



LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Phạm Minh Sáng

Nhóm học phần: 06

- 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. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
- Video hướng dẫn ở cuối bài.

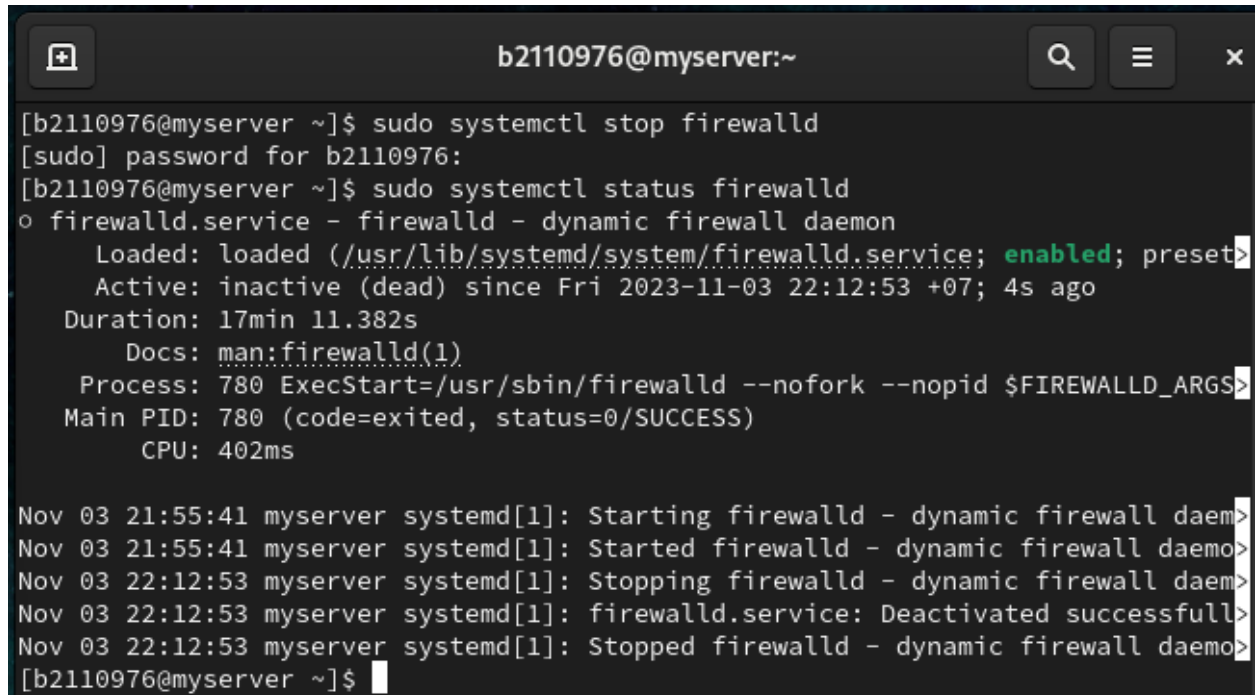
1. Triển khai dịch vụ WEB sử dụng Docker

- 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)

```
b2110976@myserver:~  
[b2110976@myserver ~]$ mkdir myweb  
[b2110976@myserver ~]$ cp index.html myweb  
[b2110976@myserver ~]$ car ./myweb/index.html  
bash: car: command not found...  
[b2110976@myserver ~]$ 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>  
[b2110976@myserver ~]$
```

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

A terminal window titled 'b2110976@myserver:~' with search, menu, and close buttons. The terminal shows the execution of 'sudo systemctl stop firewalld', followed by 'sudo systemctl status firewalld'. The status output shows the service is 'enabled' but 'inactive (dead)'. Below this, a series of log messages from systemd show the service being started and then successfully stopped. The prompt returns to the user.

```
[b2110976@myserver ~]$ sudo systemctl stop firewalld
[sudo] password for b2110976:
[b2110976@myserver ~]$ sudo systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
   Active: inactive (dead) since Fri 2023-11-03 22:12:53 +07; 4s ago
   Duration: 17min 11.382s
   Docs: man:firewalld(1)
   Process: 780 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS>
   Main PID: 780 (code=exited, status=0/SUCCESS)
   CPU: 402ms

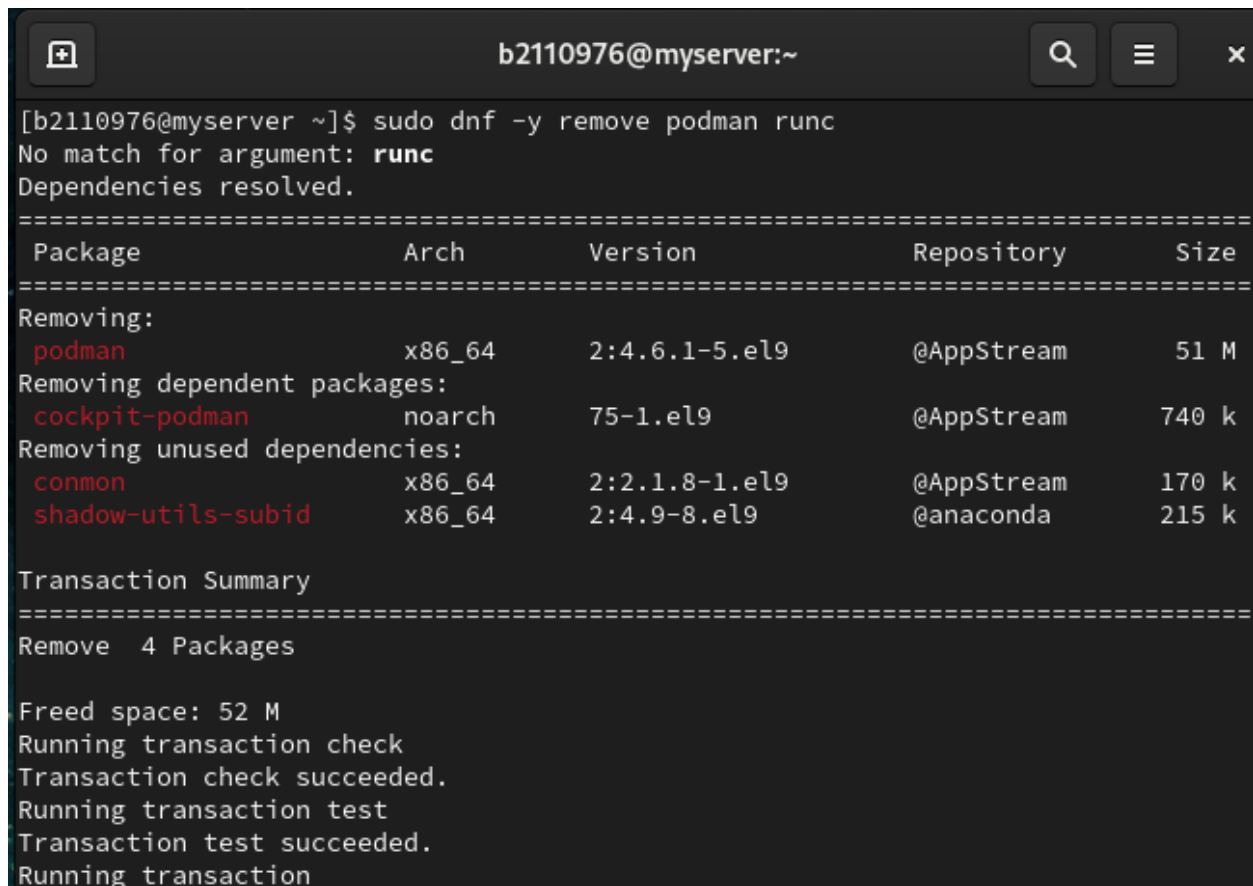
Nov 03 21:55:41 myserver systemd[1]: Starting firewalld - dynamic firewall daem>
Nov 03 21:55:41 myserver systemd[1]: Started firewalld - dynamic firewall daemo>
Nov 03 22:12:53 myserver systemd[1]: Stopping firewalld - dynamic firewall daem>
Nov 03 22:12:53 myserver systemd[1]: firewalld.service: Deactivated successfull>
Nov 03 22:12:53 myserver systemd[1]: Stopped firewalld - dynamic firewall daemo>
[b2110976@myserver ~]$
```

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
```



```
[b2110976@myserver ~]$ sudo dnf -y remove podman runc
No match for argument: runc
Dependencies resolved.
=====
Package                Arch      Version      Repository    Size
=====
Removing:
podman                 x86_64     2:4.6.1-5.el9    @AppStream    51 M
Removing dependent packages:
cockpit-podman         noarch     75-1.el9         @AppStream    740 k
Removing unused dependencies:
common                x86_64     2:2.1.8-1.el9    @AppStream    170 k
shadow-utils-subid    x86_64     2:4.9-8.el9      @anaconda     215 k

Transaction Summary
=====
Remove  4 Packages

Freed space: 52 M
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
```

- Cài đặt công cụ yum-utils

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

```
b2110976@myserver:~  
[b2110976@myserver ~]$ sudo dnf install -y yum-utils  
Last metadata expiration check: 0:40:58 ago on Fri 03 Nov 2023 09:33:51 PM +07.  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
yum-utils	noarch	4.3.0-11.el9	baseos	37 k
Upgrading:				
dnf-plugins-core	noarch	4.3.0-11.el9	baseos	38 k
python3-dnf-plugins-core	noarch	4.3.0-11.el9	baseos	247 k

```
Transaction Summary  
=====
```

