LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Võ Thành Em B2012081

Nhóm học phần: CT179_01

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.

- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.

1. **Triển khai dịch vụ WEB sử dụng Docker**

1.1. Thực hiện cài đặt CentOS 9 vào máy tính cá nhân (hoặc máy ảo).

1.2. Cấu hình mạng cho máy ảo giao tiếp được với máy vật lý và kết nối được vào Internet. (Câu 2 - Lab04)

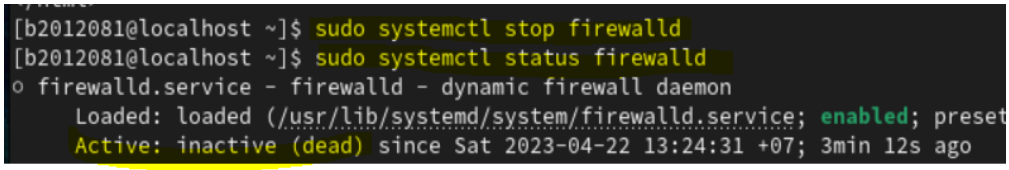
1.3. Tạo thư mục `~/myweb`, sau đó tạo một trang web đơn giản `index.html` lưu vào thư mục `~/myweb`.(Câu 6 - Lab04)

Dùng lệnh $tree xem lại cây thư mục


```
[b2012081@localhost ~]$ cat myweb/index.html
<!doctype html>
<html>
<head>
        <meta charset="utf-8">
        <title>Tổng công ty bánh kẹo Lương Sơn Bạc</title>
</head>
<body>
        <H1>Welcome!<H1>
        <marquee>Designed by B12345678</marquee>
</body>
</html>
```

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```



Xem lại thông tin cấu hình của Centos9 và kiểm tra kết nối mạng

```
[b2012081@localhost ~]$ nmcli -f ipv4.dns,ipv4.addresses,ipv4.gateway con show enp0s3
ipv4.dns:                               203.113.188.1,203.113.131.3
ipv4.addresses:                         192.168.1.245/24
ipv4.gateway:                           192.168.1.1
[b2012081@localhost ~]$
```

```
C:\Users\Thanh Em>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
[b2012081@localhost ~]$ 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=56 tim
e=58.9 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=2 ttl=56 tim
e=70.0 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=3 ttl=56 tim
e=61.7 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
```

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

1.4. Cài đặt Docker lên máy ảo CentOS 9

- Gỡ bỏ PodMan (do sẽ đụng độ với Docker)

```
$sudo dnf -y remove podman runc
```

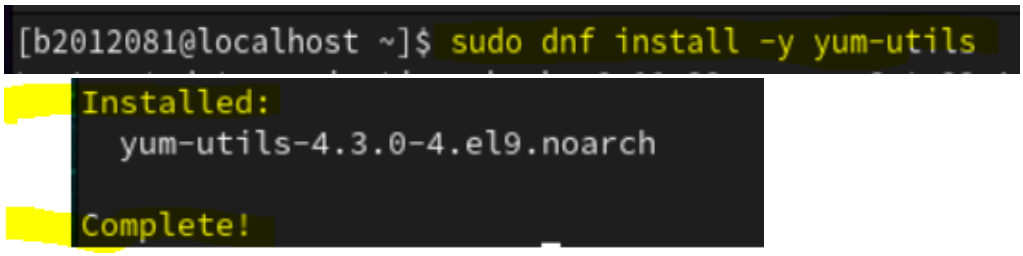
```
[b2012081@localhost ~]$ sudo dnf -y remove podman runc
Dependencies resolved.

Removed:
  cockpit-podman-63.1-1.el9.noarch
  podman-2:4.4.1-3.el9.x86_64
  shadow-utils-subid-2:4.9-6.el9.x86_64

Complete!
```

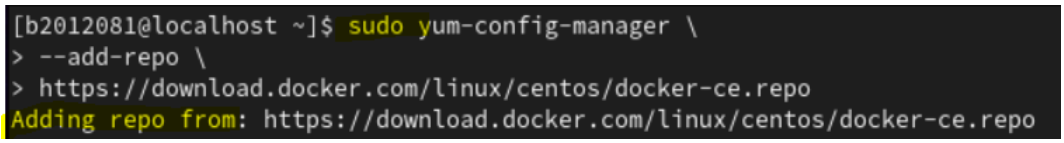
- Cài đặt công cụ yum-utils

```
$sudo dnf install -y yum-utils
```



