**BÀI TẬP TỔNG HỢP CUỐI KỲ**

Môn: **Quản Trị Hệ Thống**

**Học kỳ 2 - Năm học 2022-2023**

**Họ tên và MSSV:** Võ Thành Em b2012081

**Nhóm học phần:** CT179\_01

Sinh viên (làm cá nhân) hoàn thành một báo cáo bài tập tổng hợp theo mô tả.

**Lưu ý:**

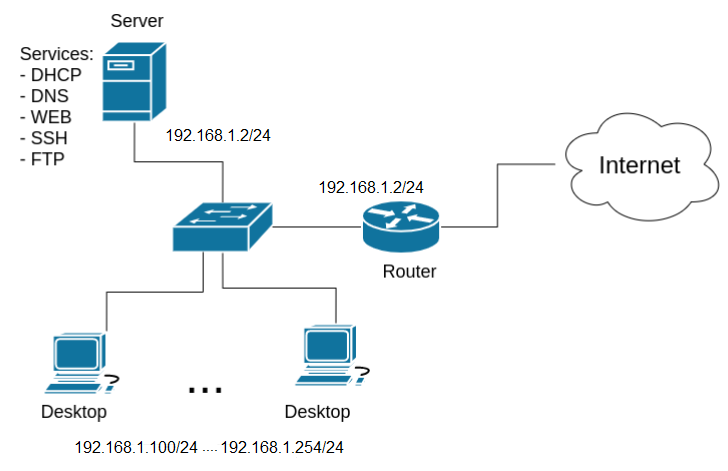
- Bài tập tổng hợp chiếm 15% điểm đánh giá môn học.

- Mọi sao chép bài của nhau giữa các sinh viên sẽ nhận 0đ cho điểm của phần bài tập tổng hợp.

- Thời gian nộp báo cáo dự kiến: trước khi thi cuối kỳ (tuần 19), nộp qua Google classroom của môn học. File báo cáo phải có định dạng PDF.

**Mô tả bài tập tổng hợp:**

Công ty Lương Sơn Bạc chuyên kinh doanh trà sữa có nhu cầu xây dựng hệ thống mạng cục bộ phục vụ cho công việc của công ty như sau:



**1. Cài đặt và cấu hình Server/Desktop (70%)**

**1.1.** (10%) Sử dụng phần mềm VirtualBox/VMware/UTM/Parallels/…:

- Tạo 1 NAT Network tên "QTHT" có địa chỉ mạng là 192.168.1.0/24. Tắt dịch vụ DHCP có sẵn trên NAT Network "QTHT".

- Tạo 2 máy ảo với thông tin như sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | |  |  | **Desktop** | |
| **Host name** | Server |  |  | **Host name** | Desktop |
| **Hệ điều hành** | CentOS 9 |  |  | **Hệ điều hành** | Lubuntu 22.04,  hoặc bất kỳ hệ điều hành khác |
| **CPU/RAM/DISK** | 1core/2G/10G  Hoặc tùy chỉnh theo cấu hình máy của sinh viên |  |  | **CPU/RAM/DISK** | 1core/2G/20G  Hoặc tùy chỉnh theo cấu hình máy của sinh viên |
| **Network** | NAT Network  Name: "QTHT" |  |  | **Network** | NAT Network  Name: "QTHT" |
| **IP** | 192.168.1.2 |  |  | **IP** | Cấu hình động sử dụng dịch vụ DHCP trên server |
| **Subnet mask** | 255.255.255.0 |  |  | **Subnet mask** |
| **Gateway** | 192.168.1.1 |  |  | **Gateway** |
| **DNS** | 192.168.1.1 |  |  | **DNS** |

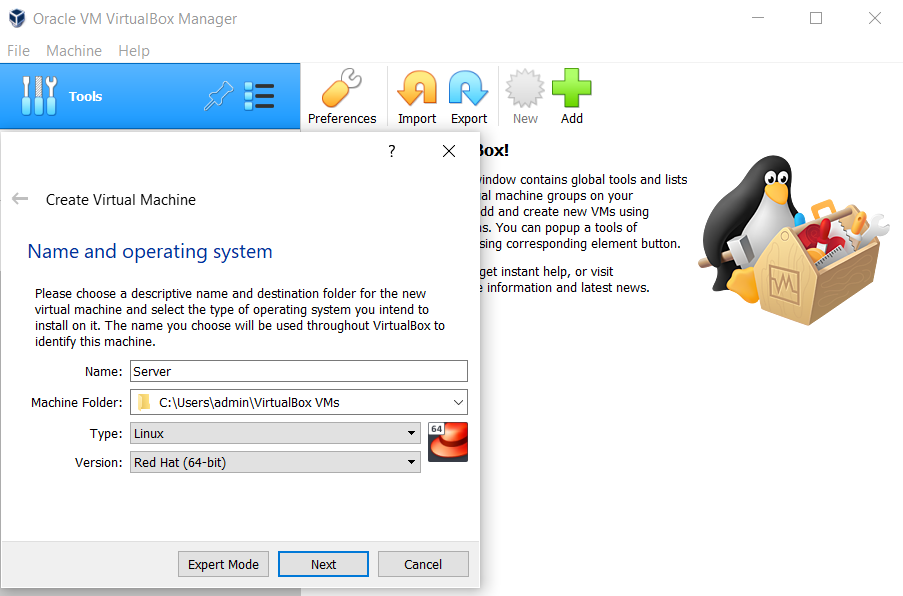
- Trong quá trình cài hệ điều hành CentOS 9, tạo 1 tài khoản với username là <Mã số sinh viên>; firstname và lastname là họ tên của sinh viên. Cấp quyền quản trị (sudo) cho tài khoản. Sử dụng tài khoản vừa tạo để thực hiện bài tập tổng hợp (không dùng tài khoản root).

- lấy hình 1. Giao diện người dùng đăng nhập centos 9 (của lab1)

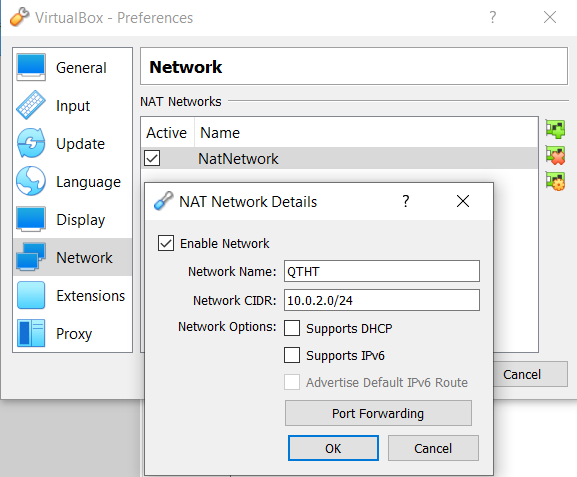
- Tắt dịch vụ tường lửa trên Server.