Install	1 Package
Upgrade	2 Packages

```
Total download size: 322 k  
Downloading Packages:  
(1/3): dnf-plugins-core-4.3.0-11.el9.noarch.rpm 31 kB/s | 38 kB 00:01  
(2/3): yum-utils-4.3.0-11.el9.noarch.rpm 30 kB/s | 37 kB 00:01  
(3/3): python3-dnf-plugins-core-4.3.0-11.el9.no 142 kB/s | 247 kB 00:01  
-----  
Total 78 kB/s | 322 kB 00:04
```

- 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.

```
b2110976@myserver:~  
[b2110976@myserver ~]$ sudo yum-config-manager \  
> --add-repo \  
> https://download.docker.com/linux/centos/docker-ce.repo  
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo  
[b2110976@myserver ~]$
```

- Cài đặt Docker

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

```
b2110976@myserver:~ — sudo dnf install docker-ce -y
[b2110976@myserver ~]$ sudo dnf install docker-ce -y
Docker CE Stable - x86_64 11 kB/s | 32 kB 00:02
Dependencies resolved.
=====
Package Arch Version Repository Size
=====
Installing:
docker-ce x86_64 3:24.0.7-1.el9 docker-ce-stable 24 M
Installing dependencies:
containerd.io x86_64 1.6.24-3.1.el9 docker-ce-stable 33 M
docker-ce-cli x86_64 1:24.0.7-1.el9 docker-ce-stable 7.1 M
Installing weak dependencies:
docker-buildx-plugin x86_64 0.11.2-1.el9 docker-ce-stable 13 M
docker-ce-rootless-extras x86_64 24.0.7-1.el9 docker-ce-stable 3.9 M
docker-compose-plugin x86_64 2.21.0-1.el9 docker-ce-stable 13 M
Transaction Summary
=====
Install 6 Packages

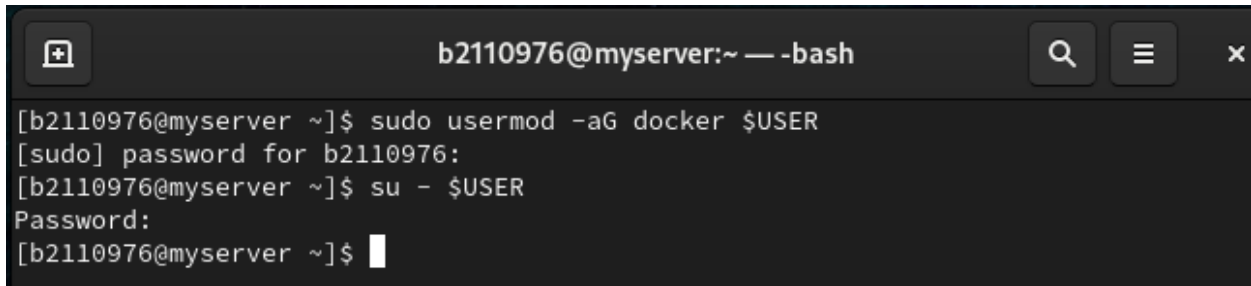
Total download size: 93 M
Installed size: 367 M
Downloading Packages:
(1/6): docker-buildx-plugin-0.11.2-1.el9.x86_64 102 kB/s | 13 MB 02:08
```

- 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
```

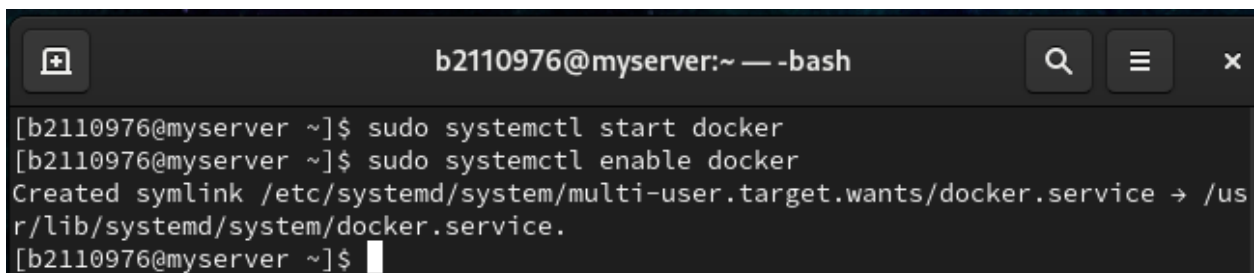
```
b2110976@myserver:~
[b2110976@myserver ~]$ sudo usermod -aG docker $USER
[sudo] password for b2110976:
[b2110976@myserver ~]$
```

- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng
`$su - $USER`



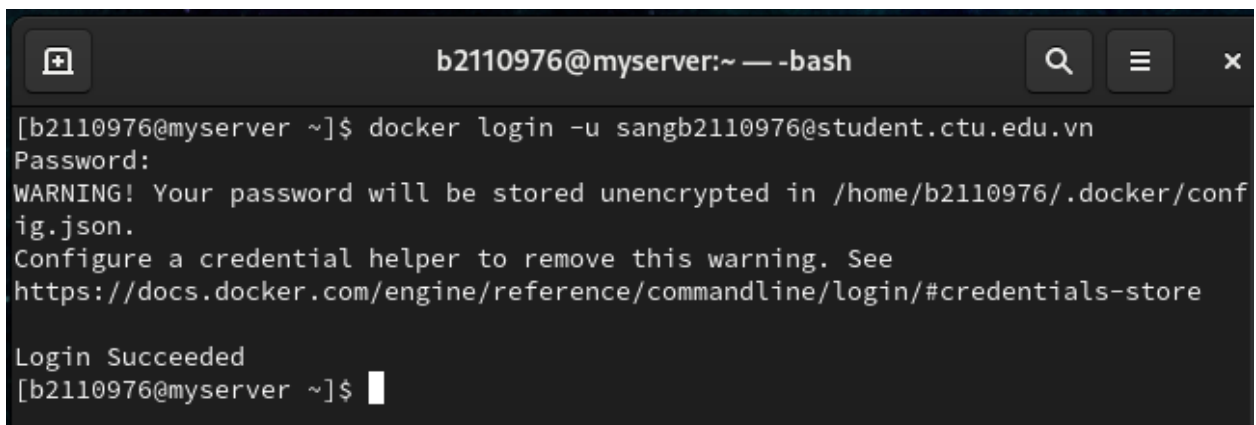
```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ sudo usermod -aG docker $USER
[sudo] password for b2110976:
[b2110976@myserver ~]$ su - $USER
Password:
[b2110976@myserver ~]$
```

- Chạy dịch vụ Docker
`$sudo systemctl start docker`
`$sudo systemctl enable docker`



```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ sudo systemctl start docker
[b2110976@myserver ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
[b2110976@myserver ~]$
```

- Tạo 1 tài khoản trên DockerHub (<https://hub.docker.com/>), sau đó đăng nhập sử dụng lệnh sau:
`$docker login -u <docker-username>`

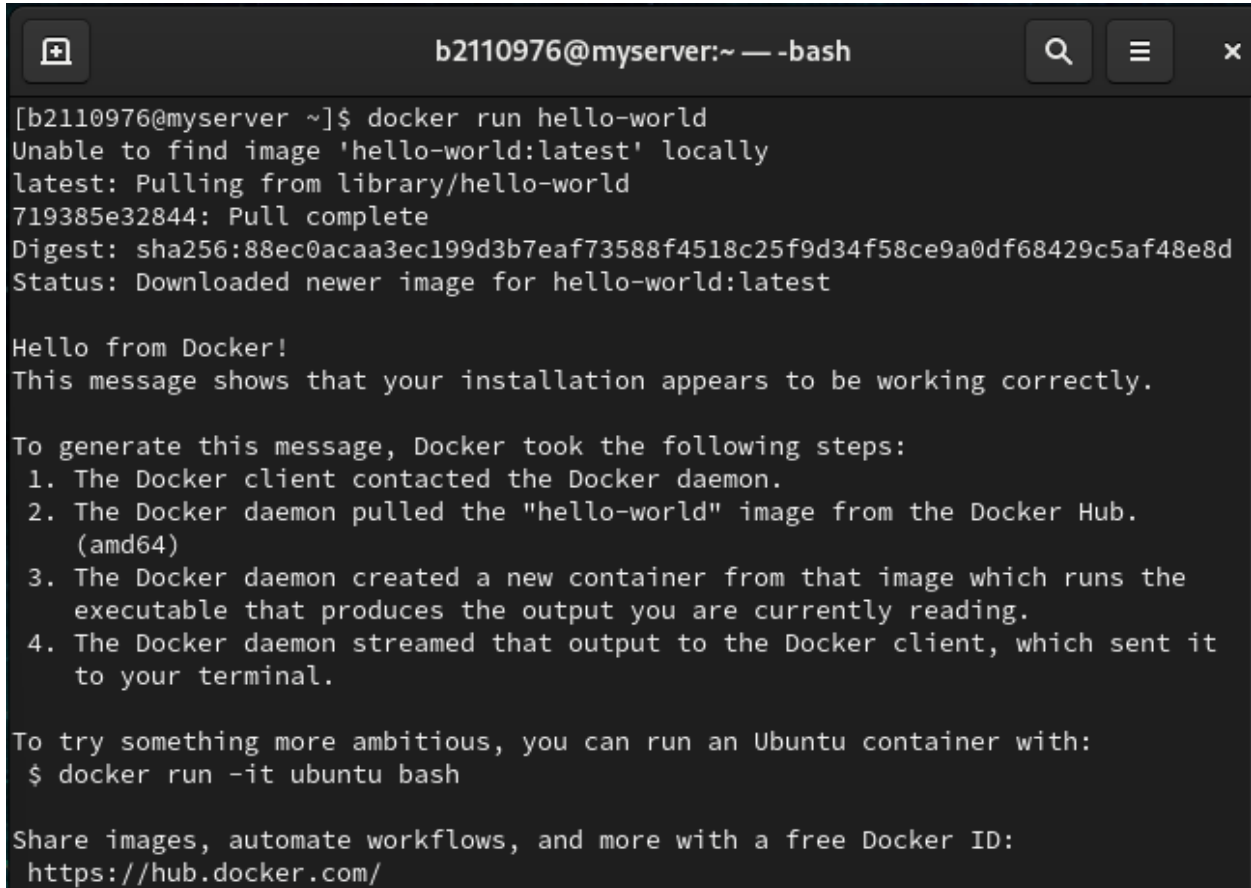