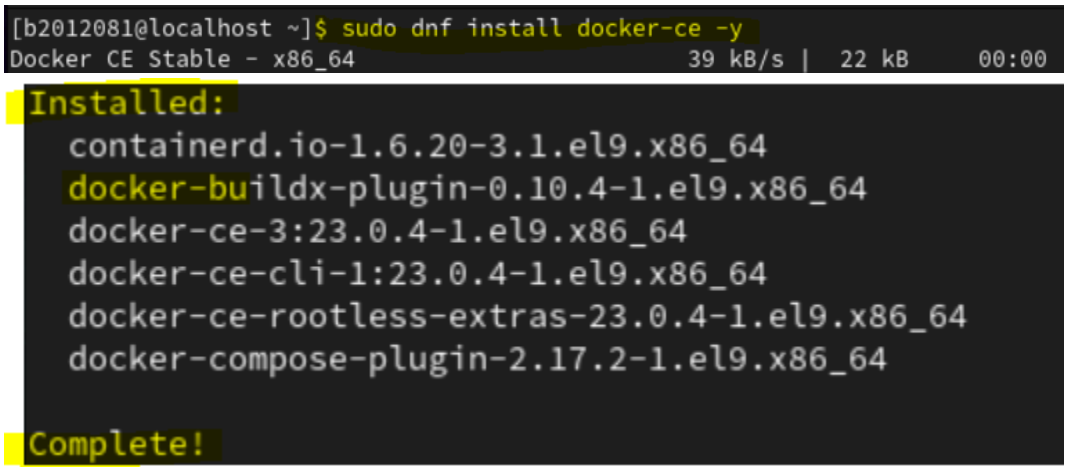
- Thêm địa repo của Docker vào công cụ yum

```
$sudo yum-config-manager \
--add-repo \
https://download.docker.com/linux/centos/docker-ce.repo
#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.
```



- Cài đặt Docker

```
$sudo dnf install docker-ce -y
```



- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo

```
$sudo usermod -aG docker $USER
```

- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng

```
$su - $USER
```

```
[b2012081@localhost ~]$ sudo usermod -aG docker $USER
[sudo] password for b2012081:
[b2012081@localhost ~]$ su - $USER
```

- Chạy dịch vụ Docker

```
$sudo systemctl start docker
$sudo systemctl enable docker
```

```
[b2012081@localhost ~]$ sudo systemctl start docker
[b2012081@localhost ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /us
r/lib/systemd/system/docker.service.
```

```
[b2012081@localhost ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: d
     Active: active (running) since Sat 2023-04-22 13:43:16 +07; 1min 30s ago
```

- Tạo 1 tài khoản trên DockerHub (https://hub.docker.com/), sau đó đăng nhập sử dụng lệnh sau:

```
$docker login -u <docker-username>
```

```
[b2012081@localhost ~]$ docker login -u emvo2002
Password:
WARNING! Your password will be stored unencrypted in /home/b2012081/.docker/conf
ig.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

- Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.

```
$docker run hello-world
```

```
[b2012081@localhost ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:4e83453afed1b4fa1a3500525091dbfca6ce1e66903fd4c01ff015dbcb1ba33e
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
```

1.5. Triển khai dịch vụ web server lên máy ảo CentOS 9 sử dụng một Docker container

- Tìm kiếm image với từ khóa httpd, kết quả sẽ thấy 1 image tên httpd ở dòng đầu tiên.

```
$docker search httpd
```

```
centos/httpd-24-centos7             Platform for running Apache httpd 2.4 or bui…   45

manageiq/httpd                      Container with httpd, built on CentOS for Ma…   1
                [OK]
centos/httpd-24-centos8                                                             1