Cài đặt hệ điều hành CentOS9:

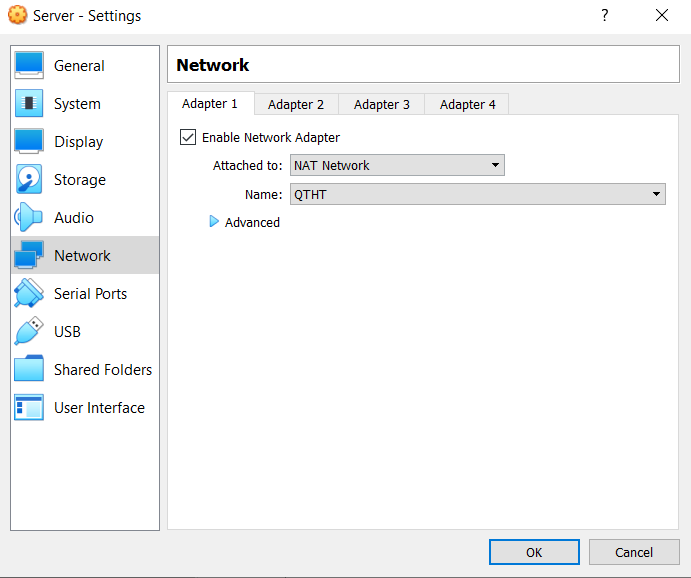
* Mở phần mềm VirtualBox

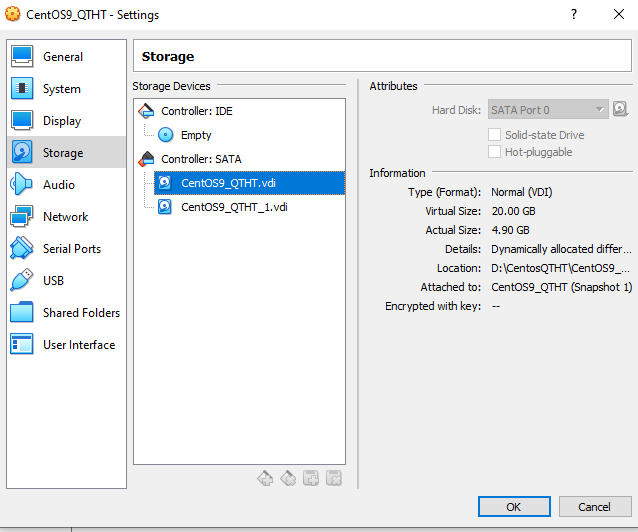
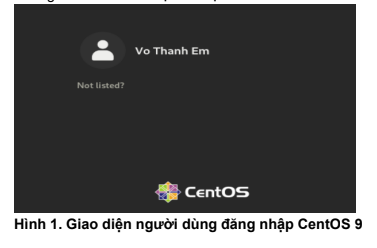


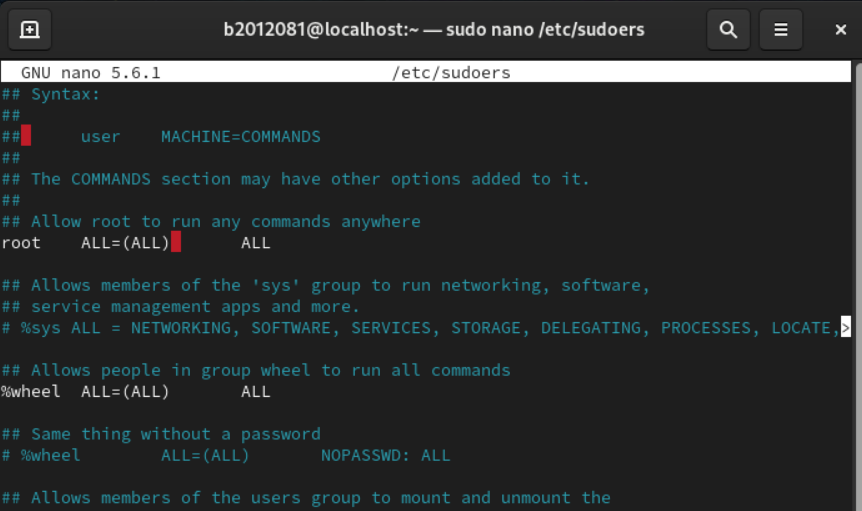
* Tạo một nhánh mạng NAT Network có tên là QTHT.



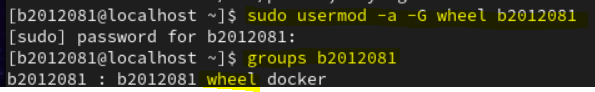
* Kết nối máy ảo Server vừa tạo vào nhánh mạng QTHT



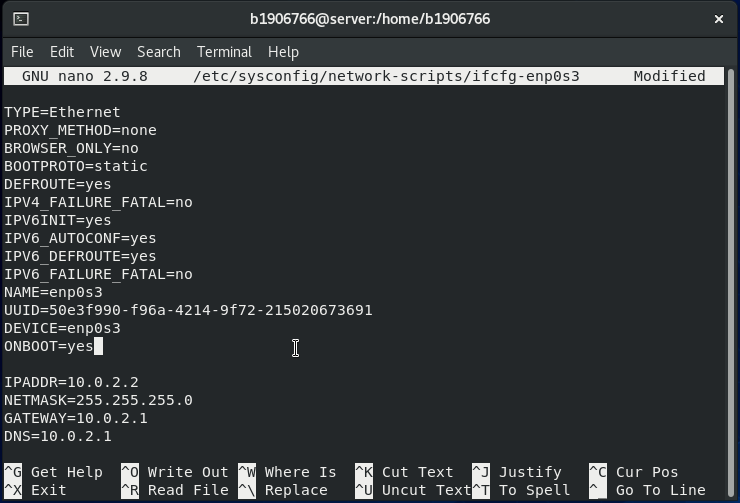
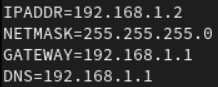
* Thêm đĩa cứng CD/DVD ảo.
* Tiến hành cài đặt máy ảo.
* Thêm tài khoản b202081 vào nhóm người dùng wheel để có quyền sudo



* Lệnh **$sudo usermod -a -G wheel b2012081** để thêm người dùng b2012081 vào nhóm wheel

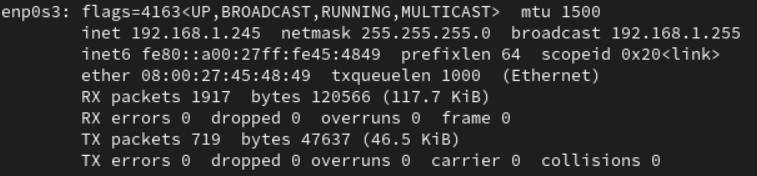


* Cấu hình IP tĩnh cho máy ảo CentOS9



**\*\* Thay đổi DNS => DNS1**

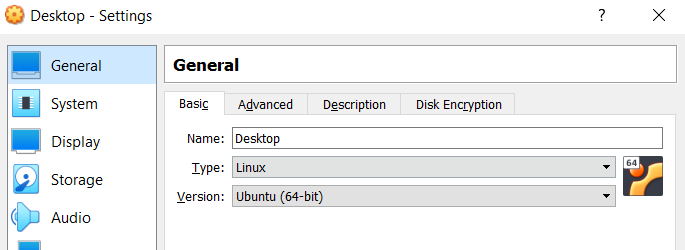
* Xem lại địa chỉ IP đã thay đổi bằng lệnh **ifconfig -a**