```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ docker login -u sangb2110976@student.ctu.edu.vn
Password:
WARNING! Your password will be stored unencrypted in /home/b2110976/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
[b2110976@myserver ~]$
```

- 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
```



```
b2110976@myserver:~ — -bash

[b2110976@myserver ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
719385e32844: Pull complete
Digest: sha256:88ec0acaa3ec199d3b7eaf73588f4518c25f9d34f58ce9a0df68429c5af48e8d
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

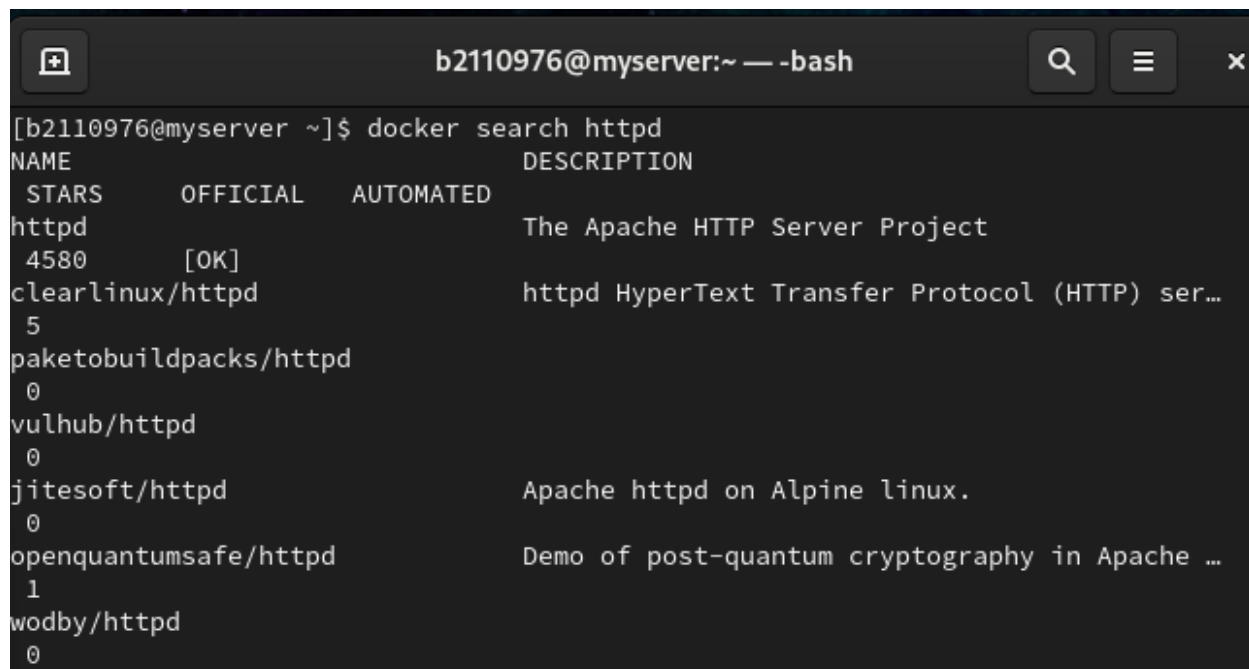
To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/
```

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
```



A terminal window titled 'b2110976@myserver:~ — -bash' showing the command 'docker search httpd' and its output. The output lists several Docker images with their names, star counts, official status, automated status, and descriptions. The first result is 'httpd' with 4580 stars, marked as official and automated, with the description 'The Apache HTTP Server Project'.

```
[b2110976@myserver ~]$ docker search httpd
```

NAME	STARS	OFFICIAL	AUTOMATED	DESCRIPTION
httpd	4580	[OK]		The Apache HTTP Server Project
clearlinux/httpd	5			httpd HyperText Transfer Protocol (HTTP) ser...
paketobuildpacks/httpd	0			
vulhub/httpd	0			
jitesoft/httpd	0			Apache httpd on Alpine linux.
openquantumsafe/httpd	1			Demo of post-quantum cryptography in Apache ...
wodby/httpd	0			

- Tạo container từ image httpd

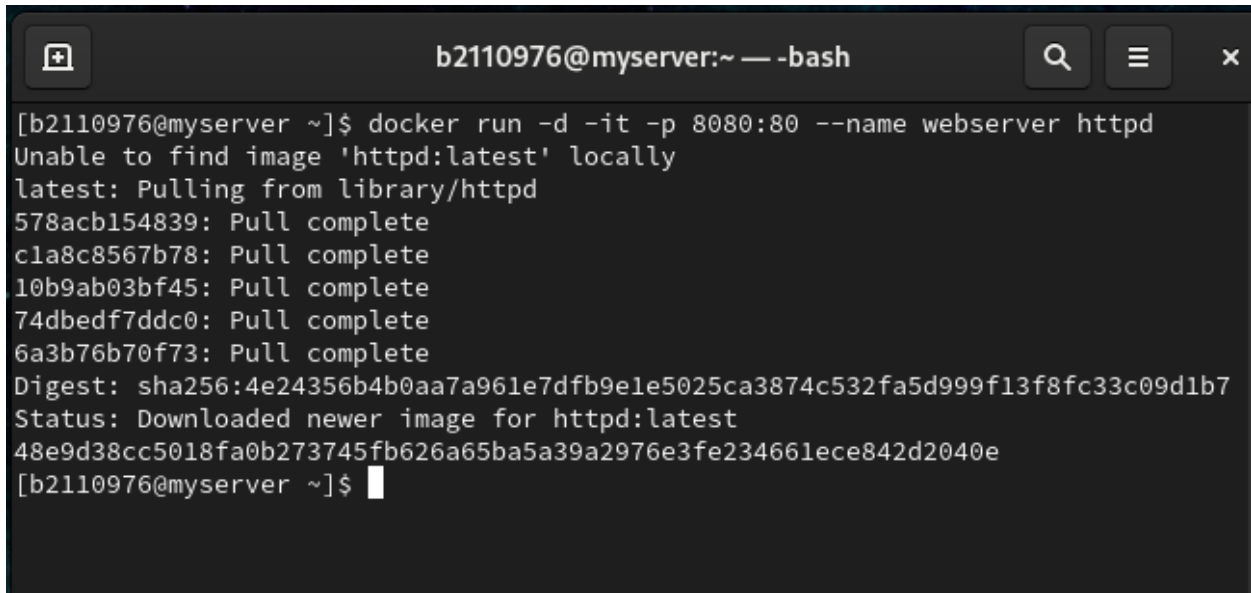
```
$docker run -d -it -p 8080:80 --name webserver httpd
```

-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

--name webserver: đặt tên container là webserver

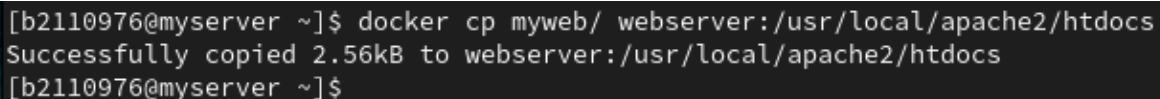
-p 8080:80 gán cổng 8080 của máy CentOS vào cổng 80 của container.