dockerpinata/httpd                                                                  1
```

- Tạo container từ image httpd

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

  `-d`: chạy container ở chế độ background

  `-it`: tạo shell để tương tác với container

  `--name webserver`: đặt tên container là webserver

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

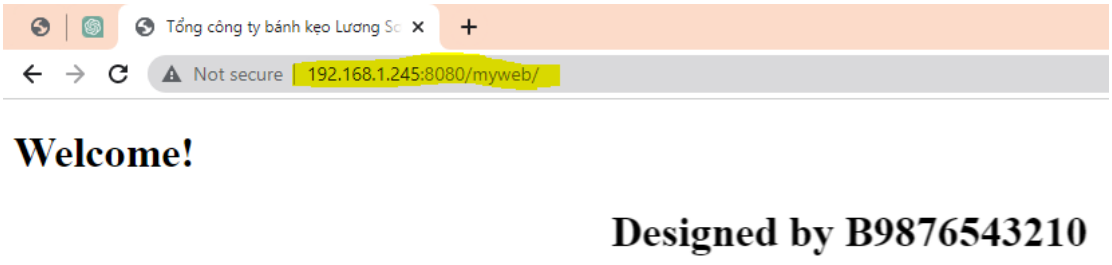
```
[b2012081@localhost ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
26c5c85e47da: Pull complete
2d29d3837df5: Pull complete
2483414a5e59: Pull complete
e78016c4ba87: Pull complete
757908175415: Pull complete
Digest: sha256:a182ef2350699f04b8f8e736747104eb273e255e818cd55b6d7aa50a1490ed0c
Status: Downloaded newer image for httpd:latest
492b769fc398a4b6fc03412c89a77e813bfbf7128c24a854df7fb262797a075c
```

- Sao chép thư mục `~/myweb` vào thư mục gốc của dịch vụ của web trên Docker container

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

```
[b2012081@localhost ~]$ nano myweb/index.html
[b2012081@localhost ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
```

- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ `http://<Địa chỉ IP máy ảo CentOS>:8080/myweb` để kiểm chứng trang web vừa tạo.



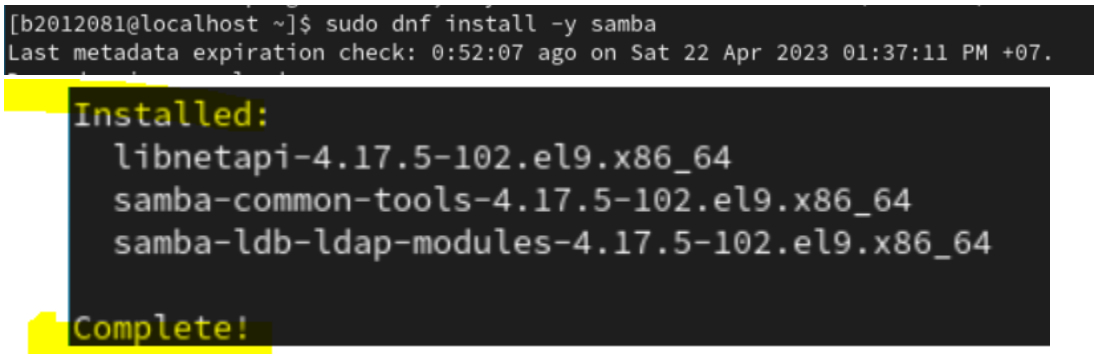
2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các hệ điều hành khác nhau như Windows và Linux bằng cách sử dụng giao thức SMB/CIFS. Trong bài thực hành sinh viên sẽ cài đặt và cấu hình dịch vụ Samba trên máy chủ CentOS và sử dụng máy Windows để truy cập tới dịch vụ.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

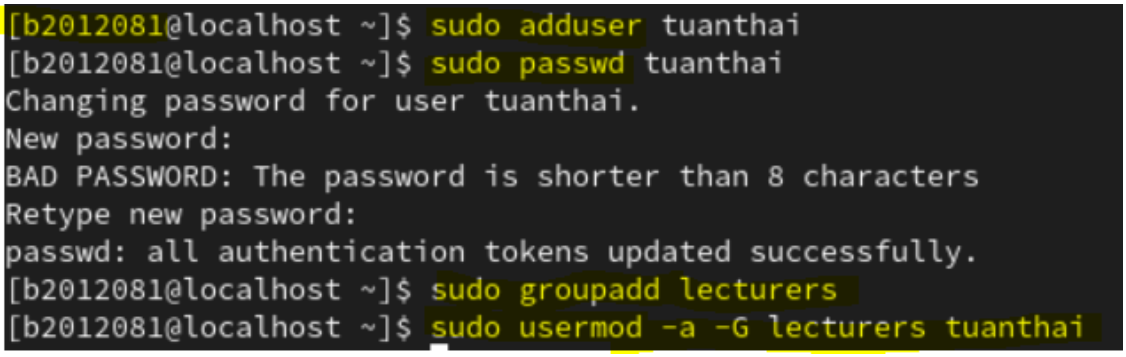
- Cài đặt dịch vụ Samba:

```
$sudo dnf install -y samba
```



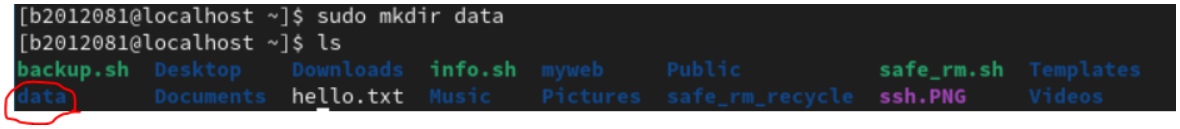
- Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

```
$sudo adduser tuanthai
$sudo passwd tuanthai
$sudo groupadd lecturers
$sudo usermod -a -G lecturers tuanthai
```



- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
$sudo chown :lecturers /data
$sudo chmod -R 775 /data
```



```
[b2012081@localhost ~]$ sudo chown :lecturers data
[b2012081@localhost ~]$ sudo chmod -R 775 data
[b2012081@localhost ~]$ ls -l
total 92
-rwxr-xr-x. 1 root     root        349 Mar 27 08:10 backup.sh
drwxrwxr-x. 2 root     lecturers     6 Apr 22 14:35 data
```

- Cấu hình dịch vụ Samba:

```
$sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
$sudo nano /etc/samba/smb.conf
#Thêm đoạn cấu hình bên dưới vào cuối tập tin

[data]
     comment = Shared folder for lecturers
     path = /data
     browsable = yes
     writable = yes
     read only = no
     valid users = @lecturers
```

```
[b2012081@localhost ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[b2012081@localhost ~]$ sudo nano /etc/samba/smb.conf
```

```
[data]
        comment = Shared folder for lecturers
        path = /data
        browsable = yes
        writable = yes
        read only = no
        valid users = @lecturers
```

- Thêm người dùng cho dịch vụ Samba:

```
$sudo smbpasswd -a tuanthai
#Đặt mật khẩu Samba cho người dùng
```

```
[b2012081@localhost ~]$ sudo smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
```

```
Người dùng tuanthai trong dịch vụ samba
(passwd: 321)
```

- Cấu hình SELINUX cho phép Samba

```
$sudo setsebool -P samba_export_all_rw on
$sudo setsebool -P samba_enable_home_dirs on
```

```
[b2012081@localhost ~]$ sudo setsebool -P samba_export_all_rw on
[b2012081@localhost ~]$ sudo setsebool -P samba_enable_home_dirs on
```

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

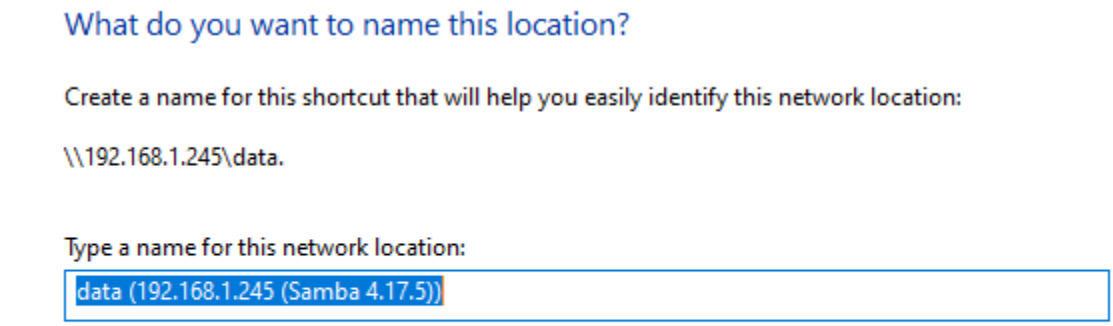
```
[b2012081@localhost ~]$ sudo systemctl stop firewalld
[b2012081@localhost ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: inactive (dead) since Sat 2023-04-22 14:50:25 +07; 11s ago
```

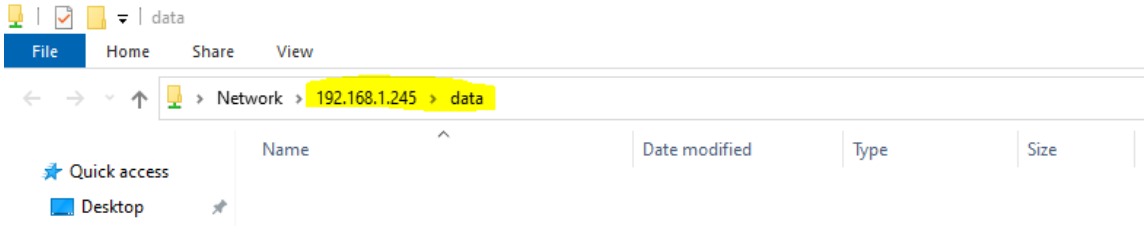
- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

```
$sudo systemctl start smb
$sudo systemctl enable smb
```

```
[b2012081@localhost ~]$ sudo systemctl start smb
[b2012081@localhost ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/
smb.service.
```