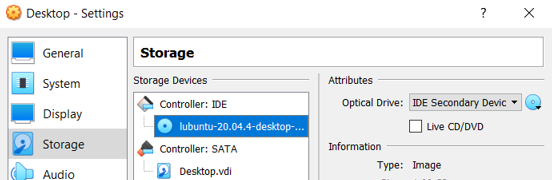


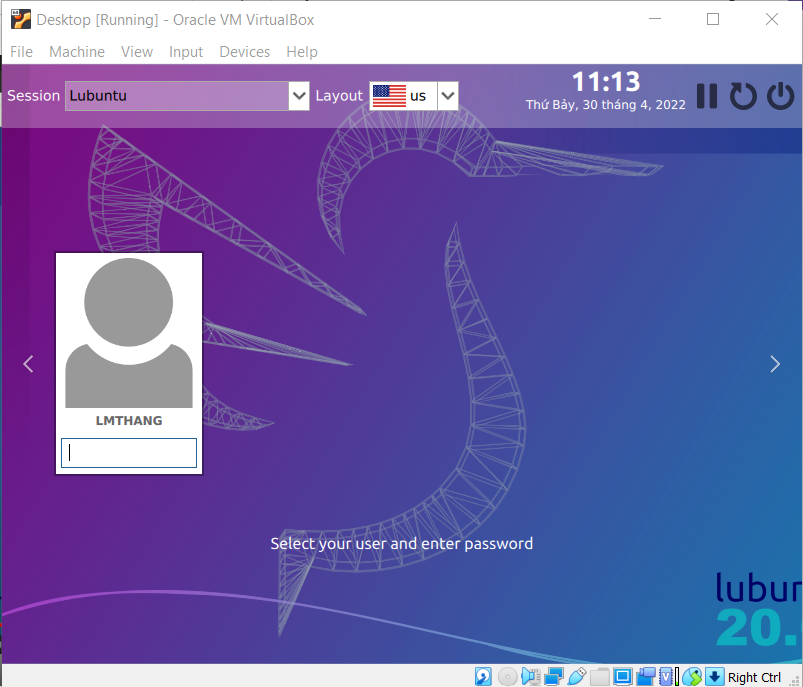
**Cài đặt hệ điều hành Lubuntu**

[Downloads – Lubuntu](https://lubuntu.me/downloads/)

* Tương tự như CentOS9 nhưng chọn đĩa CD/DVD của Lubuntu







Thứ Bảy, 29 tháng 4, 2023

**1.2.** (10%)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 Lư Tuấn Nghĩa.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Họ Tên** | **Nhóm** | **Username** | **Password** | **Mô tả** |
| 1 | Tống Giang | bangiamdoc | giang.tong | tgiang | Giám đốc |
| 2 | Lư Tuấn Nghĩa | bangiamdoc | nghia.lu | ltnghia | Phó giám đốc |
| 3 | Ngô Dụng | banhang | dung.ngo | ndung | Trưởng phòng |
| 4 | Lâm Xung | banhang | xung.lam | lxung | Nhân viên |
| 5 | Võ Tòng | banhang | tong.vo | vtong | Nhân viên |
| 6 | Lỗ Trí Thâm | hanhchanh | tham.lo | lttham | Trưởng phòng |
| 7 | Lý Quỳ | hanhchanh | quy.ly | lquy | Nhân viên |

* Thêm người dùng lệnh **$sudo adduser <tentaikhoan>**
* Thêm mật khẩu cho người dùng bằng lệnh **$sudo passwd <tentaikhoan>**

1.



2.



3.



4.



5.



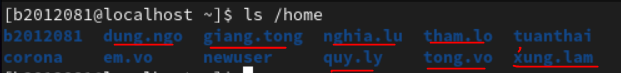
6.

**7.**



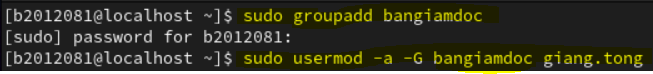
**Kiểm tra lại người dùng đã tạo**



* Tạo nhóm người dùng **bangiamdoc,** thêm người dùng **giang.tong** và **nghia.lu** vào nhóm người dùng **bangiamdoc**.
* Dùng lệnh :

**$sudo groupadd <<tên nhóm>>**

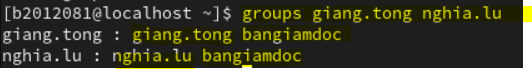
**$sudo usermod -a -G <<tên nhóm>> <<tên người dùng>>**



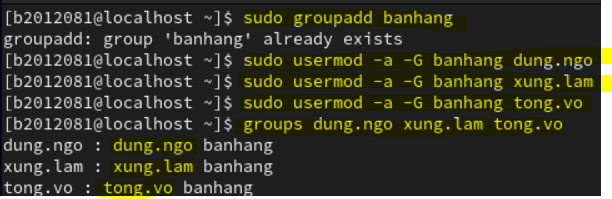




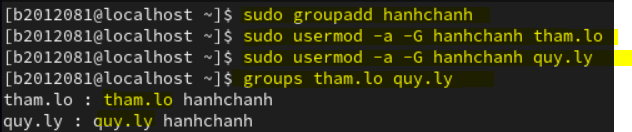
* kiểm tra lại dùng lệnh **thuộc nhóm nào**

**$groups <<tên người dùng>>** 

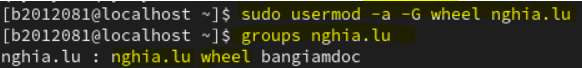
* Tạo nhóm người dùng **banhang,** thêm người dùng **dung.ngo**, **xung.lam** và **tong.vo** vào nhóm người dùng **banhang**.



* Tạo nhóm người dùng **hanhchanh,** thêm người dùng **tham.lo** và **quy.ly** vào nhóm người dùng **hanhchanh**.



* **Để cấp quyền sudo cho người dùng Lư Tuấn Nghĩa ta thêm người dùng này vào nhóm wheel**



**1.3.** (10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server.

- Chỉ có thành viên ban giám đốc và tài khoản <Mã số sinh viên> mới có quyền điều khiển từ xa Server. Tài khoản root không được nối kết tới server từ xa.

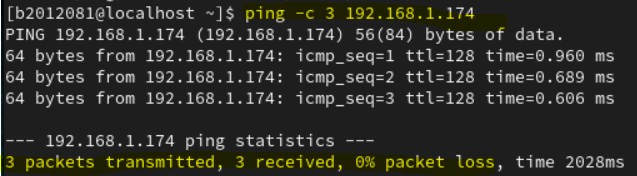
- Chỉ cho phép chứng thực bằng private key, không cho phép chứng thực bằng password. Tạo private/public key cho người dùng <Mã số sinh viên> để có thể SSH tới server.