```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
578acb154839: Pull complete
c1a8c8567b78: Pull complete
10b9ab03bf45: Pull complete
74dbedf7ddc0: Pull complete
6a3b76b70f73: Pull complete
Digest: sha256:4e24356b4b0aa7a961e7dfb9e1e5025ca3874c532fa5d999f13f8fc33c09d1b7
Status: Downloaded newer image for httpd:latest
48e9d38cc5018fa0b273745fb626a65ba5a39a2976e3fe234661ece842d2040e
[b2110976@myserver ~]$
```

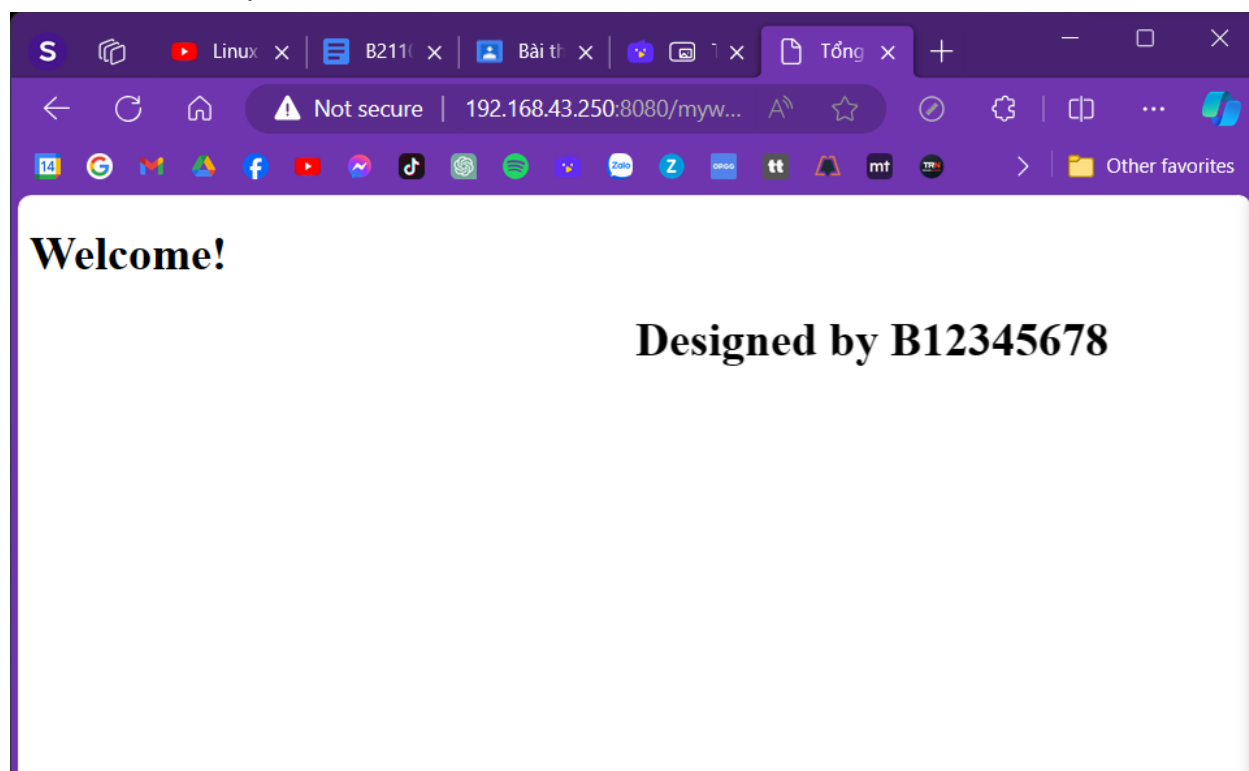
- Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.

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



```
[b2110976@myserver ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs
[b2110976@myserver ~]$
```

- 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.



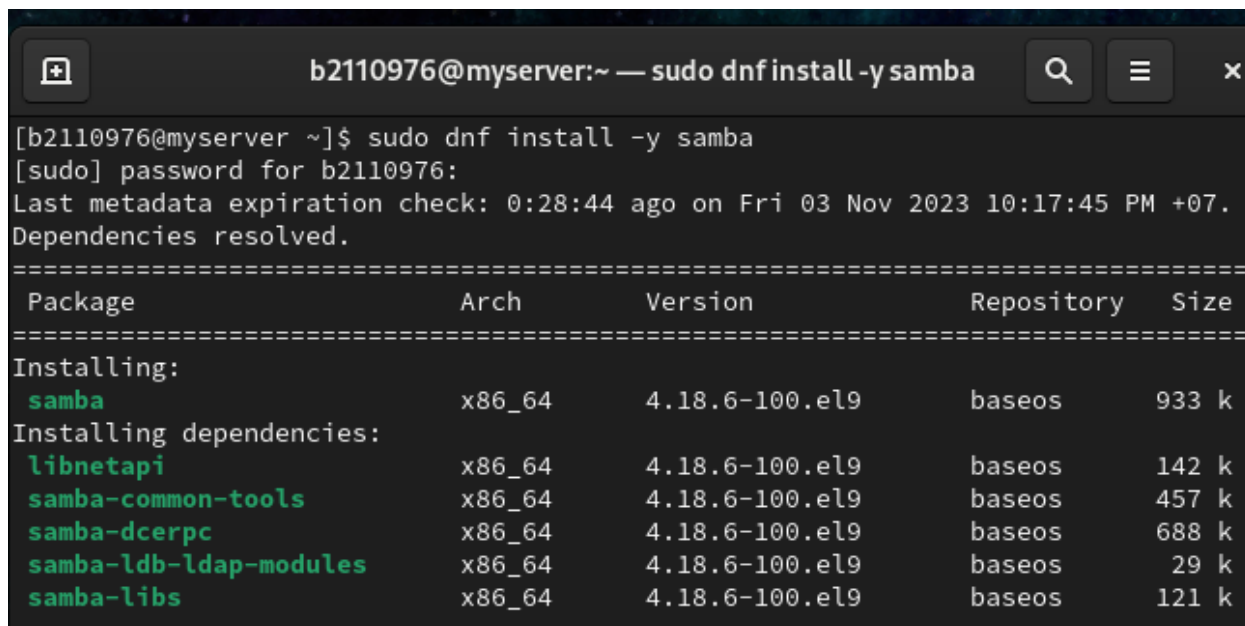
2. Cài đặt và cấu hình dịch vụ SAMBA

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
```

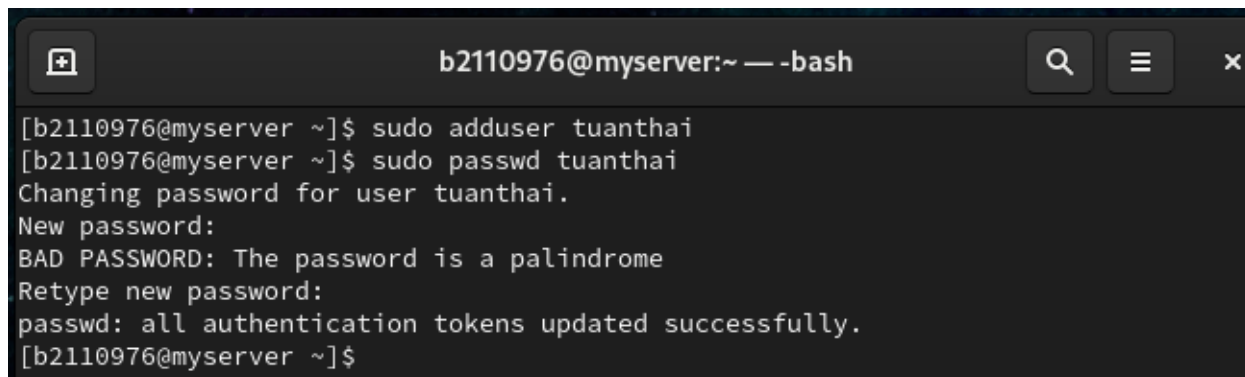


```
b2110976@myserver:~ — sudo dnf install -y samba
[b2110976@myserver ~]$ sudo dnf install -y samba
[sudo] password for b2110976:
Last metadata expiration check: 0:28:44 ago on Fri 03 Nov 2023 10:17:45 PM +07.
Dependencies resolved.
=====
Package                        Arch      Version      Repository    Size
=====
Installing:
samba                          x86_64     4.18.6-100.el9    baseos        933 k
Installing dependencies:
libnetapi                      x86_64     4.18.6-100.el9    baseos        142 k
samba-common-tools             x86_64     4.18.6-100.el9    baseos        457 k
samba-dcerpc                   x86_64     4.18.6-100.el9    baseos        688 k
samba-ldb-ldap-modules         x86_64     4.18.6-100.el9    baseos         29 k
samba-libs                     x86_64     4.18.6-100.el9    baseos        121 k
```

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

```
$sudo adduser tuanthai
```

```
$sudo passwd tuanthai
```



```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ sudo adduser tuanthai
[b2110976@myserver ~]$ sudo passwd tuanthai
Changing password for user tuanthai.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[b2110976@myserver ~]$
```

```
$sudo groupadd lecturers
```

```
$sudo usermod -a -G lecturers tuanthai
```

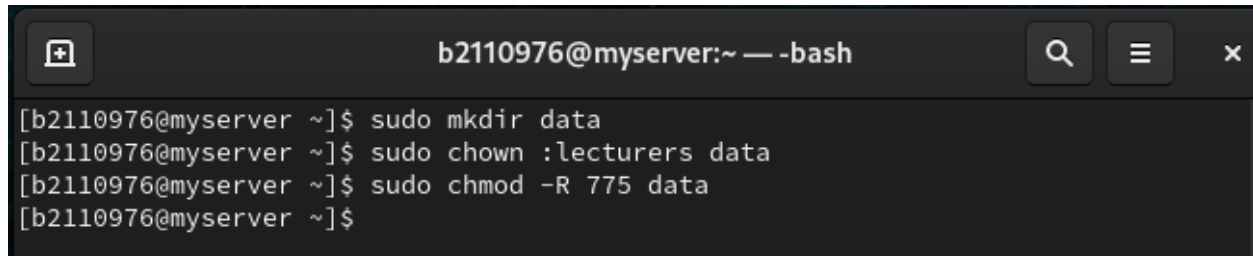
```
[b2110976@myserver ~]$ sudo groupadd lecturers
[b2110976@myserver ~]$ sudo usermod -aG lecturers tuanthai
[b2110976@myserver ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
```

```
$sudo chown :lecturers /data
```