- Trên File Explorer của máy Windows, chọn tính năng “Add a network location” để nối kết tới Samba server sử dụng địa chỉ `\\<IP máy CentOS>\data`





3. Cài đặt và cấu hình dịch vụ DNS

DNS (Domain Name System) là giải pháp dùng tên miền thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Truy cập đến website của Trường CNTT-TT- Trường ĐH Cần Thơ bằng địa chỉ nào dễ nhớ hơn ?

http://123.30.143.202 hay http://www.cit.ctu.edu.vn

Trong bài thực hành này sinh viên cần cài đặt phần mềm BIND trên CentOS để phân giải tên miền “`qtht.com.vn`”

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

3.1. Cài đặt BIND và các công cụ cần thiết:

```
$sudo dnf install bind bind-utils -y
```

```
[b2012081@localhost ~]$ sudo dnf install bind bind-utils -y
[sudo] password for b2012081:
Last metadata expiration check: 1:26:05 ago on Sat 22 Apr 2023 01:37:11 PM +07.
Package bind-utils-32:9.16.23-11.el9.x86_64 is already installed.
Dependencies resolved.
```

```
Installed:
  bind-32:9.16.23-11.el9.x86_64
  bind-dnssec-utils-32:9.16.23-11.el9.x86_64
  python3-ply-3.11-14.el9.noarch

Complete!
```

3.2. Cấu hình DNS server:

```
$sudo nano /etc/named.conf
#(tham khảo file mẫu)
...
options {
      listen-on port 53 { 127.0.0.1; any;};
      ...
      allow-query     { localhost; any; };
      recursion yes;
      forwarders {192.168.55.1; };
      ..
};

logging {
        ..
        };
};

zone "." IN {
      ...
};

zone "qtht.com.vn" IN {
      type master;
      file "forward.qtht";
      allow-update { none; };
};

zone "55.168.192.in-addr.arpa" IN {
      type master;
      file "reverse.qtht";
      allow-update { none; };
};
...
```

```
[b2012081@localhost ~]$ sudo nano /etc/named.conf
```

```
[b2012081@localhost ~]$ nmcli -f ipv4.dns con show enp0s3
ipv4.dns:                               203.113.188.1,203.113.131.3
```

```
recursion yes;
forwarders {203.113.188.1;}
```

```
listen-on port 53 { 127.0.0.1; any;};
```

```
allow-query     { localhost; any;};
```

```
zone "qtht.com.vn" IN {
        type master;
        file "forward.qtht";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "reverse.qtht";
        allow-update { none; };
};
```

3.3. Tạo tập tin cấu hình phân giải xuôi:

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

#(tham khảo file mẫu)

```
$TTL 1D
@    IN  SOA @ qtht.com.vn. (
                    0     ;Serial
                    1D    ;Refresh
                    1H    ;Retry
                    1W    ;Expire
                    3H    ;Minimum TTL
)
@       IN    NS    dns.qtht.com.vn.
dns     IN    A     192.168.55.250
www     IN    A     192.168.55.250
htql    IN    A     8.8.8.8
```

