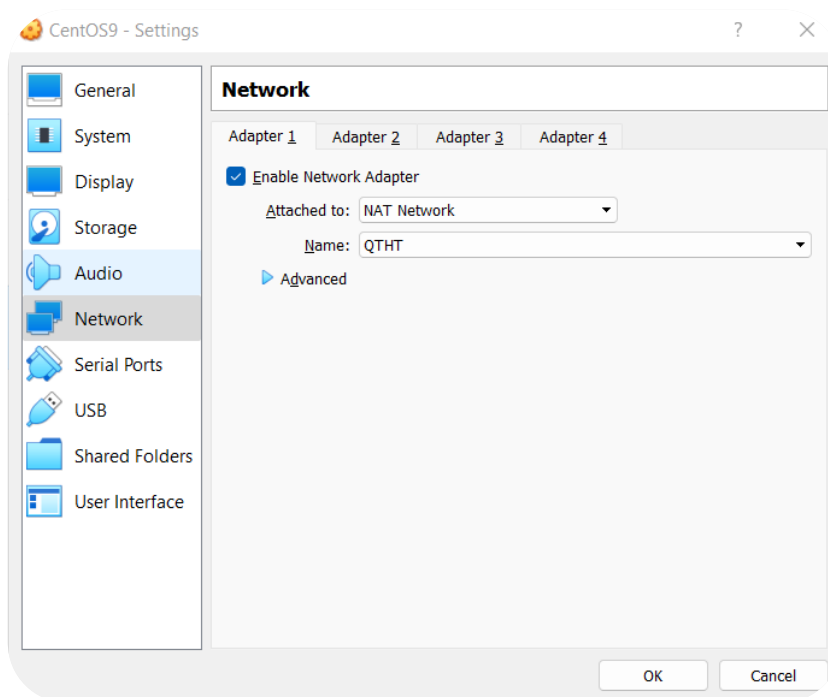
+ Từ menu của VirtualBox ta chọn File > Preferences > Network > Adds new NAT network > Edit NAT network.

+ Cấu hình chi tiết NAT network như hình dưới.



Hình 1: Cấu hình NAT network

+ Từ menu setting của máy ảo Ubuntu/CentOS 9 ta chọn Network > Attached to: NAT Network, Name: QTHT.



Hình 2: Chọn mạng NAT network vừa tạo cho các máy ảo

1.1.2. Cấu hình máy ảo CentOS 9 (Server)

Ta sẽ cấu hình máy ảo CentOS với các thông số như sau:

- Hostname: **server**
- IP: **10.0.2.2**
- Subnet mask: 255.255.255.0 (**/24**)
- Gateway: **10.0.2.1**
- DNS: **10.0.2.1**

+ Đổi tên hostname mặc định:

Lệnh: `$sudo nmcli general hostname <server>`

```
[b1705292@localhost ~]$ sudo nmcli general hostname server
[b1705292@localhost ~]$ su - $USER
Password:
[b1705292@server ~]$ hostname
server
```

Hình 3: Đổi tên hostname

+ Cấu hình thông số IP, Subnet mask, Gateway, DNS:

Lệnh: `$nmcli con mod enp0s3 ipv4.method manual ipv4.addresses 10.0.2.2/24 ipv4.gateway 10.0.2.1 ipv4.dns 10.0.2.1`

+ Xem lại cấu hình đã cài đặt:

Lệnh: `$nmcli -f ipv4.addresses,ipv4.gateway,ipv4.dns con show enp0s3`

```
[b1705292@server ~]$ nmcli con mod enp0s3 ipv4.method manual ipv4.addresses 10.0.2.2/24 ipv4.gateway 10.0.2.1 ipv4.dns 10.0.2.1
[b1705292@server ~]$ nmcli -f ipv4.addresses,ipv4.gateway,ipv4.dns con show enp0s3
ipv4.addresses:          10.0.2.2/24
ipv4.gateway:            10.0.2.1
ipv4.dns:                10.0.2.1
```

Hình 4: Cấu hình mạng đã cài đặt thủ công

+ Cập nhật lại các thay đổi:

Lệnh: `$nmcli con down enp0s3`

Lệnh: `$nmcli con up enp0s3`

```
[b1705292@server ~]$ nmcli con down enp0s3
Connection 'enp0s3' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
[b1705292@server ~]$ nmcli con up enp0s3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
```

Hình 5: Cập nhật các thay đổi trên card mạng enp0s3

1.1.3. Cấu hình máy ảo Ubuntu (Desktop)

Ta sẽ cấu hình máy ảo Ubuntu với các thông số như sau:

- Hostname: **desktop**
- IP, Subnet mask, gateway, DNS : **Automatic (DHCP)**

+ Đổi tên hostname mặc định:

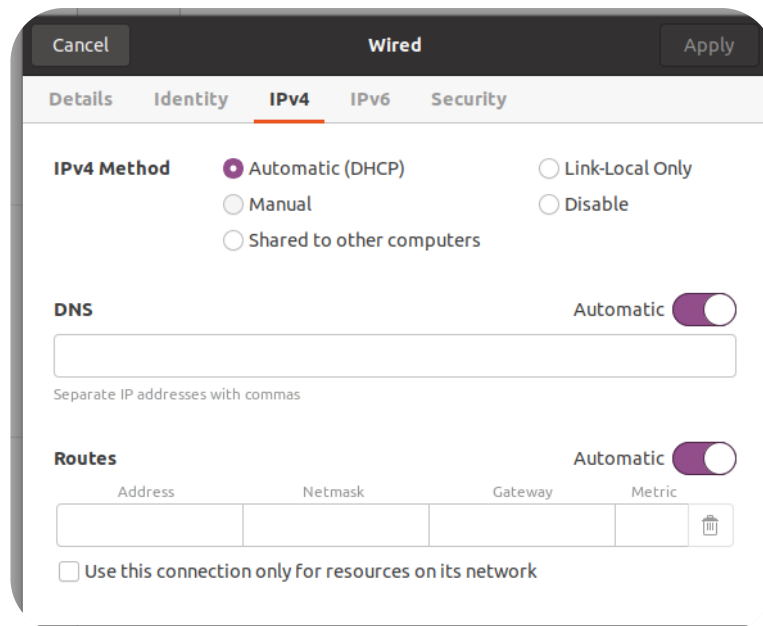
Lệnh: `$sudo nmcli general hostname <desktop>`

```
b1705292@phat-VirtualBox:~$ sudo nmcli general hostname desktop
b1705292@phat-VirtualBox:~$ su - $USER
Password:
b1705292@desktop:~$ hostname
desktop
```

Hình 6: Đổi tên hostname

+ Đầu tiên để cấu hình động cho các client, ta phải cài đặt dịch vụ DHCP Server trên máy Server CentOS 9 trước (**làm câu 1.4 trước**).

+ Sau khi cài đặt dịch vụ DHCP, tiếp theo từ máy ảo Desktop Ubuntu ta vào Settings > Network > Wired > IPv4 > IPv4 Method: Automatic (DHCP).

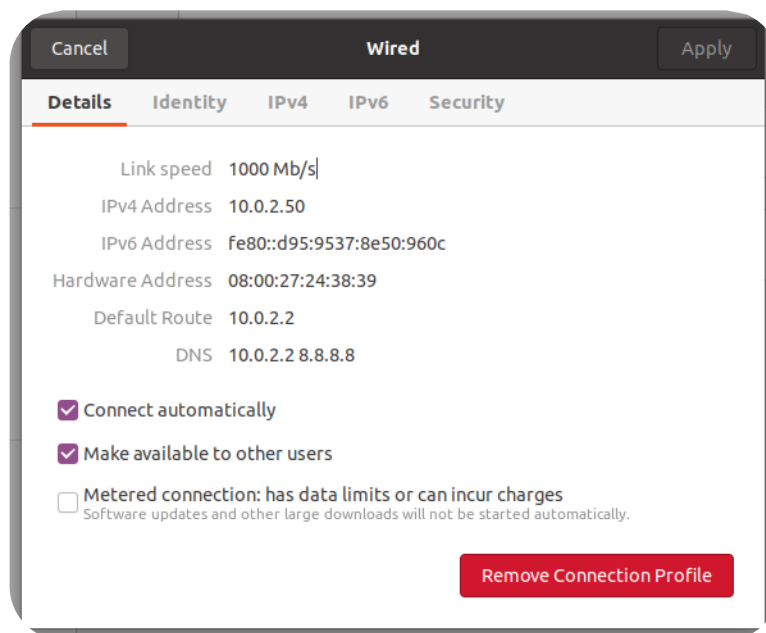


Hình 7: Cấu hình động DHCP

+ Kiểm tra các thông số IP, Subnetmask, gateway, DNS:

```
b1705292@desktop:~$ ifconfig enp0s3
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::d95:9537:8e50:960c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:24:38:39 txqueuelen 1000 (Ethernet)
    RX packets 1782 bytes 204969 (204.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4716 bytes 545903 (545.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 8: Thông số cấu hình động (1)



Hình 9: Thông số cấu hình động (2)

+ Ping từ desktop đến server, từ desktop đến internet:

```
b1705292@desktop:~$ ping -c 3 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.280 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=64 time=0.328 ms

--- 10.0.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.280/0.341/0.415/0.055 ms
```

Hình 10: Ping từ desktop đến server

```
b1705292@desktop:~$ ping -c 3 youtube.com
PING youtube.com (142.250.66.110) 56(84) bytes of data.
64 bytes from hkg12s28-in-f14.1e100.net (142.250.66.110): icmp_seq=1 ttl=112 time=54.6 ms
64 bytes from hkg12s28-in-f14.1e100.net (142.250.66.110): icmp_seq=2 ttl=112 time=55.1 ms
64 bytes from hkg12s28-in-f14.1e100.net (142.250.66.110): icmp_seq=3 ttl=112 time=54.9 ms

--- youtube.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 54.569/54.840/55.100/0.216 ms
```

Hình 11: Ping từ desktop ra ngoài internet

+ Ping từ server đến desktop, từ server đến internet:

```
[b1705292@server ~]$ ping -c 3 10.0.2.50
PING 10.0.2.50 (10.0.2.50) 56(84) bytes of data.
64 bytes from 10.0.2.50: icmp_seq=1 ttl=64 time=0.310 ms
64 bytes from 10.0.2.50: icmp_seq=2 ttl=64 time=0.302 ms
64 bytes from 10.0.2.50: icmp_seq=3 ttl=64 time=0.369 ms

--- 10.0.2.50 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.302/0.327/0.369/0.029 ms
```

Hình 12: Ping từ server đến desktop

```
[b1705292@server ~]$ ping -c 3 google.com
PING google.com (142.250.204.142) 56(84) bytes of data.
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=1 ttl=112 time=57.6 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=2 ttl=112 time=55.9 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=3 ttl=112 time=54.7 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
```

Hình 13: Ping từ server ra ngoài internet

1.2. 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.

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

+ Để tạo một user mới ta dùng lệnh: `$sudo adduser <user_name>`

```
[b1705292@server home]$ ls
b1705292  luong.giacat  phi.truong  trung.hoang  vu.quan
bi.luu    phatly        sieu.ma     van.trieu
```

Hình 14: Các user đã tạo

+ Để tạo mật khẩu cho username vừa tạo ta dùng lệnh: `$sudo passwd <user_name>`

```
[b1705292@server home]$ 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.
```

Hình 15: Tạo mật khẩu cho các user

+ Để tạo nhóm người dùng ta dùng lệnh: `$sudo groupadd <group_name>`

```
bangiamdoc:x:1009:
hanhchanh:x:1010:
banhang:x:1011:
```

Hình 16: Xem các nhóm đã tạo `$sudo cat /etc/group`

+ Để thêm các user vào 1 nhóm ta dùng lệnh: `$sudo usermod -a -G <group_name> <user_name>`

```
bangiamdoc:x:1009:bi.luu,luong.giacat
hanhchanh:x:1010:vu.quan,phi.truong
banhang:x:1011:van.trieu,sieu.ma,trung.hoang
```

Hình 17: Thêm user vào các nhóm tương ứng

+ Cấp quyền sudo cho người dùng Gia Cát Lượng:

- Ta sẽ không cấp quyền sudo trực tiếp cho người dùng Gia Cát Lượng, mà ta sẽ thêm người dùng này nhóm có quyền sudo. Ở đây để tiết kiệm thời gian, ta sẽ thêm người dùng Gia Cát Lượng vào nhóm **wheel**.
- Lệnh để thêm một người dùng vào nhóm: `$sudo usermod -a -G <group_name> <user_name>`

```
[b1705292@server home]$ groups luong.giacat
luong.giacat : luong.giacat wheel
```

Hình 18: Thêm user luong.giacat vào nhóm wheel

1.3. 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.

+ Tạo thư mục /data:

- Dùng lệnh: `$sudo mkdir /data`

+ Để phân quyền như yêu cầu, ta sử dụng kỹ thuật ACL (Access Control List) kết hợp sticky bit.

+ Phân quyền cho thành viên ban giám đốc có toàn quyền (rwx) trên thư mục /data:

Ta dùng lệnh: `$sudo setfacl -m g:bangiamdoc:rwx /data`

+ Phân quyền cho trưởng phòng quyền read và execute, các nhân viên không có bất cứ quyền gì:

- Phân tích vấn đề ta sẽ thấy các trưởng phòng nằm ở nhóm hanhchanh và nhóm banhang, đồng thời các nhóm này đều có các nhân viên (không có quyền). Trên thực tế, số lượng nhân viên có thể rất nhiều, trưởng phòng thì chỉ có khoảng vài người, do đó ta sẽ thiết lập cho nhóm hanhchanh và nhóm banhang không có quyền trên thư mục /data. Ta có 2 hướng giải quyết như sau:
 1. Ta sẽ thiết lập riêng cho từng cá nhân là trưởng phòng có quyền read và execute trên thư mục /data
 2. Ta sẽ tạo thêm một nhóm truongphong, và cho các cá nhân là trưởng phòng vào nhóm này, sau đó ta sẽ phân quyền read và excute trên thư mục /data cho nhóm này.

Ở đây ta sẽ làm theo cách 2.

- Do đó ta có các lệnh để tạo nhóm và phân quyền trên nhóm như sau:

- + `$sudo groupadd truongphong`
- + `$sudo usermod -a -G truongphong vu.quan`
- + `$sudo usermod -a -G truongphong van.trieu`
- + `$sudo setfacl -m g:hanhchanh:--- /data`
- + `$sudo setfacl -m g:banhang:--- /data`
- + `$sudo setfacl -m g:truongphong:r-x /data`

```
bangiamdoc:x:1009:bi.luu,luong.giacat
hanhchanh:x:1010:vu.quan,phi.truong
banhang:x:1011:van.trieu,sieu.ma,trung.hoang
truongphong:x:1012:vu.quan,van.trieu
```

Hình 19 Tạo nhóm truongphong và thêm các user tương ứng vào nhóm

+ Chủ sở hữu tập tin mới có quyền xóa hoặc đổi tên tập tin:

Dùng lệnh: `$sudo chmod +t /data`

```
[b1705292@server ~]$ 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:hanhchanh:---
group:banhang:---
group:truongphong:r-x
mask::rwx
other::r-x
```

Hình 20: Kết quả phân quyền sử dụng ACL và Sticky bit (1)

```
drwxrwxr-t+  2 root root  33 Nov 24 22:36 data
```

Hình 21: Kết quả phân quyền sử dụng ACL và Sticky bit (2)

1.4. 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 trên server CentOS 9:

Lệnh: \$sudo dnf -y install dhcp-server

```
Installed:
  dhcp-common-12:4.4.2-18.b1.el9.noarch  dhcp-server-12:4.4.2-18.b1.el9.x86_64
Complete!
```

Hình 22: Cài đặt dịch vụ DHCP Server

1.4.2. Cấu hình DHCP

+ Mở tập tin để tiến hành cấu hình: \$sudo nano /etc/dhcp/dhcp.conf

+ Nội dung file cấu hình như sau:

```
#default lease time
default-lease-time 600;

#max lease time
max-lease-time 7200;

#update ddns
ddns-update-style none;

#this DHCP server to be declared valid
authoritative;

#specify network address, subnetmask, gateway, DNS
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 subnet-mask 255.255.255.0;
    option domain-name-servers 10.0.2.2, 8.8.8.8;
}
```

Hình 23: Nội dung file cấu hình dhcpd.conf

+ Khởi động dịch vụ DHCP, cho phép DHCP tự chạy mỗi khi máy khởi động.

Lệnh: `$sudo systemctl start dhcpd`

Lệnh: `$sudo systemctl enable dhcpd`

+ Kiểm tra trạng thái dịch vụ DHCP Server:

Lệnh: `$sudo systemctl status dhcpd`