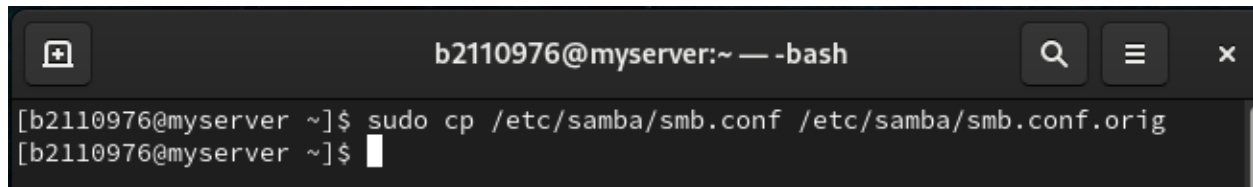
```
$sudo chmod -R 775 /data
```



```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ sudo mkdir data
[b2110976@myserver ~]$ sudo chown :lecturers data
[b2110976@myserver ~]$ sudo chmod -R 775 data
[b2110976@myserver ~]$
```

- Cấu hình dịch vụ Samba:

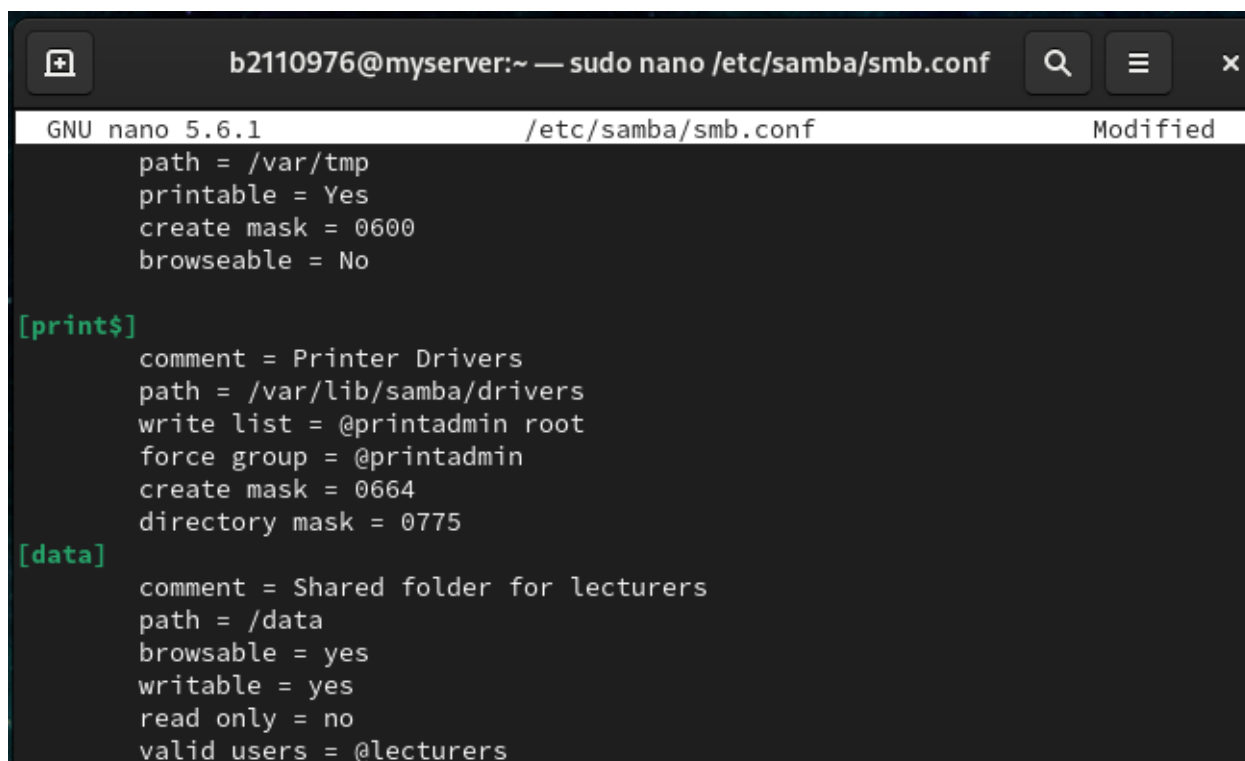
```
$sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```



```
b2110976@myserver:~ — -bash
[b2110976@myserver ~]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[b2110976@myserver ~]$
```

```
$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
```



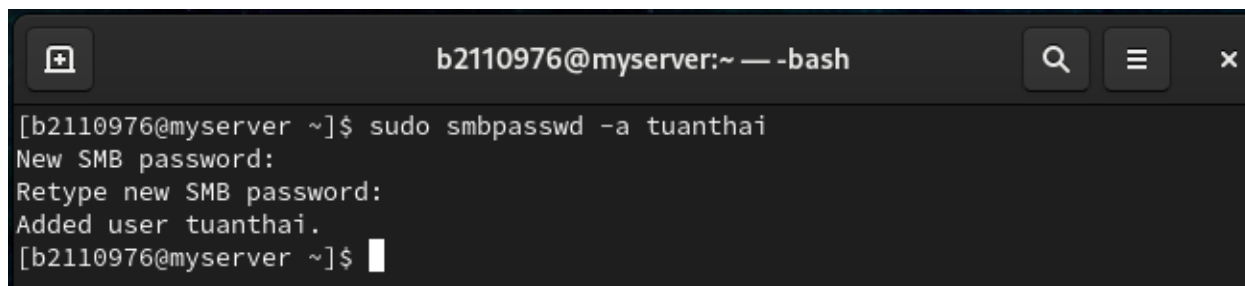
```
GNU nano 5.6.1 /etc/samba/smb.conf Modified
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @printadmin root
    force group = @printadmin
    create mask = 0664
    directory mask = 0775

[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
```

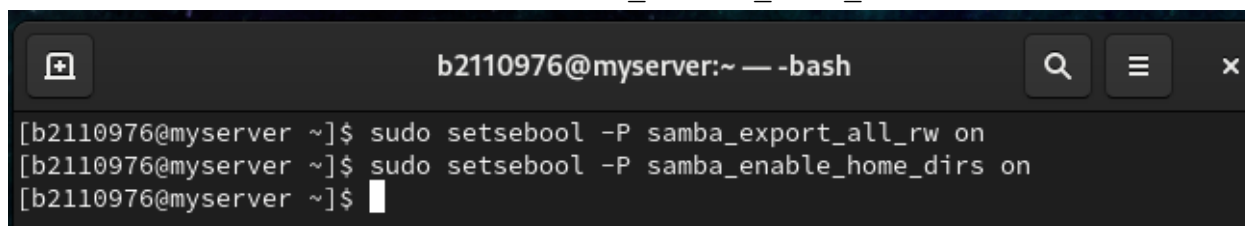


```
[b2110976@myserver ~]$ sudo smbpasswd -a tuanthai
New SMB password:
Retype new SMB password:
Added user tuanthai.
[b2110976@myserver ~]$
```

- Cấu hình SELINUX cho phép Samba

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

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

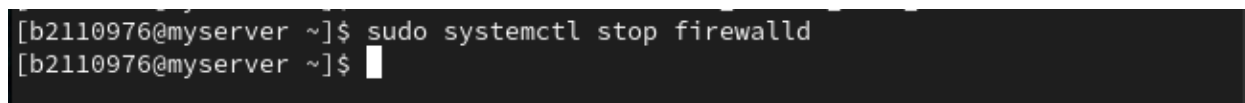


A terminal window titled 'b2110976@myserver:~ — -bash' showing the execution of two 'sudo setsebool' commands to configure SELinux for Samba. The first command sets 'samba_export_all_rw' to 'on', and the second sets 'samba_enable_home_dirs' to 'on'. The prompt returns to the user after each command.

```
[b2110976@myserver ~]$ sudo setsebool -P samba_export_all_rw on
[b2110976@myserver ~]$ sudo setsebool -P samba_enable_home_dirs on
[b2110976@myserver ~]$
```

- Tắt tường lửa:

```
$sudo systemctl stop firewalld
```



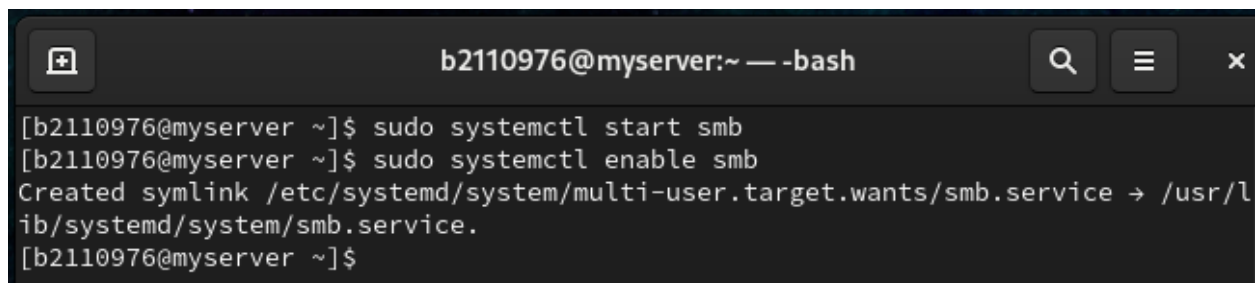
A terminal window titled 'b2110976@myserver:~ — -bash' showing the execution of 'sudo systemctl stop firewalld'. The command is entered and the prompt returns to the user.