SSH (Secure Shell) là một giao thức mạng được dùng để thực hiện các giao dịch an toàn giữa client/server. Trong thực tế, người quản trị hệ thống thường điều khiển các máy chủ Linux từ xa thông qua kết nối SSH. Trong bài thực hành này, sinh viên cần thiết lập một kết nối SSH giữa hai máy sau:

Máy ảo (virtual machine): là máy bị điều khiển. Máy này cần được cài SSH Server, ví dụ như OpenSSH, và chạy dịch vụ tương ứng ở cổng nào đó (thông thường là cổng 22) để lắng nghe các yêu cầu kết nối.

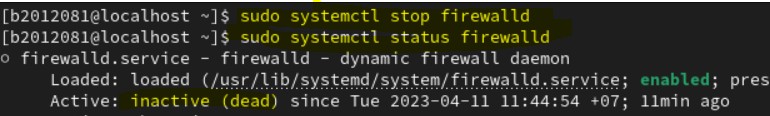
Máy vật lý (physical machine): là máy ra lệnh điều khiển. Đối với Linux/Mac OS, hệ thống có sẵn lệnh ssh để thực hiện kết nối. Đối với Windows, ta cần cài thêm SSH Client, ví dụ như Mobaxterm hoặc PuTTY.

* + - Cấu hình mạng và ghi lại địa chỉ IP. Đảm bảo rằng bạn có thể truy cập Internet từ máy ảo. (đã làm ở câu 1.1)

**$ping -c 3 <IP của máy vật lý>**

**#Tắt tường lửa trên máy vật lý nếu không ping được**

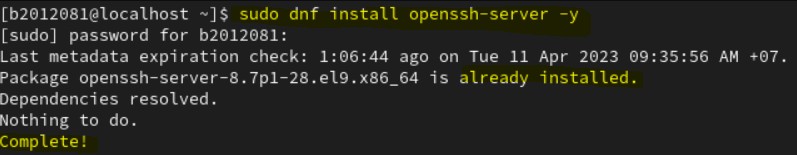
* Tắt tường lửa:

**$sudo systemctl stop firewalld**

**$ping -c 3 google.com**

# 

* + - **Cài đặt OpenSSH:**

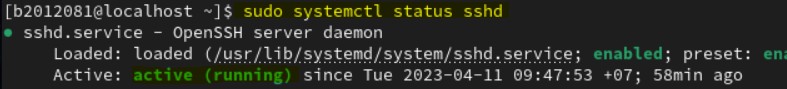
$sudo dnf install openssh-server -y

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

$sudo systemctl start sshd

$sudo systemctl enable sshd

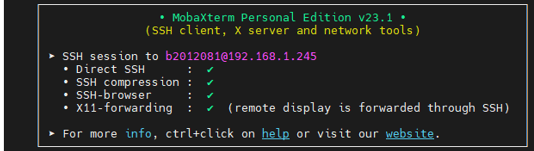
* + - **Kiểm tra xem SSH Server có đang thực thi hay chưa:**

$sudo systemctl status sshd

**Kết nối tới SSH server từ máy vật lý**

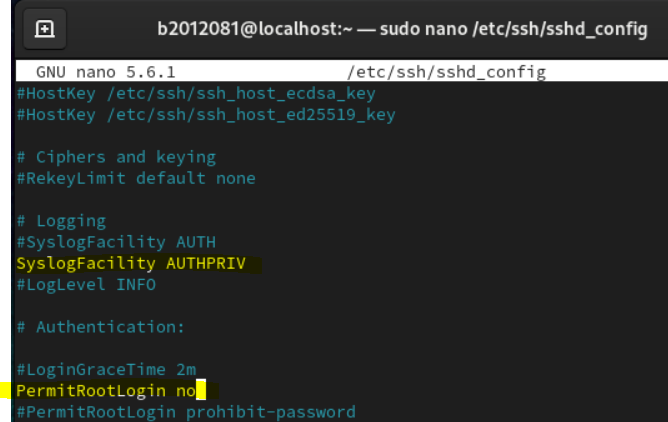
* + - Nếu là hệ điều hành Windows: cài đặt phần mềm SSH Client như [MobaXterm](https://mobaxterm.mobatek.net/) (<https://mobaxterm.mobatek.net/>) hoặc [PuTTY](http://www.putty.org/), nhập các thông số và thực hiện kết nối.
    - 



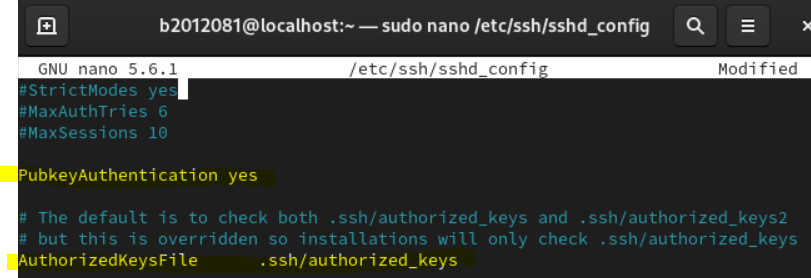


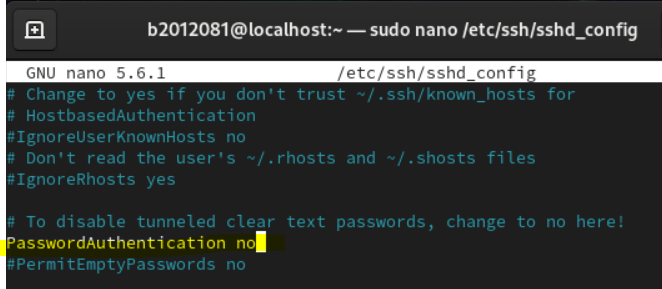
- Thay đổi file cấu hình **/etc/ssh/sshd\_config** để chỉ có **thành viên ban giám đốc** và tài **khoản <mã số sinh viên>** mới có quyền điều khiển từ xa server.

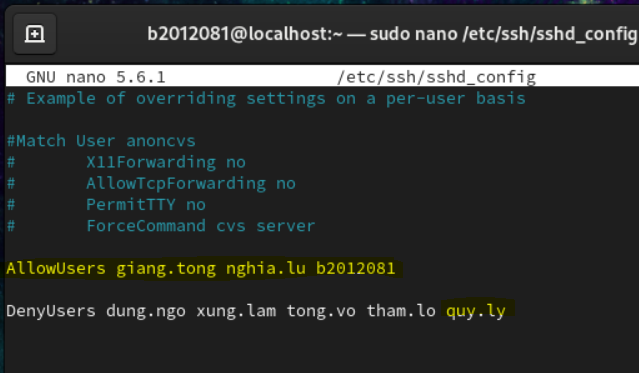
- Tài khoản root **không** được nối kết tới server từ xa.