```
[b1705292@server ~]$ sudo systemctl status dhcpd
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor pre>
   Active: active (running) since Thu 2022-11-24 17:50:53 +07; 3min 43s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
  Main PID: 6980 (dhcpd)
    Status: "Dispatching packets..."
     Tasks: 1 (limit: 10945)
    Memory: 4.6M
       CPU: 7ms
    CGroup: /system.slice/dhcpd.service
            └─6980 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -gr>
```

Hình 24: Kiểm tra trạng thái dịch vụ DHCP

1.5. 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.

+ Cài đặt dịch vụ SSH: `$sudo dnf install openssh-server -y`

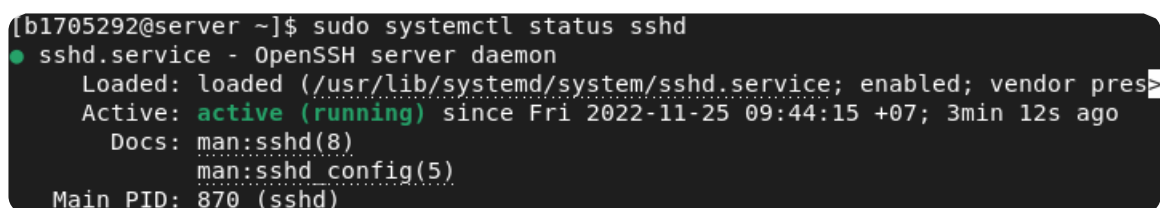
+ Khởi động và cho phép dịch vụ SSH tự động thực thi khi khởi động hệ điều hành:

`$sudo systemctl start sshd`

`$sudo systemctl enable sshd`

+ Kiểm tra trạng thái dịch vụ SSH:

`$sudo systemctl status sshd`



```
[b1705292@server ~]$ sudo systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-25 09:44:15 +07; 3min 12s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 870 (sshd)
```

Hình 25: Kiểm tra trạng thái dịch vụ SSH

1.5.1. Cấu hình SSH cho phép (hoặc chặn) nhóm (hoặc người) dùng điều khiển server từ xa:

Lưu ý 1: nhóm *truongphong* (đã tạo ở câu 1.3) gồm 2 người dùng là Quan Vũ và Triệu Vân.

Lưu ý 2: *AllowGroups* và *AllowUsers* trong file *sshd_config*.

AllowGroups: nếu sau này muốn thêm người dùng khác có quyền điều khiển server từ xa thì chỉ cần thêm người dùng này vào nhóm, không cần phải mở file cấu hình *sshd_config* như *AllowUsers*.

AllowUsers: nếu muốn thêm người dùng khác có quyền điều khiển server từ xa thì phải mở file cấu hình *sshd_config* và thêm user này vào. Nhược điểm: nếu số lượng người dùng lớn, thì rất tốn thời gian.

- Tiến hành cấu hình SSH server:

1. Mở file config SSH: `$sudo nano /etc/ssh/sshd_config`
2. Cho phép nhóm *bangiamdoc*, *truongphong* điều khiển server từ xa, thêm dòng này: *AllowGroups bangiamdoc truongphong*
3. Chặn tài khoản root điều khiển server từ xa: tìm đến dòng “*#PermitRootLogin yes*”, bỏ ghi chú dấu “*#*” và thay “*yes*” thành “*no*”. Nếu không có dòng “*#PermitRootLogin*” mà chỉ có dòng “*#PermitRootLogin prohibit-password*” thì ta thêm dòng “*PermitRootLogin no*”

```
Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
AllowGroups bangiamdoc truongphong
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

Hình 26: Nội dung file cấu hình sshd_config

4. Khởi động lại dịch vụ SSH: \$sudo systemctl restart sshd
5. Kiểm tra kết quả:

```
b1705292@desktop:~$ ssh root@10.0.2.2
root@10.0.2.2's password:
Permission denied, please try again.
```

Hình 27: Truy cập SSH server thất bại bằng tài khoản root

```
b1705292@desktop:~$ ssh b1705292@10.0.2.2
b1705292@10.0.2.2's password:
Permission denied, please try again.
```

Hình 28: Truy cập SSH server thất bại bằng tài khoản b1705292

```
b1705292@desktop:~$ ssh bi.luu@10.0.2.2
bi.luu@10.0.2.2's password:
Last login: Fri Nov 25 11:12:56 2022 from 10.0.2.50
[bi.luu@server ~]$
```

Hình 29: Truy cập SSH server thành công là thành viên nhóm bangiamdoc (1)

```
b1705292@desktop:~$ ssh luong.giacat@10.0.2.2
luong.giacat@10.0.2.2's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Nov 25 11:12:33 2022 from 10.0.2.50
[luong.giacat@server ~]$
```

Hình 30: Truy cập SSH server thành công là thành viên nhóm bangiamdoc (2)

```
b1705292@desktop:~$ ssh vu.quan@10.0.2.2
vu.quan@10.0.2.2's password:
Last login: Fri Nov 25 11:09:51 2022 from 10.0.2.50
[vu.quan@server ~]$
```

Hình 31: Truy cập SSH server thành công là thành viên nhóm truongphong (1)

```
b1705292@desktop:~$ ssh van.trieu@10.0.2.2
van.trieu@10.0.2.2's password:
Last login: Fri Nov 25 10:41:40 2022 from 10.0.2.50
[van.trieu@server ~]$
```

Hình 32: Truy cập SSH server thành công là thành viên nhóm truongphong (2)

```
b1705292@desktop:~$ ssh truong.phu@10.0.2.2
truong.phu@10.0.2.2's password:
Permission denied, please try again.
```

Hình 33: Truy cập SSH server thất bại nếu không thuộc 2 nhóm trên (1)

```
b1705292@desktop:~$ ssh sieu.ma@10.0.2.2
sieu.ma@10.0.2.2's password:
Permission denied, please try again.
```

Hình 34: Truy cập SSH server thất bại nếu không thuộc 2 nhóm trên (2)

```
b1705292@desktop:~$ ssh trung.hoang@10.0.2.2
trung.hoang@10.0.2.2's password:
Permission denied, please try again.
```

Hình 35: Truy cập SSH server thất bại nếu không thuộc 2 nhóm trên (3)

1.5.2. Chỉ cho chứng thực bằng private key, tạo private/public key cho người dùng luong.giacat:

+ Kết nối desktop đến server bằng người dùng luong.giacat:

```
b1705292@desktop:~$ ssh luong.giacat@10.0.2.2
luong.giacat@10.0.2.2's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Nov 25 20:35:05 2022
[luong.giacat@server ~]$
```

Hình 36: Kết nối desktop đến SSH server

+ Tạo keygen SSH: \$ssh-keygen

```

[luong.giacat@server ~]$ ssh-keygen
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:F1Lqm0AwEIVtqxZocrSCA/E5xEKpZPp0jQ0UVw9nPDQ luong.giacat@server
The key's randomart image is:
+---[RSA 3072]-----+
|o=*B+.ooE .|
|o**.+o =o+|
|B++= +. +..|
|O.=.=... . .|
|o* + .. S .|
| + . +|
|. o|
+---[SHA256]-----+

```

Hình 37: Tạo keygen SSH

+ Nhận được tập tin chứa private key (dùng cho client) và tập tin chứa public key (dùng cho server).

```

[luong.giacat@server ~]$ ls .ssh/
id_rsa id_rsa.pub

```

Hình 38: Các tập tin chứa public và private key

+ Đổi tên tập tin chứa public key thành tên khác và nằm trong thư mục .ssh/, ví dụ như: authorized_keys

Lệnh: `$mv .ssh/id_rsa.pub .ssh/authorized_keys`

```

[luong.giacat@server ~]$ ls .ssh/
authorized_keys id_rsa

```

Hình 39: Public key là Authorized_keys

+ Phân quyền lại cho tập tin chứa public key.