```
[b2110976@myserver ~]$ sudo systemctl stop firewalld
[b2110976@myserver ~]$
```

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

```
$sudo systemctl start smb
```

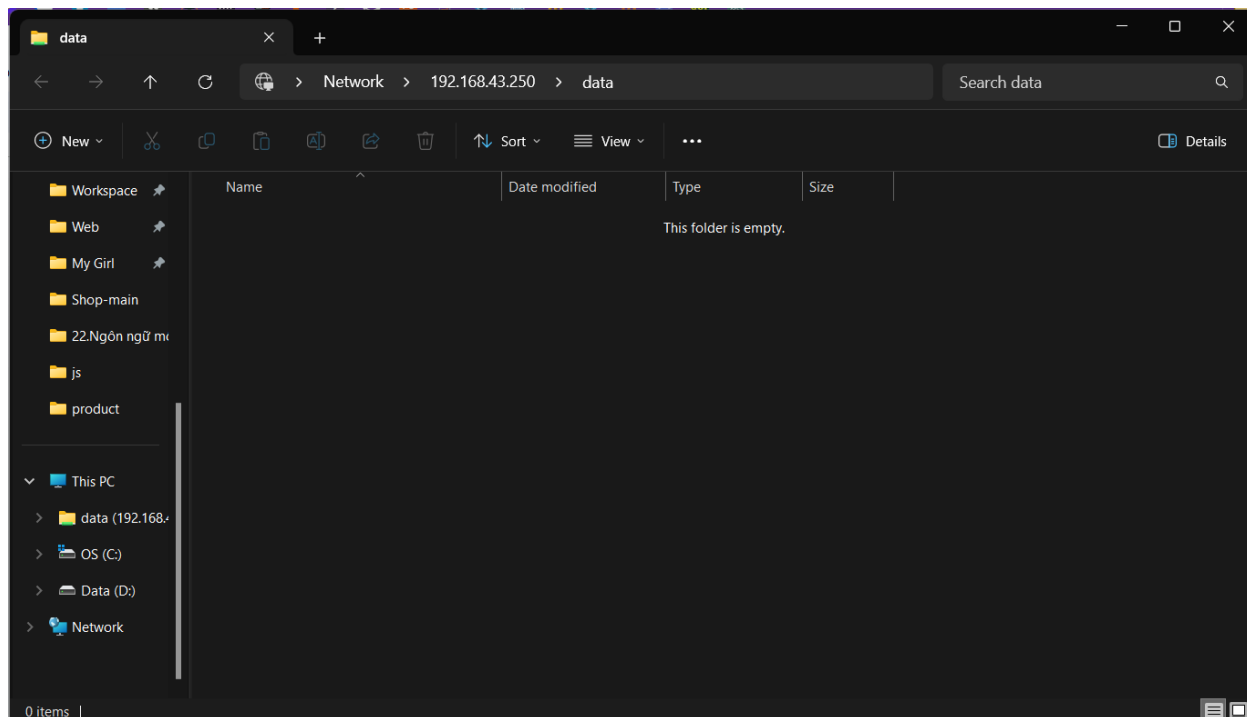
```
$sudo systemctl enable smb
```



A terminal window titled 'b2110976@myserver:~ — -bash' showing the execution of 'sudo systemctl start smb' and 'sudo systemctl enable smb'. The second command outputs a message indicating that a symlink was created to enable the service at boot. The prompt returns to the user after each command.

```
[b2110976@myserver ~]$ sudo systemctl start smb
[b2110976@myserver ~]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[b2110976@myserver ~]$
```

- 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 ?

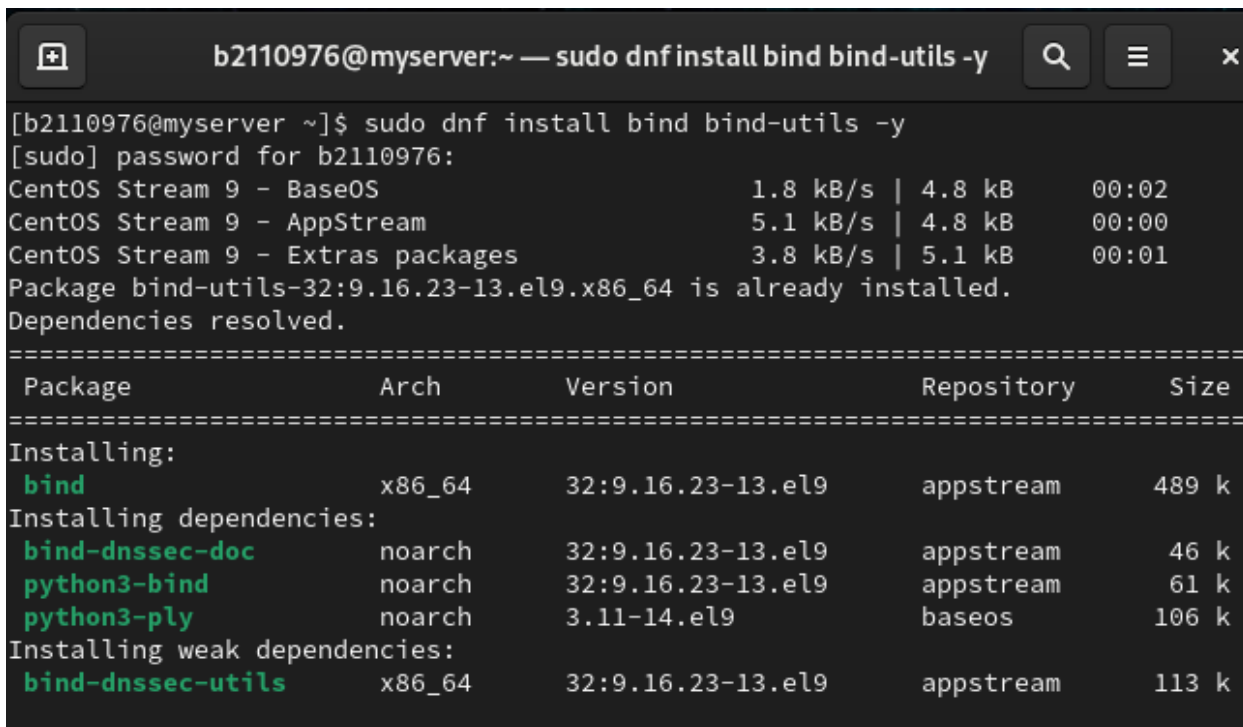
<http://123.30.143.202> hay <http://www.cit.ctu.edu.vn>

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
```



```
[b2110976@myserver ~]$ sudo dnf install bind bind-utils -y
[sudo] password for b2110976:
CentOS Stream 9 - BaseOS          1.8 kB/s | 4.8 kB      00:02
CentOS Stream 9 - AppStream       5.1 kB/s | 4.8 kB      00:00
CentOS Stream 9 - Extras packages 3.8 kB/s | 5.1 kB      00:01
Package bind-utils-32:9.16.23-13.el9.x86_64 is already installed.
Dependencies resolved.
=====
Package                Arch      Version              Repository           Size
=====
Installing:
bind                   x86_64    32:9.16.23-13.el9    appstream            489 k
Installing dependencies:
bind-dnssec-doc        noarch    32:9.16.23-13.el9    appstream            46 k
python3-bind           noarch    32:9.16.23-13.el9    appstream            61 k
python3-ply            noarch    3.11-14.el9          baseos               106 k
Installing weak dependencies:
bind-dnssec-utils      x86_64    32:9.16.23-13.el9    appstream            113 k
```


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; };
```

```
options {
listen-on port 53 { 127.0.0.1; any; };
listen-on-v6 port 53 { ::1; };
directory      "/var/named";
dump-file      "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
secroots-file  "/var/named/data/named.secroots";
recursing-file  "/var/named/data/named.recursing";
allow-query    { localhost; any; };
```