ban đầu

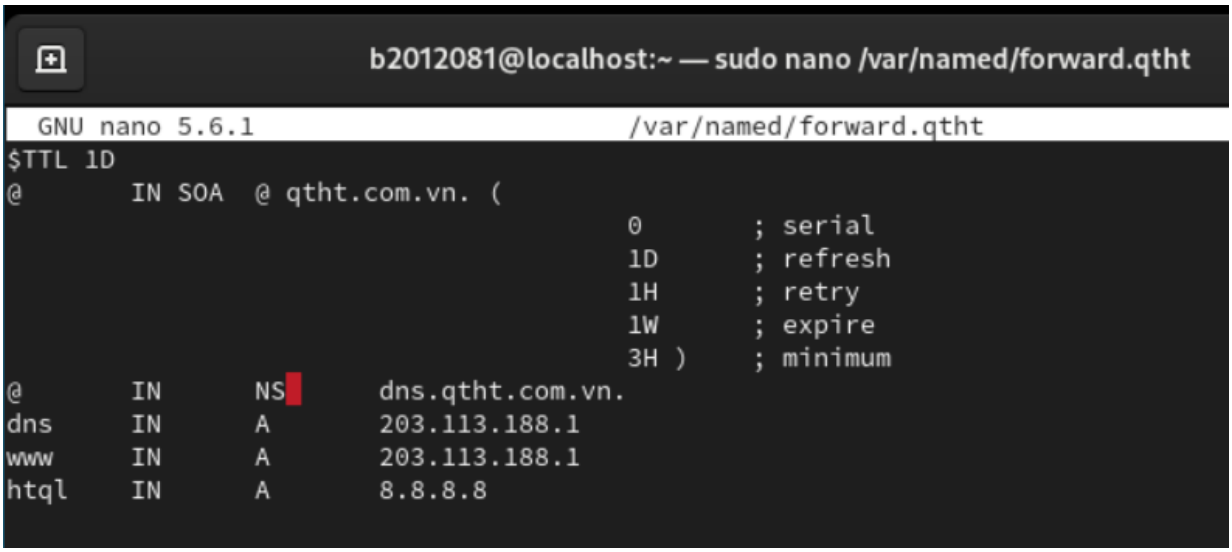
```
[b2012081@localhost ~]$ sudo ls -l /var/named/
[sudo] password for b2012081:
total 16
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named  168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
```

sau đó

```
[b2012081@localhost ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[b2012081@localhost ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  root   152 Apr 22 15:24 forward.qtht
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named  168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
```

Tiến hành đổi tên nhóm chủ sở hữu thành nhóm named

```
[b2012081@localhost ~]$ sudo chgrp named /var/named/forward.qtht
[b2012081@localhost ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Feb 27 21:25 data
drwxrwx---. 2 named named    6 Feb 27 21:25 dynamic
-rw-r-----. 1 root  named  152 Apr 22 15:24 forward.qtht
-rw-r-----. 1 root  named 2253 Feb 27 21:25 named.ca
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.empty
-rw-r-----. 1 root  named  152 Feb 27 21:25 named.localhost
-rw-r-----. 1 root  named  168 Feb 27 21:25 named.loopback
drwxrwx---. 2 named named    6 Feb 27 21:25 slaves
```



3.4. Tạo tập tin cấu hình phân giải ngược:

```
$sudo cp /var/named/forward.qtht /var/named/reverse.qtht
$sudo chgrp named /var/named/reverse.qtht
$sudo nano /var/named/reverse.qtht

$TTL 1D
@    IN  SOA @ qtht.com.vn. (
                    0     ;Serial
                    1D    ;Refresh
                    1H    ;Retry
                    1W    ;Expire
                    3H    ;Minimum TTL
)
@     IN    NS    dns.qtht.com.vn.
dns   IN    A     192.168.55.250
250   IN    PTR   www.qtht.com.vn.
```

```
[b2012081@localhost ~]$ sudo cp /var/named/named.localhost /var/named/reverse.qtht
[sudo] password for b2012081:
[b2012081@localhost ~]$ sudo chgrp named /var/named/reverse.qtht
[b2012081@localhost ~]$ sudo nano /var/named/reverse.qtht
```

```
b2012081@localhost:~ — sudo nano /var/named/reverse.qtht
 GNU nano 5.6.1                          /var/named/reverse.qtht
$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      dns.qtht.com.vn.
dns     IN      A       203.113.188.1
1       IN      PTR     www.qtht.com.vn.
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:
  `$sudo systemctl stop firewalld`
- Khởi động dịch vụ DNS:
  `$sudo systemctl start named`

```
[b2012081@localhost ~]$ sudo systemctl start named
[b2012081@localhost ~]$ sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
     Active: active (running) since Sat 2023-04-22 15:49:35 +07; 9s ago
```

- Kiểm tra kết quả:
  `nslookup www.qtht.com.vn <địa chỉ IP máy ảo>`

```
[b2012081@localhost ~]$ nslookup www.qtht.com.vn 192.168.1.245
Server:         192.168.1.245
Address:        192.168.1.245#53

Name:   www.qtht.com.vn
Address: 203.113.188.1
```

`nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>`

```
[b2012081@localhost ~]$ nslookup htql.qtht.com.vn 192.168.1.245
Server:         192.168.1.245
Address:        192.168.1.245#53

Name:   htql.qtht.com.vn
Address: 8.8.8.8
```

`nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>`

```
[b2012081@localhost ~]$ nslookup www.ctu.edu.vn 192.168.1.245
Server:         192.168.1.245
Address:        192.168.1.245#53