`$chmod 600 .ssh/authorized_keys`

```

[luong.giacat@server ~]$ ls -l .ssh/authorized_keys
-rw-----. 1 luong.giacat luong.giacat 573 Nov 25 20:36 .ssh/authorized_keys

```

Hình 40: Phân quyền cho Public key

+ Tắt chức năng chứng thực bằng password và mở chứng thực bằng public key:

`$sudo nano /etc/ssh/sshd_config`

Tìm đến dòng PubkeyAuthentication và PasswordAuthentication ta thay đổi như sau:

```
PubkeyAuthentication yes
PasswordAuthentication no
```

+ Private key nằm ở trên máy client, do đó ta sẽ tải tập tin chữ Private key này về máy client

```
[luong.giacat@server ~]$ scp luong.giacat@10.0.2.2:~/.ssh/id_rsa .
The authenticity of host '10.0.2.2 (10.0.2.2)' can't be established.
ED25519 key fingerprint is SHA256:04zlSE46ouI3S+J0W7MMWhaJXKLWid9Mo4H6tzt7TaB8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.2' (ED25519) to the list of known hosts.
id_rsa                                100% 2610    4.3MB/s   00:00
```

Hình 41: Tải Private key về desktop

+ Tập tin private key sau khi tải về có tên là known_hosts, ta sẽ đổi tên lại để dễ nhớ, ở đây ta sẽ đổi thành id_rsa:

```
b1705292@desktop:~$ cd ~/.ssh/
b1705292@desktop:~/.ssh$ ls
known_hosts
```

Hình 42: Privatekey khi tải về desktop có tên là known_hosts

```
b1705292@desktop:~$ mv ~/.ssh/known_hosts ~/.ssh/id_rsa
b1705292@desktop:~$ ls ~/.ssh/
id_rsa
```

Hình 43: Đổi tên Private key để dễ quản lý

+ Tiến hành kết nối đến server bằng private/public key với người dùng luong.giacat

Lệnh: `ssh -i <private_key_path> <username>@<ipaddress>`

Cụ thể: `ssh -i id_rsa luong.giacat@10.0.2.2`

Lưu ý: mặc định tập tin private key sẽ nằm trong thư mục .ssh/, nếu không thì phải chỉ dẫn cụ thể đường dẫn.

```
b1705292@desktop:~$ ssh -i id_rsa luong.giacat@10.0.2.2
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Nov 25 21:25:38 2022 from 10.0.2.50
[luong.giacat@server ~]$
```

Hình 44: Kết nối thành công SSH server thông qua xác thực key với người dùng luong.giacat


```
b1705292@desktop:~$ ssh -i id_rsa bi.luu@10.0.2.2
bi.luu@10.0.2.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
b1705292@desktop:~$ ssh -i id_rsa vu.quan@10.0.2.2
vu.quan@10.0.2.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

Hình 45: Kết nối thất bại đến SSH server với người dùng bi.luu (chưa tạo private key/private key không đúng)

1.6. 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 lautamquoc.com với nội dung trang chủ giới thiệu về các thành viên trong công ty.

+ Chuẩn bị trang web (gioithieu.html) được đặt trong thư mục ~/myweb, với nội dung trang chủ giới thiệu về các thành viên trong công ty.

```
[b1705292@server ~]$ mkdir ~/myweb
[b1705292@server ~]$ cd ~/myweb
[b1705292@server myweb]$ nano gioithieu.html
[b1705292@server myweb]$ cat gioithieu.html
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Công Ty Lầu Tam Quốc</title>
</head>
<body>
<H1>Welcome!</H1>
<h3>Giới thiệu các thành viên công ty:</h3>
<p>Giám đốc: Lưu Bị</p>
<p>Phó giám đốc: Gia Cát Lượng</p>
<p>Trưởng phòng: Quan Vũ, Triệu Vân</p>
<p>Nhân viên: Trương Phi, Mã Siêu, Hoàng Trung</p>
<marquee>Designed by Lý Đại Phát B1705292</marquee>
</body>
</html>
```

Hình 46: Nội dung trang web gioithieu.html

+ Tiến hành tải, chạy và đăng nhập docker (bài thực hành 5)

Các bước tiến hành:

1. Gỡ bỏ PodMan do sẽ xung đột với Docker: `$sudo dnf -y remove podman runc`
2. Cài đặt công cụ yum-utils: `$sudo dnf install -y yum-utils`
3. Thêm địa chỉ repo của Docker vào công cụ yum:

```
$sudo yum-config-manager \
```

```
--add-repo \
```

```
https://download.docker.com/linux/centos/docker-ce.repo
```

4. Cài đặt Docker: `$sudo dnf install docker-ce -y`

5. Thêm người dùng hiện tại vào nhóm docker: `$sudo usermod -aG docker $USER`
6. Login lại vào shell: `$su - $USER`
7. Chạy dịch vụ Docker và cho phép Docker khởi động cùng hệ thống:

`$sudo systemctl start docker`

`$sudo systemctl enable docker`

8. Đăng nhập vào Docker: `$docker login -u <docker-username>`
9. Kiểm tra Docker đã hoạt động tốt chưa: `$docker run hello-world`

+ Triển khai dịch vụ web:

Kiểm tra thông tin các image httpd có trên docker hub: `$docker search httpd`

Tạo container từ image httpd:

`$docker run -d -it -p 8080:80 --name tamquocwebserver httpd`

-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

--name tamquocwebserver: đặt tên container là tamquocwebserver

-p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container

```
[b1705292@server ~]$ docker run -d -it -p 8080:80 --name tamquocwebserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
a603fa5e3b41: Pull complete
4691bd33efec: Pull complete
ff7b0b8c417a: Pull complete
9df1012343c7: Pull complete
b1c114085b25: Pull complete
Digest: sha256:f2e89def4c032b02c83e162c1819ccfcbd4ea6bdb5ff784bbc68cba940a9046
Status: Downloaded newer image for httpd:latest
31743a4b7581096fd23cf8fa3c8459ca98e469d2c7a6c28b18ed776f06ee5d57
[b1705292@server ~]$
```

Hình 47: Tạo container tamquocwebserver từ image httpd

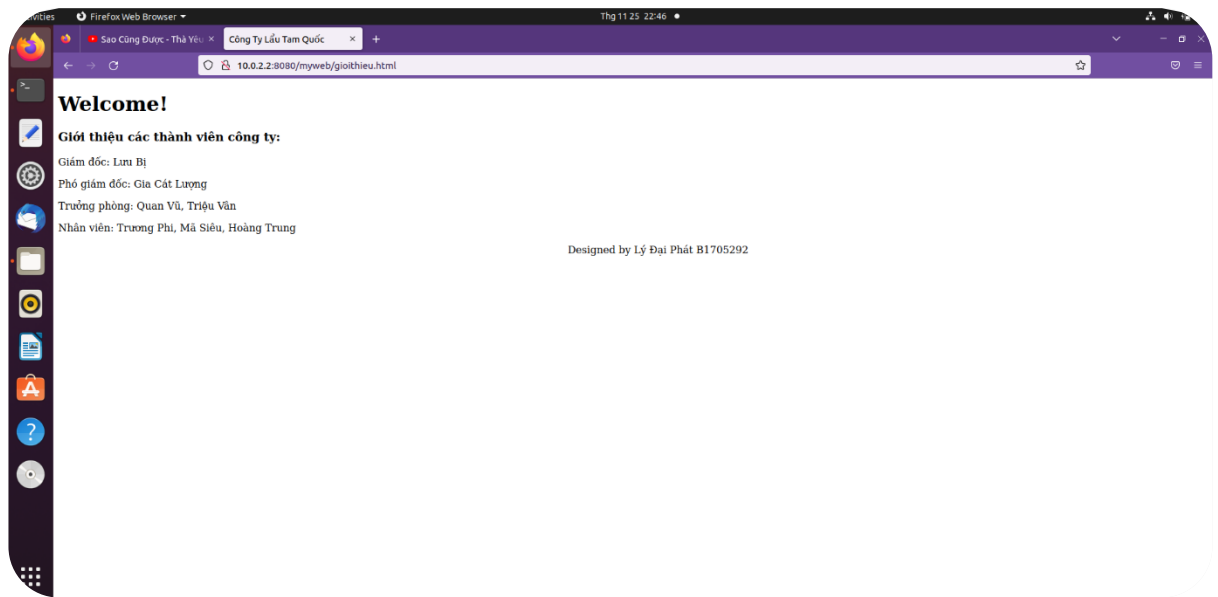
Sao chép thư mục ~/myweb chứa nội dung gioithieu.html vào thư mục gốc của dịch vụ web trên Docker container.

`$docker cp myweb/ tamquocwebserver:/usr/local/apache2/htdocs/`

Sao chép thư mục ~/myweb chứa nội dung gioithieu.html vào thư mục gốc của dịch vụ máy chủ web Apache.

`$sudo cp myweb/ /var/www/html`

+ Trên máy desktop, vào địa chỉ 10.0.2.2:8080/myweb/gioithieu.html tiến hành kiểm chứng trang web vừa tạo:



Hình 48: Triển khai dịch vụ web với Docker thành công

1.7. 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.

+ Cài đặt dịch vụ FTP trên server: `$sudo dnf install -y vsftpd`

+ Cấu hình dịch vụ FTP: `$sudo nano /etc/vsftpd/vsftpd.conf`