**Chỉ cho phép chứng thực bằng private key, không cho phép chứng thực bằng password**





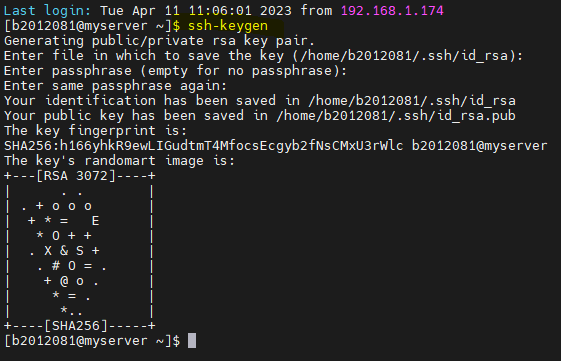


**Tạo private/public key cho người dùng <Mã số sinh viên> để có thể SSH tới server.**

* 1. Ngoài cách đăng nhập tới SSH server sử dụng username/password, chúng ta có thể sử dụng private/public key (an toàn hơn).
     + Trên máy vật lý sử dụng công cụ Mobaxterm để kết nối tới máy CentOS 9.
     + Tạo private/public keys:

$ssh-keygen

**# Chọn các thông mặc định khi được hỏi**



* + - **Di chuyển public key đến vị trí mặc định(.ssh/authorized\_keys):**

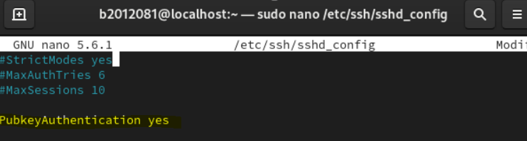
$mv .ssh/id\_rsa.pub .ssh/authorized\_keys

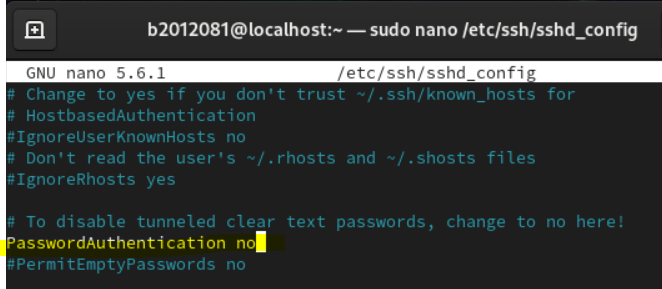
* + - **Phân quyền lại cho file chứa public key**:

$chmod 600 .ssh/authorized\_keys

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

$sudo nano /etc/ssh/sshd\_config # Thay đổi PubkeyAuthentication yes PasswordAuthentication no

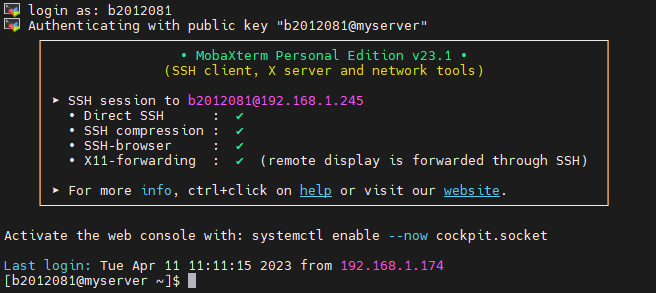
 



* + - Download file private key (.ssh/id\_rsa) về máy vật lý.
    - Khởi động lại Khởi động SSH Server:

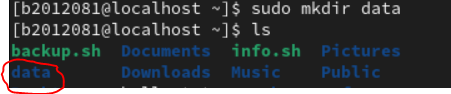
$sudo systemctl restart sshd

* + - Sử dụng Mobaxterm lần lượt kết nối SSH tới máy CentOS 9 sử dụng chứng thực bằng password và private key. Cho biết kết quả (chụp lại ảnh minh họa).



**1.4.** (10%)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 /data.

* Tạo thư mục bằng lệnh **$sudo mkdir data**

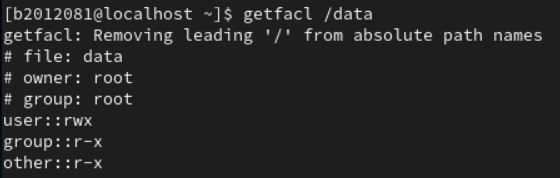


**Cài đặt ACL package**



* Dùng **$ls -dl** để kiểm tra quyền:
* Kiểm tra trạng thái khởi đầu của ACL:

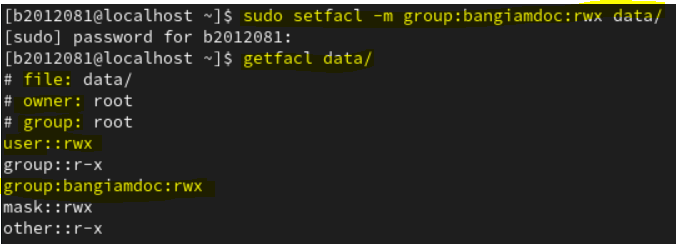




**Gán quyền**

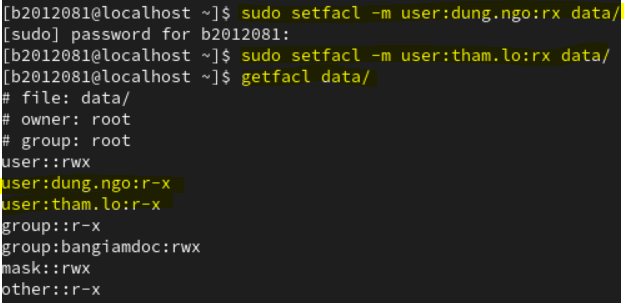
* Read, write, execute cho nhóm người dùng **bangiamdoc.**

Lệnh**: $sudo setfacl -m group:bangiamdoc:rwx data/**



* Trưởng phòng là người dùng **dung.ngo và tham.lo** có quyền read, execute

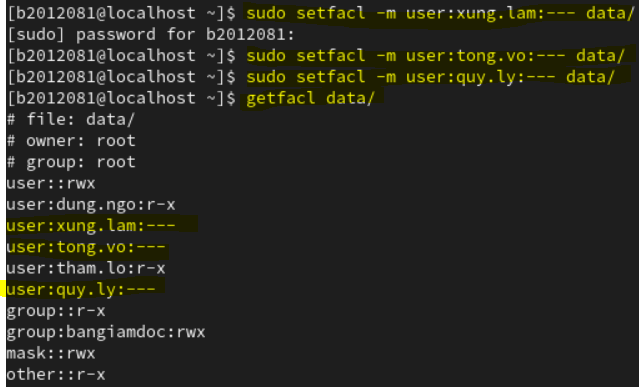
Lệnh **sudo setfacl -m user: <<tên người dùng>> :rx data/**



* Nhân Viên là người dùng **xung.lam** và **tong.vo** với **quy.ly** không có bất cứ quyền gì.