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

- Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ http://www.qtht.com.vn/myweb

4. Cấu hình tường lửa Firewalld

Công cụ Firewalld (dynamic firewall daemon) cung cấp dịch vụ tường lửa mạnh mẽ, toàn diện; được cài đặt mặc định cho nhiều bản phân phối Linux. Từ CentOS 7 trở về sau, tường lửa Firewalld được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- Firewalld sử dụng "zone" như là một nhóm các quy tắc (rule) áp đặt lên những luồng dữ liệu. Một số zone có sẵn thường dùng:
  - *drop*: ít tin cậy nhất – toàn bộ các kết nối đến sẽ bị từ chối.
  - *public*: đại diện cho mạng công cộng, không đáng tin cậy. Các máy tính/services khác không được tin tưởng trong hệ thống nhưng vẫn cho phép các kết nối đến tùy từng trường hợp cụ thể.
  - *trusted*: đáng tin cậy nhất – tin tưởng toàn bộ thiết bị trong hệ thống.
- Firewalld quản lý các quy tắc được thiết lập tự động, có tác dụng ngay lập tức mà không làm mất đi các kết nối và session hiện có.
  - *Runtime* (mặc định): có tác dụng ngay lập tức nhưng mất hiệu lực khi reboot hệ thống.
  - *Permanent*: không áp dụng cho hệ thống đang chạy, cần reload mới có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

- Khởi động tường lửa firewalld

  `$sudo systemctl start firewalld`

```
[b2012081@localhost ~]$ sudo systemctl start firewalld
[sudo] password for b2012081:
[b2012081@localhost ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Sat 2023-04-22 15:58:55 +07; 13s ago
```

- Liệt kê tất cả các zone đang có trong hệ thống
  `$firewall-cmd --get-zones`

```
[b2012081@localhost ~]$ firewall-cmd --get-zones
block dmz docker drop external home internal nm-shared public trusted work
```

- Kiểm tra zone mặc định
  `$firewall-cmd --get-default-zone`

```
[b2012081@localhost ~]$ firewall-cmd --get-default-zone
public
```

- Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *public*); và xem các rules của zone
  `$firewall-cmd --get-active-zones`

```
[b2012081@localhost ~]$ firewall-cmd --get-active-zones
docker
  interfaces: docker0
public
  interfaces: enp0s3
```

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

```
[b2012081@localhost ~]$ firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

```
C:\Users\Thanh Em>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

```
[b2012081@localhost ~]$ sudo systemctl start httpd
[b2012081@localhost ~]$ sudo systemctl status  httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2023-04-22 14:06:45 +07; 2h 6min ago
```

This site can't be reached

192.168.1.245 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

- Chuyển giao diện mạng sang zone *drop*; và xem các rules của zone

```
$sudo firewall-cmd --zone=drop --change-interface=enp0s3
$sudo firewall-cmd --list-all --zone=drop
```

```
[b2012081@localhost ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
success
```

```
[b2012081@localhost ~]$ sudo firewall-cmd --list-all --zone=drop
drop (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

```
C:\Users\Thanh Em>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Chuyển giao diện mạng sang zone *trusted*; và xem các rules của zone

```
$sudo firewall-cmd --zone=trusted --change-interface=enp0s3
$sudo firewall-cmd --list-all --zone=trusted
```

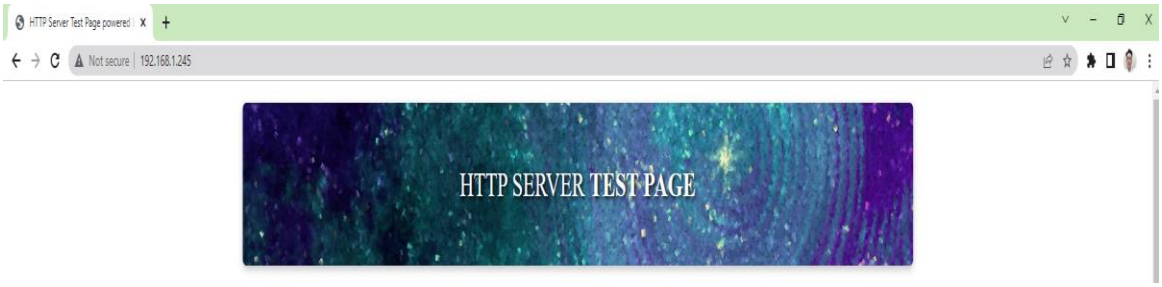
```
[b2012081@localhost ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[b2012081@localhost ~]$ sudo firewall-cmd --list-all --zone=trusted
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