```
anonymous_enable=NO
local_enable=YES
local_umask=022
anon_upload_enable=NO
local_root = /data
```

+ Khởi động lại dịch vụ FTP:

`$sudo systemctl start vsftpd`

`$sudo systemctl enable vsftpd`

`$sudo systemctl status vsftpd`

```
[b1705292@server ~]$ sudo systemctl start vsftpd
[b1705292@server ~]$ sudo systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[b1705292@server ~]$ sudo systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-25 23:26:11 +07; 12s ago
```

Hình 49: Khởi động dịch vụ FTP

+ Tắt tường lửa:

\$sudo systemctl stop firewalld

+ Kiểm tra kết quả theo yêu cầu:

Trên desktop tạo file desktop.txt: \$touch desktop.txt

```
b1705292@desktop:~$ touch desktop.txt
b1705292@desktop:~$ ls
Desktop      Documents  id_rsa     Pictures    Templates
desktop.txt  Downloads  Music      Public      Videos
```

Hình 50: Tạo file kiểm chứng trên desktop

Kết nối desktop đến server bằng một tài khoản người dùng bất kỳ (Ở đây sẽ dùng tài khoản luong.giacat): \$pftp 10.0.2.2

```
b1705292@desktop:~$ pftp 10.0.2.2
Connected to 10.0.2.2.
220 (vsFTPd 3.0.3)
Name (10.0.2.2:phat): luong.giacat
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Hình 51: Kết nối đến FTP server

Thử di chuyển đến các thư mục khác, ngoài thư mục /data:

```
ftp> pwd
257 "/data" is the current directory
ftp> cd /home/b1705292
550 Failed to change directory.
ftp> cd /home/bi.luu
550 Failed to change directory.
```

Hình 52: Các thư mục khác /data đều bị chặn truy cập

Thử upload file từ desktop lên server: \$put desktop.txt

```
b1705292@desktop:~$ pftp 10.0.2.2
Connected to 10.0.2.2.
220 (vsFTPd 3.0.3)
Name (10.0.2.2:phat): luong.giacat
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put desktop.txt
local: desktop.txt remote: desktop.txt
227 Entering Passive Mode (10,0,2,2,148,175).
550 Permission denied.
```

Hình 53: Chặn upload file từ desktop lên server

Trên server, đăng nhập với người dùng luong.giacat, tạo file server.txt:

```
[luong.giacat@server ~]$ touch server.txt
[luong.giacat@server ~]$ ls
id_rsa  server.txt
```

Hình 54: Tạo file kiểm chứng trên server

Trên desktop kết nối với ftp bằng tài khoản luong.giacat, thử download file từ server về desktop:

\$get server.txt

```
Name (10.0.2.2:phat): luong.giacat
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,0,2,2,248,49).
150 Here comes the directory listing.
-rw-----  1 1003      1003      2610 Nov 25 13:59 id_rsa
-rw-r--r--  1 1003      1003           0 Nov 25 17:29 server.txt
226 Directory send OK.
ftp> get server.txt
local: server.txt remote: server.txt
227 Entering Passive Mode (10,0,2,2,124,27).
150 Opening BINARY mode data connection for server.txt (0 bytes).
226 Transfer complete.
```

Hình 55: Cho phép download file từ server về desktop

```
b1705292@desktop:~$ ls
Desktop  Documents  id_rsa  Pictures  server.txt  Videos
desktop.txt  Downloads  Music  Public  Templates
```

Hình 56: Download file trên server thành công về desktop

1.8. 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 BIND và các công cụ cần thiết (đã cài trong lab5)

Lệnh: \$sudo dnf install bind bind-utils -y

1.8.2. Cấu hình DNS server:

+ Mở file cấu hình: \$sudo nano /etc/named.conf

+ Nội dung file cấu hình:

```
...
options {
    listen-on port 53 { 127.0.0.1; any; }; #
    ...
    allow-query { localhost; any; };
    recursion yes;
    forwarders {10.0.2.1; };
    ...
};
logging {
    ...
};
zone "." IN {
    ...
};
zone "lautamquoc.com" IN {
    type master;
    file "forward.qtht";
    allow-update { none; };
};
zone "2.0.10.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
    allow-update { none; };
};
...
```

1.8.3. Tạo tập tin cấu hình phân giải xuôi:

Bước 1: Tùý biến tập tin cấu hình phân giải xuôi từ tập tin cấu hình gốc.

```
$sudo cp /var/named/named.localhost /var/named/forward.qtht
```

Bước 2: Thay đổi nhóm sở hữu root thành nhóm named cho tập tin forward.qtht:

*Nếu giữ nguyên nhóm sở hữu là root thì dịch vụ DNS không có quyền truy cập tập tin này.

```
$sudo chgrp named /var/named/forward.qtht
```

Bước 3: Tiến hành cấu hình tập tin forward.qtht:

```
$sudo nano /var/named/forward.qtht
```

+ Nội dung file cấu hình phân giải xuôi:

```
$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
```

1.8.4. Tạo tập tin cấu hình phân giải ngược:

Bước 1: Tùy biến tập tin cấu hình phân giải ngược từ tập tin cấu hình xuôi.

```
$sudo cp /var/named/forward.qhth /var/named/reverse.qhth
```

Bước 2: Thay đổi nhóm sở hữu root thành nhóm named cho tập tin reverse.qhth:

*Nếu giữ nguyên nhóm sở hữu là root thì dịch vụ DNS không có quyền truy cập tập tin này.

```
$sudo chgrp named /var/named/reverse.qhth
```

Bước 3: Tiến hành cấu hình tập tin reverse.qhth:

```
$sudo nano /var/named/reverse.qhth
```

+ Nội dung file cấu hình phân giải ngược:

```
$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.
```

1.8.5. Kiểm tra và sử dụng dịch vụ DNS:

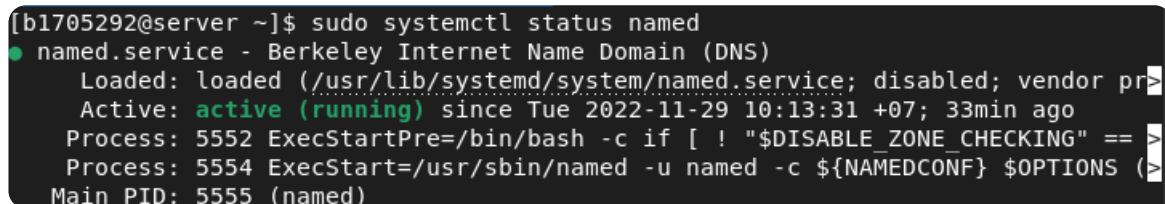
Bước 1: Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

Bước 2: Khởi động dịch vụ DNS và kiểm tra trạng thái dịch vụ DNS:

\$sudo systemctl start named

\$sudo systemctl status named



```
[b1705292@server ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor pr
   Active: active (running) since Tue 2022-11-29 10:13:31 +07; 33min ago
     Process: 5552 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==
     Process: 5554 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (
   Main PID: 5555 (named)
```

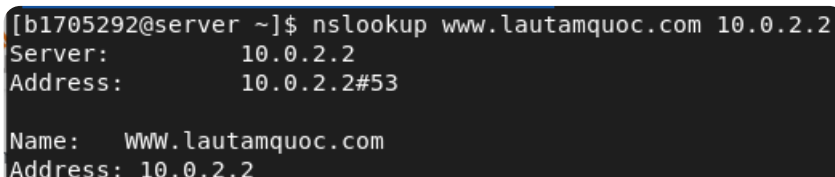
Hình 57: Khởi động và kiểm tra trạng thái dịch vụ DNS

Bước 3: Kiểm tra kết quả:

Trên Server:

+ Tiến hành phân giải xuôi các địa chỉ sau:

\$nslookup www.lautamquoc.com 10.0.2.2

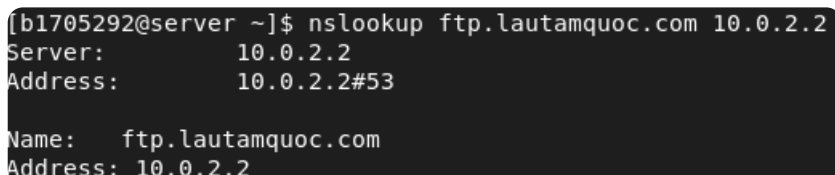


```
[b1705292@server ~]$ nslookup www.lautamquoc.com 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Name:   WWW.lautamquoc.com
Address: 10.0.2.2
```

Hình 58: Phân giải tên miền www.lautamquoc.com trên server

\$nslookup ftp.lautamquoc.com 10.0.2.2

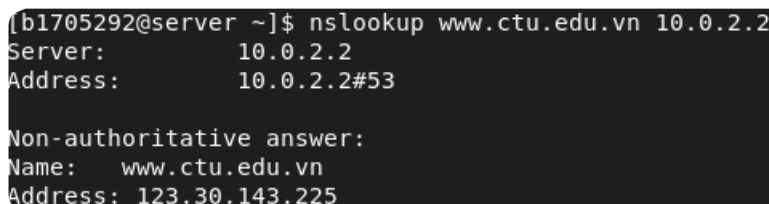


```
[b1705292@server ~]$ nslookup ftp.lautamquoc.com 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Name:   ftp.lautamquoc.com
Address: 10.0.2.2
```

Hình 59: Phân giải tên miền ftp.lautamquoc.com trên server

\$nslookup www.ctu.edu.vn 10.0.2.2



```
[b1705292@server ~]$ nslookup www.ctu.edu.vn 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Non-authoritative answer:
Name:   www.ctu.edu.vn
Address: 123.30.143.225
```

Hình 60: Phân giải tên miền www.ctu.edu.vn trên server

+ Tiến hành phân giải ngược địa chỉ IP sau:

\$nslookup 10.0.2.2 10.0.2.2


```
[b1705292@server ~]$ nslookup 10.0.2.2 10.0.2.2
2.2.0.10.in-addr.arpa    name = ftp.lautamquoc.com.
2.2.0.10.in-addr.arpa    name = www.lautamquoc.com.
```

Hình 61: Phân giải ngược địa chỉ 10.0.2.2 trên server

Trên Desktop:

+ Tiến hành phân giải xuôi các địa chỉ sau:

\$nslookup www.lautamquoc.com 10.0.2.2

```
b1705292@desktop:~$ nslookup www.lautamquoc.com 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Name:   WWW.lautamquoc.com
Address: 10.0.2.2
```

Hình 62: Phân giải tên miền www.lautamquoc.com trên desktop

\$nslookup ftp.lautamquoc.com 10.0.2.2

```
b1705292@desktop:~$ nslookup ftp.lautamquoc.com 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Name:   ftp.lautamquoc.com
Address: 10.0.2.2
```

Hình 63: Phân giải tên miền ftp.lautamquoc.com trên desktop

\$nslookup www.ctu.edu.vn 10.0.2.2

```
b1705292@desktop:~$ nslookup www.ctu.edu.vn 10.0.2.2
Server:          10.0.2.2
Address:         10.0.2.2#53

Non-authoritative answer:
Name:   www.ctu.edu.vn
Address: 123.30.143.225
```

Hình 64: Phân giải tên miền www.ctu.edu.vn trên desktop

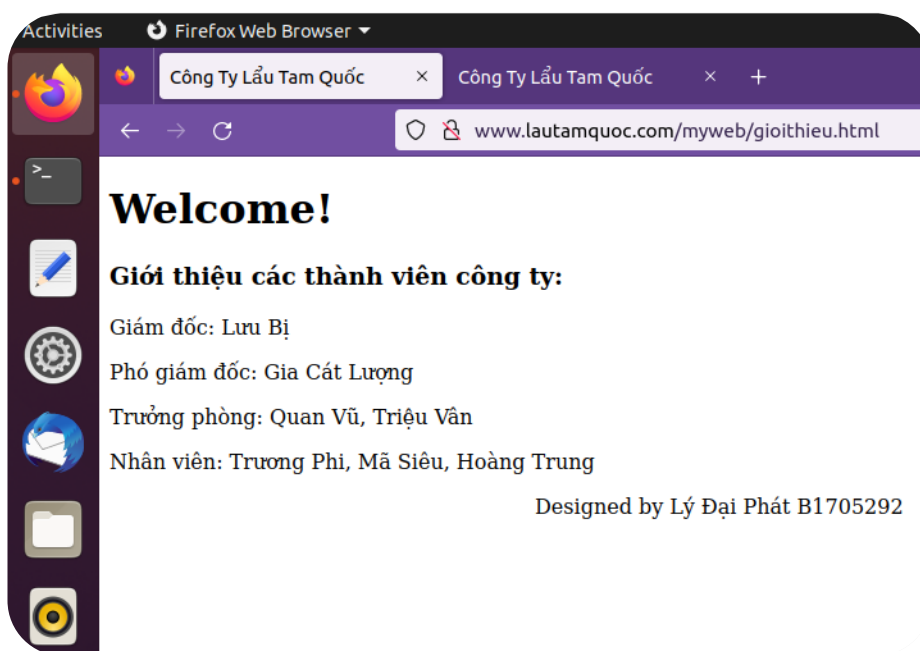
+ Tiến hành phân giải ngược địa chỉ IP sau:

\$nslookup 10.0.2.2 10.0.2.2

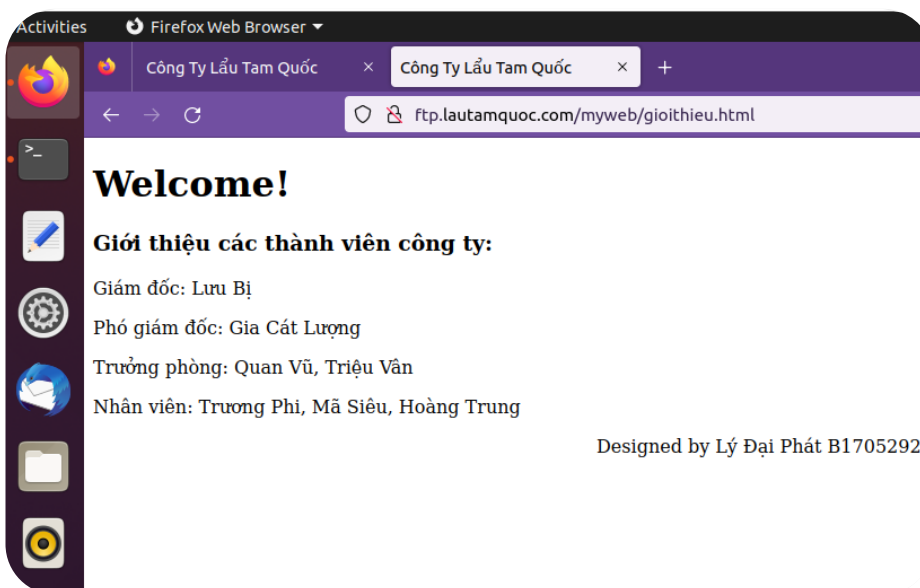
```
b1705292@desktop:~$ nslookup 10.0.2.2 10.0.2.2
2.2.0.10.in-addr.arpa    name = www.lautamquoc.com.
2.2.0.10.in-addr.arpa    name = ftp.lautamquoc.com.
```

Hình 65: Phân giải ngược địa chỉ 10.0.2.2 trên desktop

+ Vào trình duyệt web, kiểm tra các địa chỉ tên miền sau:



Hình 66: Kiểm tra tên miền www.lautamquoc.com trên trình duyệt web desktop



Hình 67: Kiểm tra tên miền ftp.lautamquoc.com trên trình duyệt web desktop

1.9. Cài đặt và cấu hình tường lửa trên server để cho phép:

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

+ **Bước 1:** Khởi động tường lửa firewalld

```
$sudo systemctl start firewalld
```