```
    recursion yes;
```

```
    forwarders {192.168.55.1; };
```

```
recursion yes;
forwarders {192.168.43.1; 1};
```

```
..
```

```
};
```

```
logging {
```

```
    ..
```

```
};
```

```
};
```

```
zone "." IN {
```

```
    ...
```

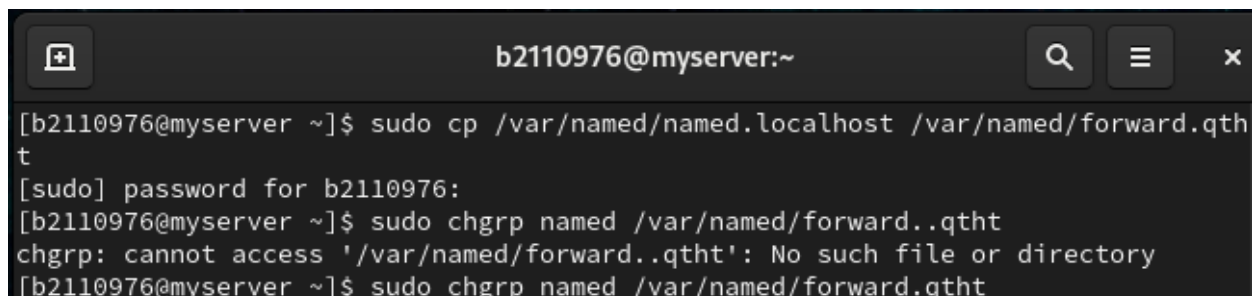
```
};
```

```
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; };  
};  
...
```

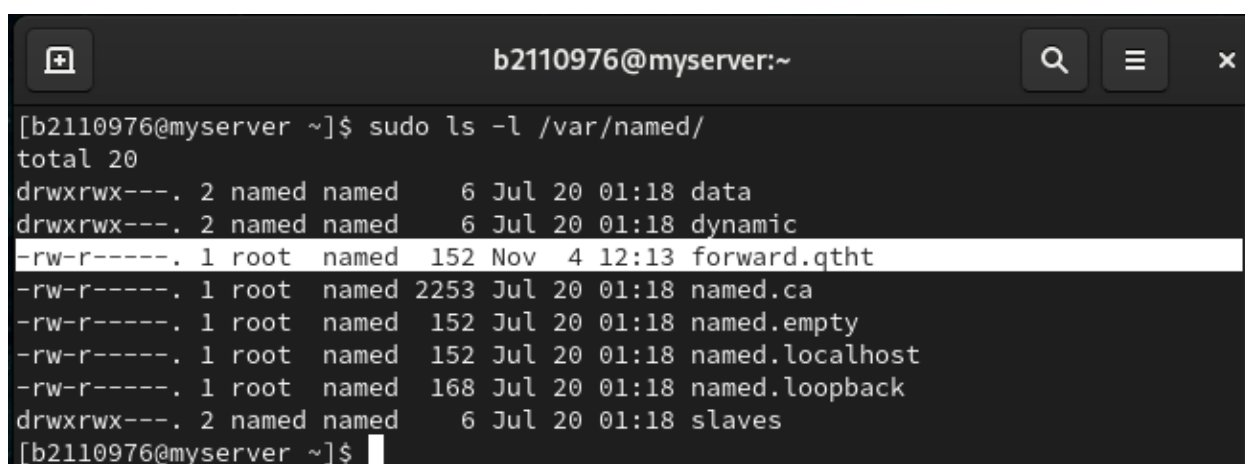
```
zone "qtht.com.vn" IN {  
    type master;  
    file "forward.qtht";  
    allow-update { none; };  
};  
zone "43.168.192.in-addr.arpa" IN {  
    type master;  
    file "reverse.qtht";  
    allow-update { none; };  
};
```

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
```



```
b2110976@myserver:~
[b2110976@myserver ~]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[sudo] password for b2110976:
[b2110976@myserver ~]$ sudo chgrp named /var/named/forward..qtht
chgrp: cannot access '/var/named/forward..qtht': No such file or directory
[b2110976@myserver ~]$ sudo chgrp named /var/named/forward.qtht
```



```
b2110976@myserver:~
[b2110976@myserver ~]$ sudo ls -l /var/named/
total 20
drwxrwx---. 2 named named    6 Jul 20 01:18 data
drwxrwx---. 2 named named    6 Jul 20 01:18 dynamic
-rw-r-----. 1 root  named  152 Nov  4 12:13 forward.qtht
-rw-r-----. 1 root  named 2253 Jul 20 01:18 named.ca
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.empty
-rw-r-----. 1 root  named  152 Jul 20 01:18 named.localhost
-rw-r-----. 1 root  named  168 Jul 20 01:18 named.loopback
drwxrwx---. 2 named named    6 Jul 20 01:18 slaves
[b2110976@myserver ~]$
```

```
$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
```



```
b2110976@myserver:~ — sudo nano /var/named/forward.qtht
GNU nano 5.6.1 /var/named/forward.qtht Modified
$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    192.168.43.250
www    IN      A    192.168.43.250
htql   IN      A    8.8.8.8
```

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
```

```
b2110976@myserver:~
[b2110976@myserver ~]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[sudo] password for b2110976:
[b2110976@myserver ~]$ sudo chgrp namedd /var/named/reverse.qtht
chgrp: invalid group: 'namedd'
[b2110976@myserver ~]$ sudo chgrp named /var/named/reverse.qtht
[b2110976@myserver ~]$
```

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

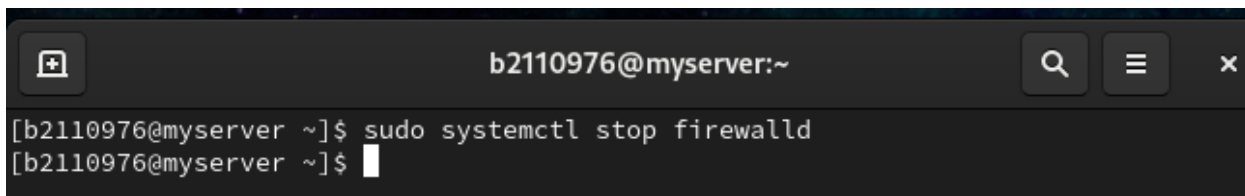
```
$TTL 1D
@      IN      SOA  @  qtht.com.vn. (
                                0      ;Serial
                                1D     ;Refresh
                                1H     ;Retry
                                1W     ;Expire
                                3H     ;Minimum TTL
)
@      IN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

```
b2110976@myserver:~ — sudo nano /var/named/reverse.qtht
GNU nano 5.6.1 /var/named/reverse.qtht Modified
$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    192.168.43.250
250    IN      PTR  www.qtht.com.vn.
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:

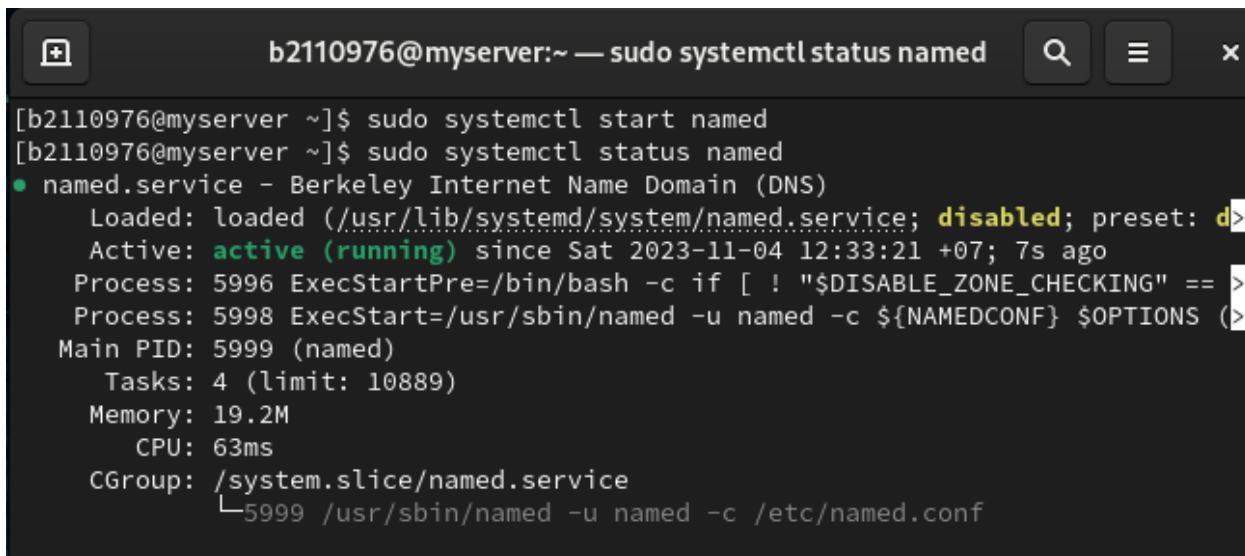
```
$sudo systemctl stop firewalld
```



```
b2110976@myserver:~  
[b2110976@myserver ~]$ sudo systemctl stop firewalld  
[b2110976@myserver ~]$
```

- Khởi động dịch vụ DNS:

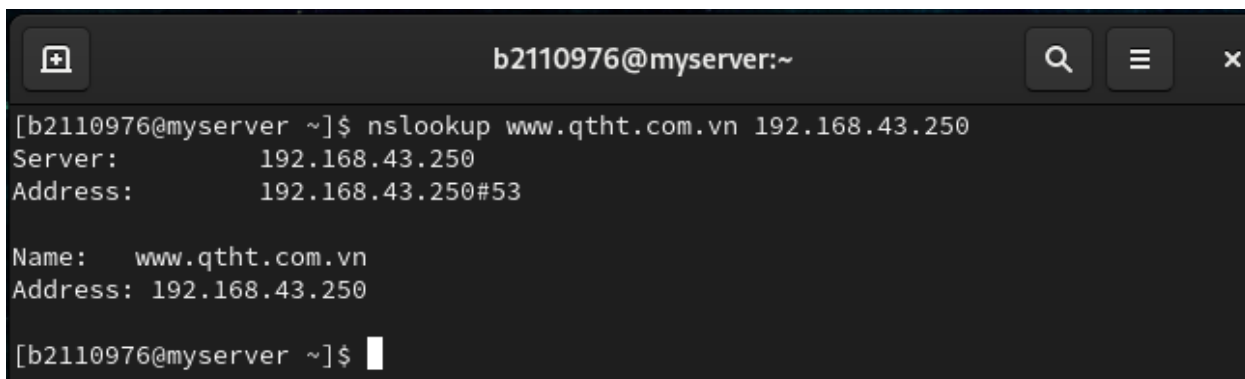
```
$sudo systemctl start named
```