Lệnh **sudo setfacl -m user: <<ten người dùng>> :--- data/**





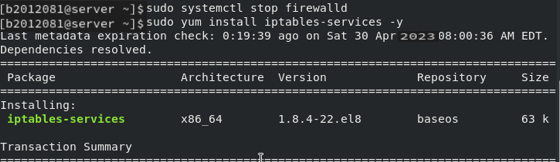
**1.5.** (5%) Cài đặt và cấu hình tường lửa trên Server để cho phép:

- Có thể truy cập các dịch vụ DNS, DHCP, SSH, Web, SAMBA trên Server. Các dịch vụ khác KHÔNG cập truy cập được.

**Thực thi tường lửa iptables:**

Dừng tường lửa firewalld **$sudo systemctl stop firewalld**

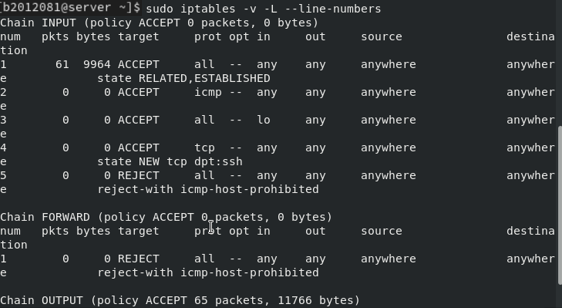
Cài đặt và thực thi tường lửa iptables **$sudo yum install iptables-services -y**





**Hiển thị các rules hiện có trên iptables**

**Lệnh $sudo iptables -v -L --line-numbers**



**Tạo rules để cho phép các máy khác truy cập tới dịch vụ Web trên server**

* **Trong đó các cổng dport lần lượt có ý nghĩa:**

+ --dprot 80 (Web), --dport 53 (DNS), --dport 67 (DHCP), --dport 22 (SSH),

**sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT**

**sudo iptables -D INPUT 6**

**sudo iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT**





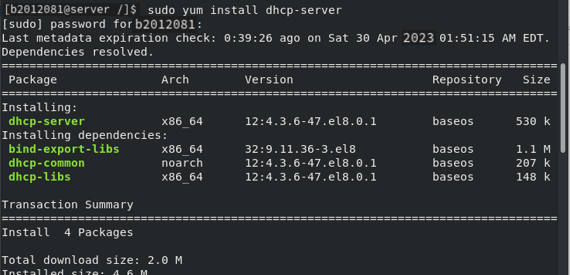
**1.6.** (5%) Cài đặt và cấu hình dịch vụ DHCP trên Server để cấu hình mạng tự động cho các máy Desktop trong nhánh mạng:

- Địa chỉ IP của desktop: trong dãy 192.168.1.100/24 đến 192.168.1.254/24

- Địa chỉ gateway: 192.168.1.1

- DNS server: 192.168.1.2 và 8.8.8.8

**Bước 1**: Cài đặt gói dhcp: sudo yum install dhcp-server



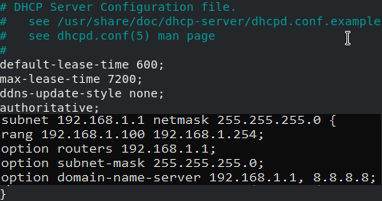
**Bước 2**: Cấu hình dhcp: **$sudo nano /etc/dhcp/dhcpd.conf**

* Tắt tường lửa và khởi động dịch vục dhcpd

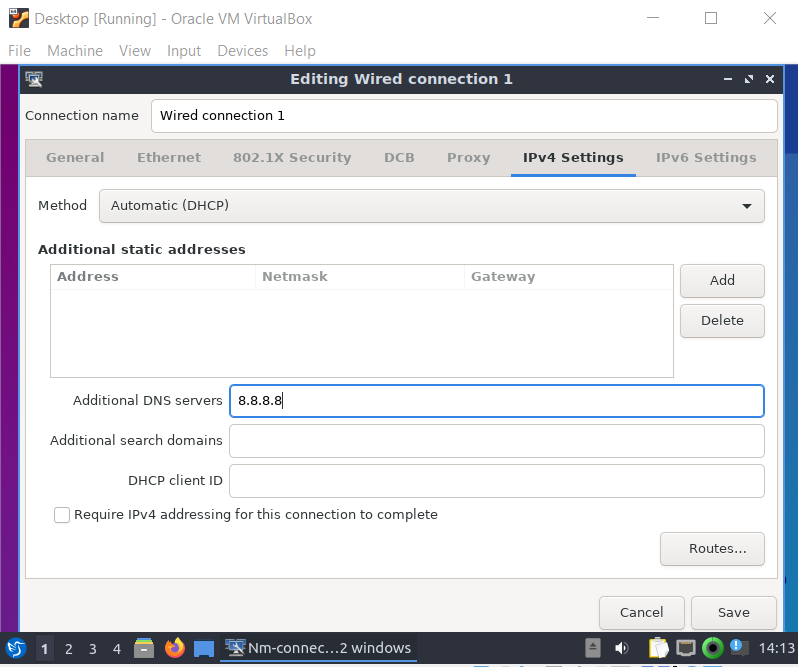


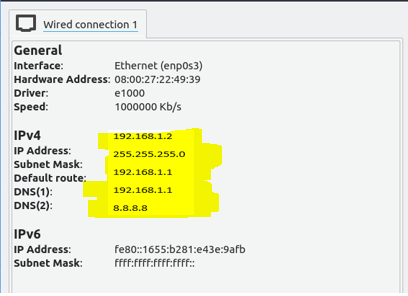
* Điều chính file dhcpd.conf

Lệnh **sudo nano /etc/dhcp/dhcpd.conf**



**Kiểm tra trên máy Lubuntu**





**1.7.** (5%)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 *thuyhu.com****(192.168.1.2)***với nội dung trang chủ giới thiệu về các thành viên trong công ty.

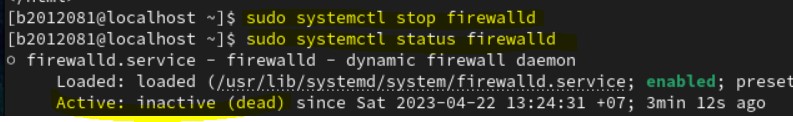
Tạo thư mục ~/myweb, sau đó tạo một trang web đơn giản index.html lưu thư mục ~/myweb

Dùng lệnh $tree xem lại cây thư mục



Tắt tường lửa:

$sudo systemctl stop firewalld

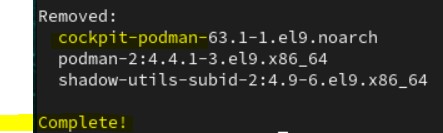


**Cài đặt Docker lên máy ảo CentOS 9**

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

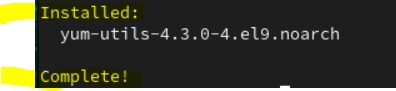
**$sudo dnf -y remove podman runc**





* + - Cài đặt công cụ yum-utils

$sudo dnf install -y yum-utils



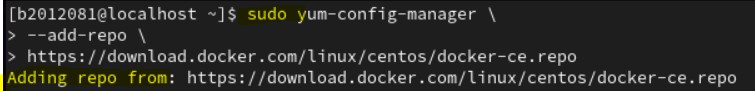
* + - Thêm địa chỉ repo của Docker vào công cụ yum

$sudo yum-config-manager \

--add-repo \

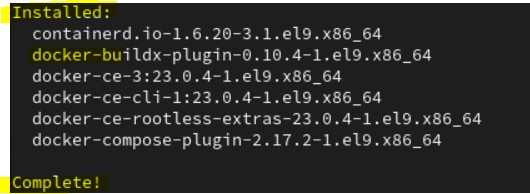
<https://download.docker.com/linux/centos/docker-ce.repo>

#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.