+ **Bước 2:** Tạo zone mới có tên là tamquocserver

```
$sudo firewall-cmd --permanent --new-zone=tamquocserver
```

```
[b1705292@server ~]$ sudo firewall-cmd --permanent --new-zone=tamquocserver
[sudo] password for b1705292:
success
```

Hình 68: Tạo zone tamquocserver

+ **Bước 3:** Khởi động lại tường lửa để áp dụng zone mới vừa tạo ra

```
$sudo systemctl restart firewalld
```

+ **Bước 4:** Kiểm tra các rule của zone tamquocserver (mặc định chặn tất cả các dữ liệu và dịch vụ mạng)

```
$sudo firewall-cmd --list-all --zone=tamquocserver
```

```
[b1705292@server ~]$ sudo firewall-cmd --list-all --zone=tamquocserver
tamquocserver
target: default
icmp-block-inversion: no
interfaces:
sources:
services:
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Hình 69: Xem các rule của zone tamquocserver vừa tạo ra

+ **Bước 5:** Cho phép các dịch vụ DNS, DHCP, SSH, Web, FTP hoạt động trên zone tamquocserver

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dhcp
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=ssh
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=https
```

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
```

```
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=dns
success
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=dhcp
success
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=ssh
success
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=http
success
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=https
success
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-service=ftp
success
```

Hình 70: Cho phép các dịch vụ được thực thi trên zone tamquocserver

Ta có thể liệt kê các dịch vụ khác có thể thêm vào zone: \$firewall-cmd --get-services

```
[b1705292@server ~]$ firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd aud
it bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bitt
orrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6
-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch
etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps f
reeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git grafana gre h
igh-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenk
ins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver k
ube-control-plane kube-controller-manager kube-scheduler kubelet-worker ldap ldaps libvirt
libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh
mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp n
ut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pm
webapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster qua
sssl radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba sam
ba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lan
sync spotify-sync squid sssd ssh steam-streaming svdrp svn syncthing syncthing-gui synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-clien
t vdsms vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client x
mpp-local xmpp-server zabbix-agent zabbix-server
```

Hình 71: Một số dịch vụ khác có thể thêm vào zone

+ **Bước 6:** Thêm rule chỉ cho phép máy desktop SSH đến server

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule
family=ipv4 source address=10.0.2.50/32 port port=22 protocol=tcp accept'
```

```
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --add-rich-rule='ru
le family=ipv4 source address=10.0.2.50/32 port port=22 protocol=tcp accept'
success
```

Hình 72: Cho phép dữ liệu mạng có giao thức IPv4 với địa chỉ 10.0.2.50 và cổng dịch vụ SSH là 22

+ **Bước 7:** Khởi động lại tường lửa, chuyển giao diện mạng sang zone tamquocserver và kiểm tra các rule đã thiết lập trên zone.

```
$sudo systemctl restart firewallld
```

```
[b1705292@server ~]$ sudo systemctl restart firewalld
[b1705292@server ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: en>
   Active: active (running) since Thu 2022-12-01 15:35:06 +07; 7s ago
     Docs: man:firewalld(1)
    Main PID: 4079 (firewalld)
      Tasks: 2 (limit: 10945)
     Memory: 25.2M
        CPU: 428ms
    CGroup: /system.slice/firewalld.service
            └─4079 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
```

Hình 73: Khởi động lại và kiểm tra trạng thái tường lửa

\$sudo firewall-cmd --permanent --zone=tamquocserver --change-interface=enp0s3

```
[b1705292@server ~]$ sudo firewall-cmd --permanent --zone=tamquocserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'tamquocserver'.
success
```

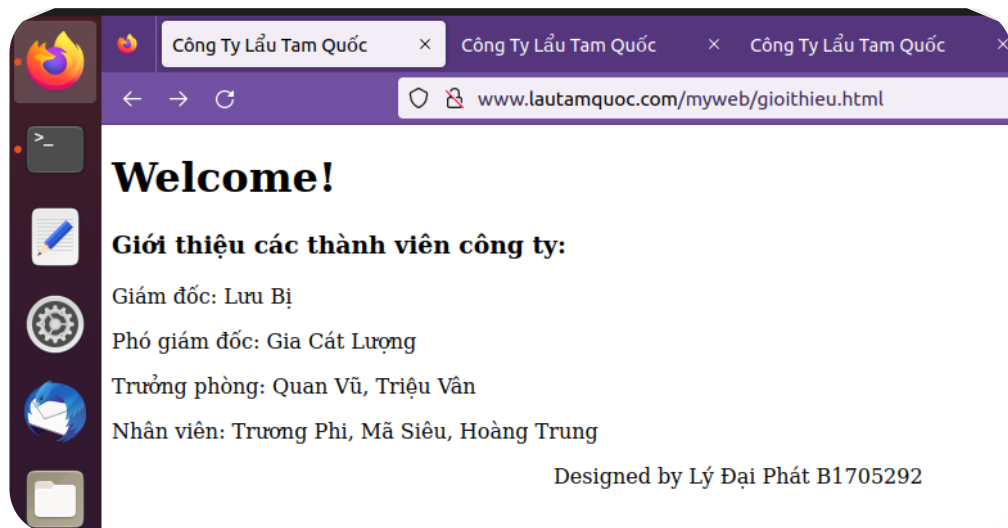
Hình 74: Áp dụng zone tamquocserver cho card mạng enp0s3

\$sudo firewall-cmd --list-all --zone=tamquocserver

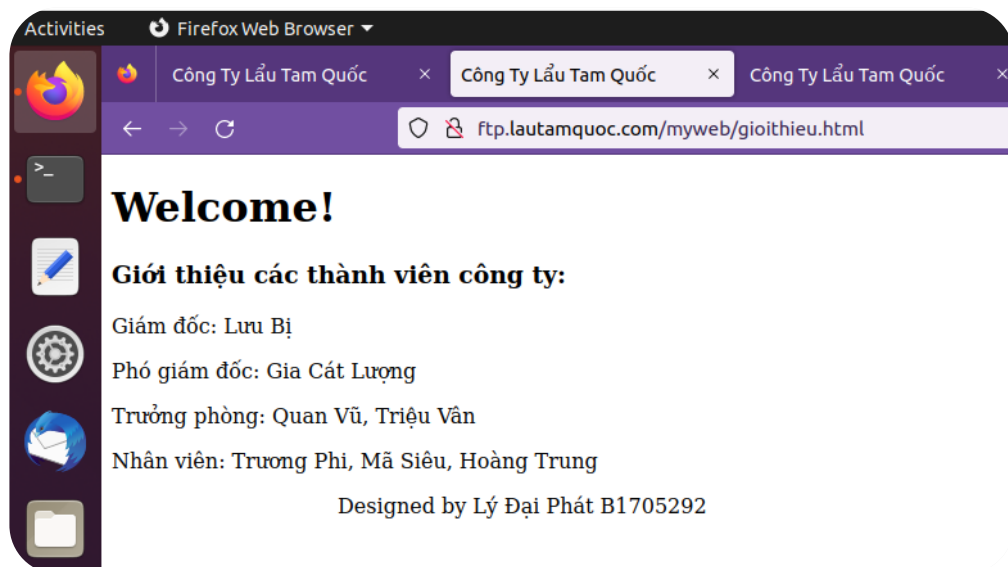
```
[b1705292@server ~]$ sudo firewall-cmd --list-all --zone=tamquocserver
tamquocserver (active)
  target: default
 icmp-block-inversion: no
 interfaces: enp0s3
  sources:
 services: dhcp dns ftp http https ssh
  ports:
 protocols:
 forward: no
 masquerade: no
 forward-ports:
 source-ports:
 icmp-blocks:
 rich rules:
 rule family="ipv4" source address="10.0.2.50/32" port port="22" protocol="tcp" accept
```

Hình 75: Liệt kê các rule của zone tamquocserver

+ **Bước 8:** Kiểm tra kết quả.