```
b2110976@myserver:~ — sudo systemctl status named  
[b2110976@myserver ~]$ sudo systemctl start named  
[b2110976@myserver ~]$ sudo systemctl status named  
● named.service - Berkeley Internet Name Domain (DNS)  
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: d>  
   Active: active (running) since Sat 2023-11-04 12:33:21 +07; 7s ago  
     Process: 5996 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == >  
     Process: 5998 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (>  
    Main PID: 5999 (named)  
       Tasks: 4 (limit: 10889)  
      Memory: 19.2M  
         CPU: 63ms  
     CGroup: /system.slice/named.service  
             └─5999 /usr/sbin/named -u named -c /etc/named.conf
```

- Kiểm tra kết quả:

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



```
b2110976@myserver:~  
[b2110976@myserver ~]$ nslookup www.qtht.com.vn 192.168.43.250  
Server:      192.168.43.250  
Address:     192.168.43.250#53  
  
Name:   www.qtht.com.vn  
Address: 192.168.43.250  
  
[b2110976@myserver ~]$
```

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

```
[b2110976@myserver ~]$ nslookup htql.qtht.com.vn 192.168.43.250
Server:      192.168.43.250
Address:     192.168.43.250#53

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

[b2110976@myserver ~]$
```

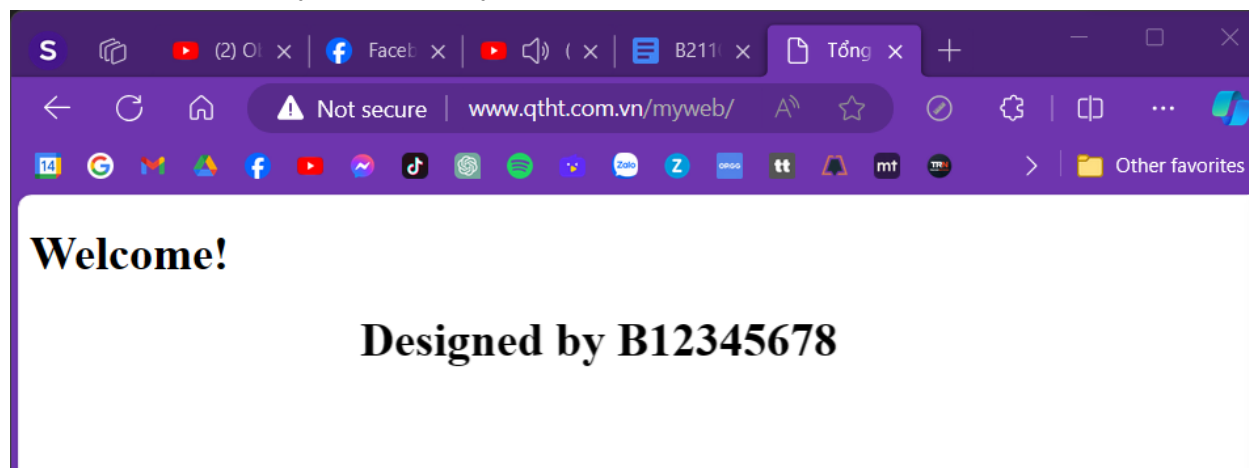
```
nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>
```

```
[b2110976@myserver ~]$ nslookup www.ctu.edu.vn 192.168.43.250
Server:      192.168.43.250
Address:     192.168.43.250#53

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

[b2110976@myserver ~]$
```

- 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 Firewallld

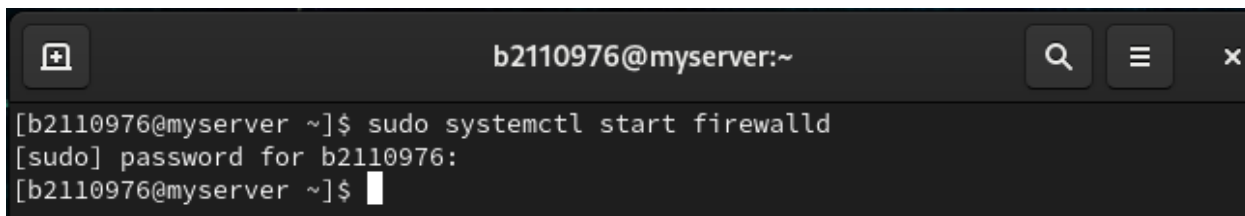
Công cụ Firewallld (dynamic firewall daemon) cung cấp dịch vụ tường lửa mạnh mẽ, toàn diện; được cài đặt mặc định cho nhiều bản phân phối Linux. Từ CentOS 7 trở về sau, tường lửa Firewallld được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- Firewallld 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.
- Firewallld 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 firewallld

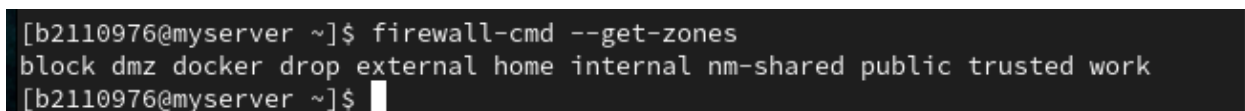
```
$sudo systemctl start firewallld
```



```
b2110976@myserver:~  
[b2110976@myserver ~]$ sudo systemctl start firewallld  
[sudo] password for b2110976:  
[b2110976@myserver ~]$
```

- Liệt kê tất cả các zone đang có trong hệ thống

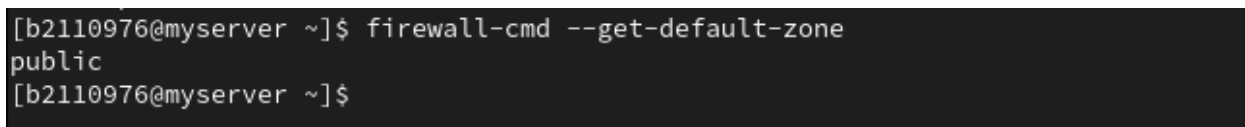
```
$firewall-cmd --get-zones
```



```
[b2110976@myserver ~]$ firewall-cmd --get-zones  
block dmz docker drop external home internal nm-shared public trusted work  
[b2110976@myserver ~]$
```

- Kiểm tra zone mặc định

```
$firewall-cmd --get-default-zone
```



```
[b2110976@myserver ~]$ firewall-cmd --get-default-zone  
public  
[b2110976@myserver ~]$
```


- 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
```

```
[b2110976@myserver ~]$ firewall-cmd --get-active-zones
docker
  interfaces: docker0
public
  interfaces: enp0s3
[b2110976@myserver ~]$
```

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --list-all --zone=public
[sudo] password for b2110976:
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:
[b2110976@myserver ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- Chuyển giao diện mạng sang zone *drop*; và xem các rules của zone

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --zone=drop --change-interface=enp0s3
[sudo] password for b2110976:
success
[b2110976@myserver ~]$
```

```
$sudo firewall-cmd --list-all --zone=drop
success
[b2110976@myserver ~]$ 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:
[b2110976@myserver ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
→ Không thể thực hiện, vì do zone DROP chặn tất cả các dịch vụ mạng nối kết đến máy

- Chuyển giao diện mạng sang zone *trusted*; và xem các rules của zone
\$sudo firewall-cmd --zone=trusted
--change-interface=enp0s3

```
[b2110976@myserver ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[b2110976@myserver ~]$
```

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

```
[b2110976@myserver ~]$ 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:
[b2110976@myserver ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
→ Có thể thực hiện được các thao tác trên. Vì zone trusted cho phép tất cả các dịch vụ có thể thực hiện nối kết đến máy

- Tạo zone mới có tên là *qthtserver*

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
success
[b2110976@myserver ~]$
```

```
$sudo systemctl restart firewalld
```

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

```
[b2110976@myserver ~]$ sudo systemctl restart firewalld
[b2110976@myserver ~]$ 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:
[b2110976@myserver ~]$
```

- 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
```

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
success
```

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
```

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
```

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

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
```



```
$sudo firewall-cmd --permanent --zone=qthtserver  
--add-port=9999/tcp
```

```
[b2110976@myserver ~]$ 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'
```

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.43.151/32 port port=22 protocol=tcp accept'  
success
```

- Khởi động lại tường lửa firewalld

```
$sudo systemctl restart firewalld
```

```
[b2110976@myserver ~]$ sudo systemctl restart firewalld  
[b2110976@myserver ~]$
```

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

```
$sudo firewall-cmd --permanent --zone=qthtserver  
--change-interface=enp0s3
```

```
[b2110976@myserver ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3  
The interface is under control of NetworkManager, setting zone to 'qthtserver'.  
success
```

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

```
[b2110976@myserver ~]$ 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="192.168.43.151/32" 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.
→ Có thể kết nối đến tất cả các dịch vụ được cài đặt rule

--- Hết ---