```
C:\Users\Thanh Em>ping 192.168.1.245

Pinging 192.168.1.245 with 32 bytes of data:
Reply from 192.168.1.245: bytes=32 time=2ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time<1ms TTL=64
Reply from 192.168.1.245: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.245:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```



- Tạo zone mới có tên là *qthtserver*

```
$sudo firewall-cmd --permanent --new-zone=qthtserver
$sudo systemctl restart firewalld
$sudo firewall-cmd --list-all --zone=qthtserver
```

```
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[b2012081@localhost ~]$ sudo systemctl restart firewalld
[b2012081@localhost ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Cho phép các dịch vụ HTTP, DNS, SAMBA, FTP và cổng 9999/tcp hoạt động trên zone *qthtserver*

```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
$sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
```

-

```
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
```

- Thêm rule để chỉ cho phép máy vật lý có thể SSH tới máy CentOS
  $sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=<IP máy vật lý>/32 port port=22 protocol=tcp accept'

```
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule fami
ly=ipv4 source address=192.168.56.1/32 port port=22 protocol=tcp accept'
[sudo] password for b2012081:
success
```

- Khởi động lại tường lửa firewalld
  `$sudo systemctl restart firewalld`

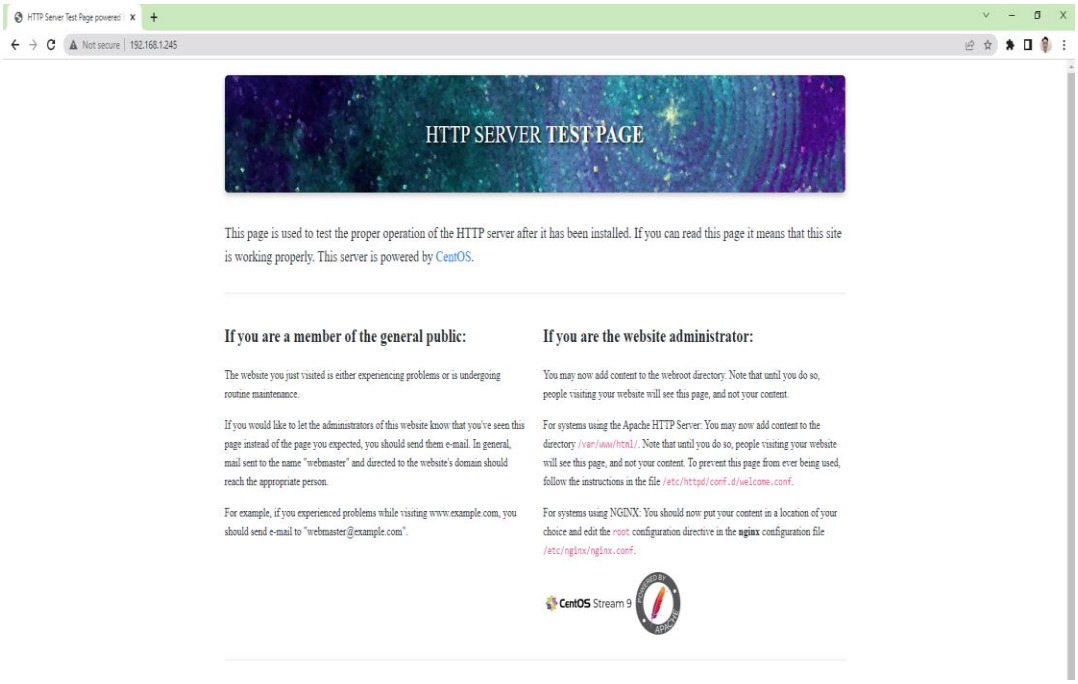
```
[b2012081@localhost ~]$ sudo systemctl restart firewalld
[b2012081@localhost ~]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Sat 2023-04-22 16:39:17 +07; 15s ago
```

- Chuyển giao diện mạng sang zone `qthtserver`; và xem các rules của zone
  `$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3`
  `$sudo firewall-cmd --list-all --zone=qthtserver`

```
[b2012081@localhost ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
```

```
[b2012081@localhost ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dns ftp http samba
  ports: 9999/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="192.168.56.1/32" port port="22" protocol="tcp" accept
```

- Kiểm tra máy vật lý có thể truy cập được tới các dịch vụ trên máy CentOS hay không.



--- Hết ---