Hình 76: Kết nối đến dịch vụ Web thành công (1)



Hình 77: Kết nối đến dịch vụ Web thành công (2)

```
b1705292@desktop:~$ nslookup www.lautamquoc.com 10.0.2.2
Server:      10.0.2.2
Address:     10.0.2.2#53

Name:   WWW.lautamquoc.com
Address: 10.0.2.2

b1705292@desktop:~$ nslookup ftp.lautamquoc.com 10.0.2.2
Server:      10.0.2.2
Address:     10.0.2.2#53

Name:   ftp.lautamquoc.com
Address: 10.0.2.2
```

Hình 78: Kết nối đến dịch vụ DNS thành công

```
b1705292@desktop:~$ ssh -i id_rsa luong.giacat@10.0.2.2
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Nov 26 00:28:05 2022
[luong.giacat@server ~]$
```

Hình 79:: Kết nối đến dịch vụ SSH thành công

```
b1705292@desktop:~$ pftp 10.0.2.2
Connected to 10.0.2.2.
220 (vsFTPD 3.0.3)
Name (10.0.2.2:phat): luong.giacat
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Hình 80: Kết nối đến dịch vụ FTP thành công

```
b1705292@desktop:~$ sudo nmap --script broadcast-dhcp-discover
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-01 15:57 +07
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 10.0.2.51
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 10.0.2.2
|     IP Address Lease Time: 5m00s
|     Subnet Mask: 255.255.255.0
|     Router: 10.0.2.1
|     Domain Name Server: 10.0.2.2, 8.8.8.8
|_
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.44 seconds
```

Hình 81: Kết nối đến dịch vụ DHCP thành công (*sudo dns install nmap)

1.10. Sử dụng dịch vụ cron và shell script tự động thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng như sau:

+ 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.

Các bước thực hiện:

+ **Bước 1:** Lần lượt tạo các shell script sao lưu các thư mục /home, /data và /etc, sau đó nén lại và lưu vào /mnt/backup với dữ liệu nén có tên như yêu cầu.

+ **Bước 2:** Dùng crontab để thực hiện công việc vào thời gian như yêu cầu.

1.10.1. Tạo shell script:

+ Tạo shellscript có tên là everyDayBackup.sh, dùng để thực hiện các công việc sau:

- Tạo thư mục /mnt/backup để chứa dữ liệu sao lưu nếu thư mục trên chưa tồn tại.
- Dữ liệu từ các thư mục sao lưu sẽ được nén và lưu với tên backup_<thứ>.
- Hiển thị file vừa tạo nếu sao lưu thành công, ngược lại báo lỗi nếu sao lưu thất bại.

+ Tạo shellscript có tên là everyWeekBackup.sh, dùng để thực hiện các công việc sau:

- Tạo thư mục /mnt/backup để chứa dữ liệu sao lưu nếu thư mục trên chưa tồn tại.
- Dữ liệu từ các thư mục sao lưu sẽ được nén và lưu với tên backup_<thứ tự tuần> (thứ tự tuần trong 1 năm, bắt đầu từ 1-53 theo chuẩn ISO).
- Hiển thị file vừa tạo nếu sao lưu thành công, ngược lại báo lỗi nếu sao lưu thất bại.

+ Tạo shellscript có tên là everyMonthBackup.sh, dùng để thực hiện các công việc sau:

- Tạo thư mục /mnt/backup để chứa dữ liệu sao lưu nếu thư mục trên chưa tồn tại.
- Kiểm tra tháng hiện tại là tháng chẵn hay tháng lẻ, nếu là tháng chẵn thì dữ liệu từ các thư mục sao lưu sẽ được nén và lưu với tên backup_month1, ngược lại là backup_month2.
- Hiển thị file vừa tạo nếu sao lưu thành công, ngược lại báo lỗi nếu sao lưu thất bại.

Nội dung file everyDayBackup.sh:

```

echo "Starting backup data everyday!"
echo "Time: $(date) "
echo "-----Waiting!-----"
if [ ! -d "mnt" ]
then
    mkdir mnt
    mkdir mnt/backup
fi

fileName="mnt/backup/backup_$(date +%A).tar"
tar -cf $fileName /home /data /etc
if [ $? -eq 0 ]
then
    echo "Successfully backup"
    echo "List information"
    ls -l mnt/backup/$filename
else
    echo "Warning: An error occurred"
fi

```

Nội dung file everyWeekBackup.sh:

```

echo "Starting backup data every week!"
echo "Time: $(date) "
echo "-----Waiting!-----"
if [ ! -d "mnt" ]
then
    mkdir mnt
    mkdir mnt/backup
fi

fileName="mnt/backup/backup_week$(date +%V).tar"
tar -cf $fileName /home /data /etc
if [ $? -eq 0 ]
then
    echo "Successfully backup"
    echo "List information"
    ls -l mnt/backup/$filename
else
    echo "Warning: An error occurred"
fi

```

Nội dung file everyMonthBackup.sh:

```

echo "Starting backup data every month!"
echo "Time: $(date) "
echo "-----Waiting!-----"
if [ ! -d "mnt" ]
then
    mkdir mnt
    mkdir mnt/backup
fi

getMonth=$(date +%m)
val=`expr $getMonth % 2 `
if [ $val -eq 0 ]
then
    fileName="mnt/backup/backup_month2.tar"
else
    fileName="mnt/backup/backup_month1.tar"
fi

tar -cf $fileName /home /data /etc
if [ $? -eq 0 ]
then
    echo "Successfully backup"
    echo "List information"
    ls -l mnt/backup/$filename
else
    echo "Warning: An error occurred"
fi
    
```

1.10.2. Lên lịch với Crontab.

+ Dùng trình soạn thảo nano để lên lịch các công việc cần thực hiện:

```
$export EDITOR=nano
```

```
$crontab -e
```

+ Giải thích:

- 59 23 * * * (/home/b1705292/everyDayBackup.sh): thực thi file everyDayBackup.sh vào 23:59 mỗi ngày từ thứ 2 đến thứ 7.
- 59 23 * * 0 (/home/b1705292/everyWeekBackup.sh): thực thi file everyWeekBackup.sh vào 23:59 mỗi chủ nhật hàng tuần.
- 59 23 1 * * (/home/b1705292/everyMonthBackup.sh): thực thi file everyMonthBackup.sh vào 23:59 ngày 1 hàng tháng.

+ Nội dung file /tmp/crontab.Vi0FH2:

```
59 23 * * * (/home/b1705292/everyDayBackup.sh)
59 23 * * 0 (/home/b1705292/everyWeekBackup.sh)
59 23 1 * * (/home/b1705292/everyMonthBackup.sh)
```

Để Crontab thực thi được cái file shell script thì ta cần cấp quyền thực thi:

\$chmod +x everyDayBackup.sh

\$chmod +x everyWeekBackup.sh

\$chmod +x everyMonthBackup.sh

```
-rwxr-xr-x. 1 b1705292 b1705292 395 Dec 1 19:52 everyDayBackup.sh
-rwxr-xr-x. 1 b1705292 b1705292 511 Dec 1 20:07 everyMonthBackup.sh
-rwxr-xr-x. 1 b1705292 b1705292 398 Dec 1 19:37 everyWeekBackup.sh
```

Hình 82: Cấp quyền thực thi cho các shell script

Vậy là ta đã lên lịch các công việc với Crontab và shell script theo như yêu cầu!

1.10.3. Kiểm tra việc lên lịch Crontab và các file shell script.

Để dễ kiểm tra, ta thay đổi nội dung file Crontab để thực thi các file shell script sau mỗi phút.

```
* * * * * (/home/b1705292/everyDayBackup.sh)
* * * * * (/home/b1705292/everyWeekBackup.sh)
* * * * * (/home/b1705292/everyMonthBackup.sh)
```

```
[b1705292@server ~]$ ls
Desktop    everyDayBackup.sh  Music      Public      Videos
Documents  everyMonthBackup.sh myweb      server.txt
Downloads  everyWeekBackup.sh Pictures    Templates
```

Hình 83: Trước khi Crontab thực thi các công việc (1)

Sau một phút, ta thử mở thư mục /mnt/backup xem các file dữ liệu nén có được tạo ra hay không?

```
[b1705292@server ~]$ ls
Desktop    everyDayBackup.sh  mnt        Pictures    Templates
Documents  everyMonthBackup.sh Music       Public      Videos
Downloads  everyWeekBackup.sh myweb      server.txt
[b1705292@server ~]$ cd mnt/backup
[b1705292@server backup]$ ls
backup_month2.tar backup_Thursday.tar backup_week48.tar
[b1705292@server backup]$
```

Hình 84: Sau 1 phút, Crontab thực thi các công việc (2)

Ta thấy các thư mục sao lưu /mnt/backup và các file backup_month2.tar, backup_Thursday.tar, backup_week48.tar đã được tạo ra. Vậy các shell script và crontab đã thực thi đúng như yêu cầu.

-HẾT-