* + - Cài đặt Docker

$sudo dnf install docker-ce -y

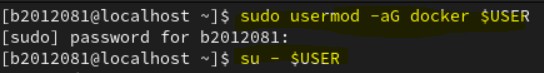


* + - Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo

$sudo usermod -aG docker $USER

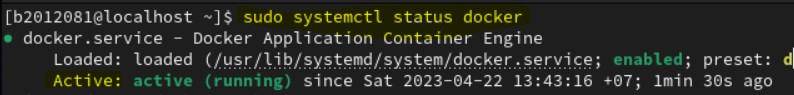
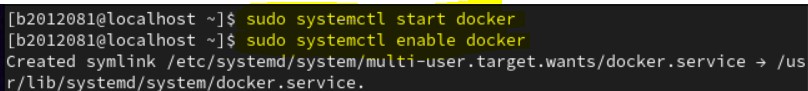
* + - Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng

$su - $USER



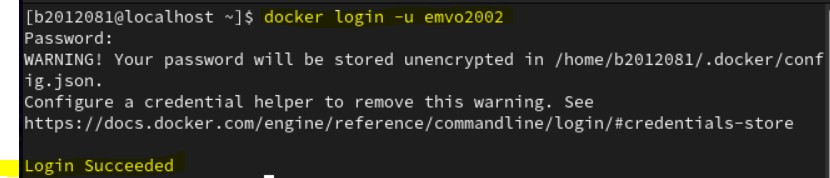
Chạy dịch vụ docker

$sudo systemctl start docker

$sudo systemctl enable docker

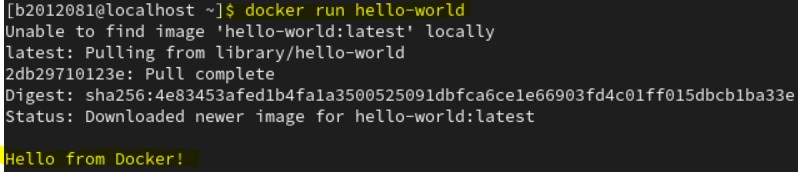


* + - Tạo 1 tài khoản trên DockerHub (<https://hub.docker.com/>), sau đó đăng nhập sử dụng lệnh sau:

$docker login -u <docker-username>

* + - 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

* + - Tạo container từ image httpd

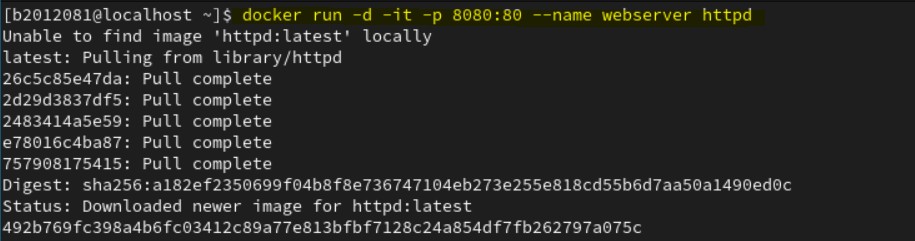
$docker run -d -it -p 8080:80 --name webserver httpd

-d: chạy container ở chế độ background

-it: tạo shell để tương tác với container

--name webserver: đặt tên container là webserver

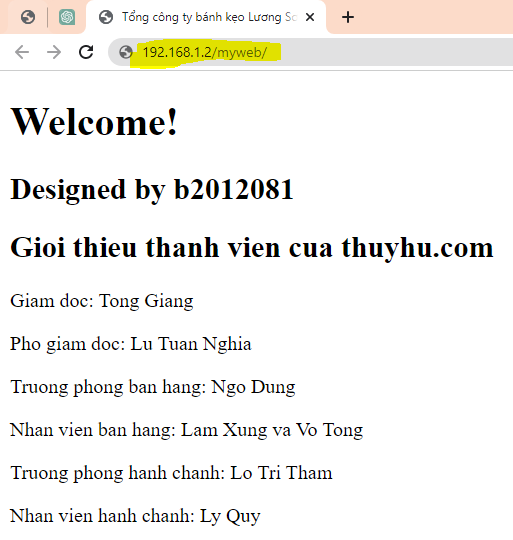
-p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container.



* Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.
* Lệnh $**sudo docker cp/myweb/ webserver:/usr/local/apache2/htdocs/**



* Trên máy desktop, mở trình duyệt web và truy cập vào địa chỉ **http:// 192.168.1.2/myweb** để kiểm chứng trang web vừa tạo



**1.8.** (5%)Cài đặt và cấu hình dịch vụ SAMBA trên Server. Cấu hình chỉ cho phép:

**- Thành viên ban giám đốc và trưởng phòng có thể truy cập vào thư mục /data trên Server.**

**- Tất cả người dùng có thể truy cập vào thư mục cá nhân của họ (/home/<username>) trên Server.**

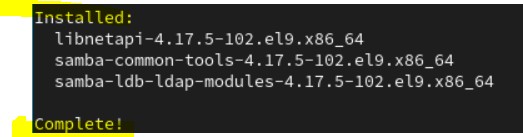
**- Trên Desktop tạo ổ cứng ảo nối kết tới dịch vụ SAMBA trên Server.**

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**

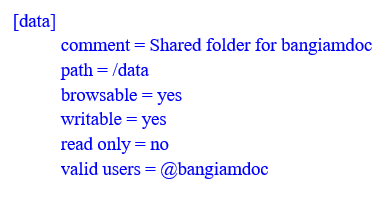


* Cấu hình dịch vụ Samba:

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

**$sudo nano /etc/samba/smb.conf**

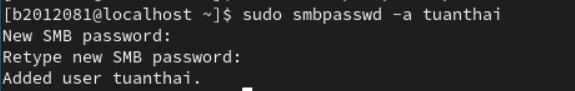
#Thêm đoạn cấu hình bên dưới vào cuối tập tin

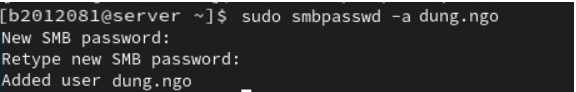


* Thêm người dùng cho dịch vụ Samba:

**$sudo smbpasswd -a <<tên người dùng>>**

#Đặt mật khẩu Samba cho người dùng



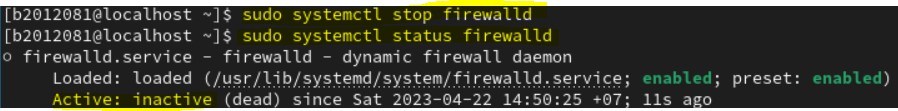


* Cấu hình SELINUX cho phép Samba

$sudo setsebool -P samba\_export\_all\_rw on

$sudo setsebool -P samba\_enable\_home\_dirs on

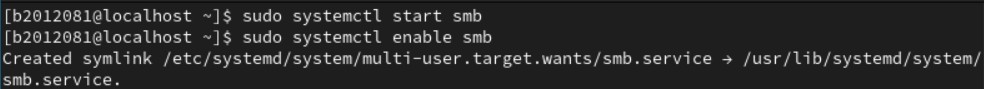
* Tắt tường lửa:

$sudo systemctl stop firewalld

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

$sudo systemctl start smb

$sudo systemctl enable smb



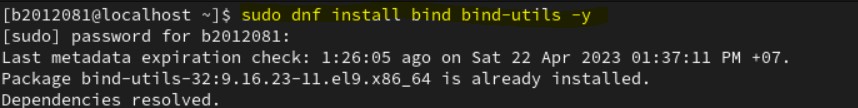
- Trên File Explorer của máy Windows, chọn tính năng “Add a network location” để nối kết tới Samba server sử dụng địa chỉ \\<IP máy CentOS>\data

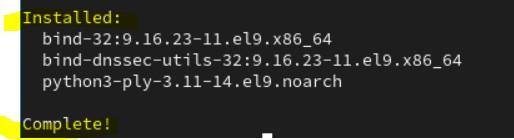
**1.9.** (5%)Cài đặt và cấu hình dịch vụ DNS trên Server để phân giải tên miền *thuyhu.com*

Tên miền: *www.thuyhu.com <----> IP:* 192.168.1.2 (Server IP)

Tên miền: *gateway.thuyhu.com <----> IP:* 192.168.1.1

* 1. Cài đặt BIND và các công cụ cần thiết:

$sudo dnf install bind bind-utils -y

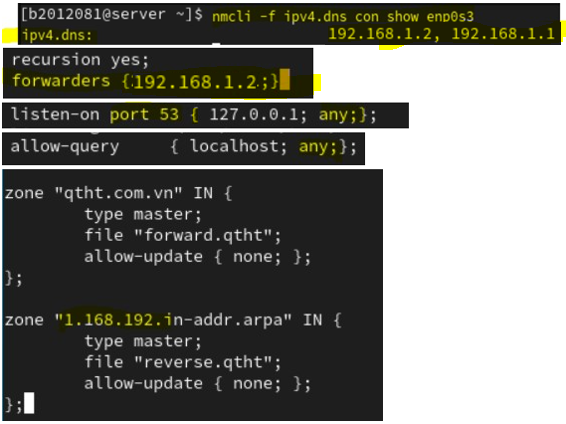


**Cấu hình DNS server:**

$sudo nano /etc/named.conf

#(tham khảo file mȁu)





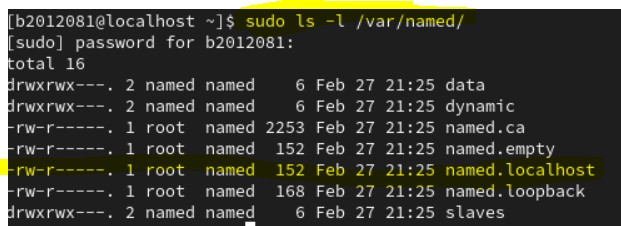
Tạo tập tin cấu hình phân giải xuôi:

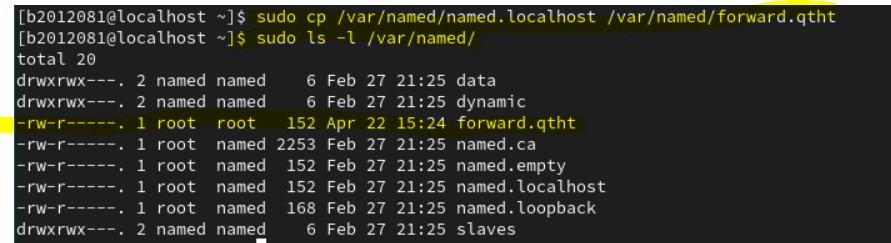
$sudo cp /var/named/named.localhost /var/named/forward.qtht

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

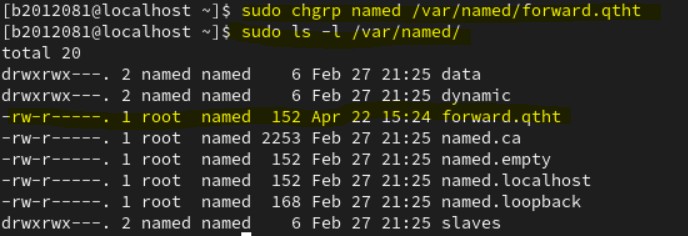
$sudo nano /var/named/forward.qtht

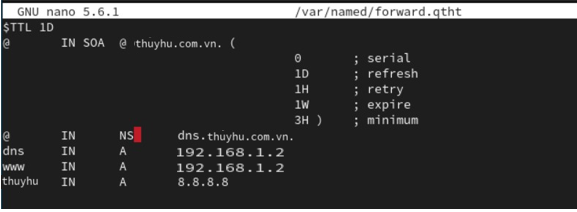
#(tham khảo file mȁu)

**ban đầu**

**sau đó**

**Tiến hành đổi tên nhóm chủ sở hữu thành nhóm named**



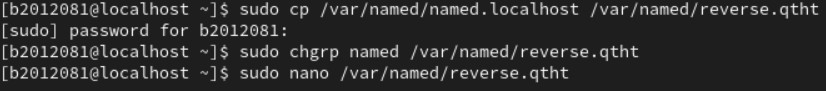


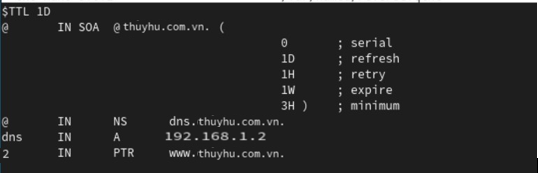
Tạo tập tin cấu hình phân giải ngược:

$sudo cp /var/named/forward.qtht /var/named/reverse.qtht

$sudo chgrp named /var/named/reverse.qtht

$sudo nano /var/named/reverse.qtht



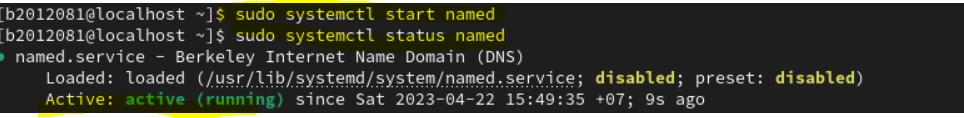


**Kiểm tra và sử dụng dịch vụ DNS**

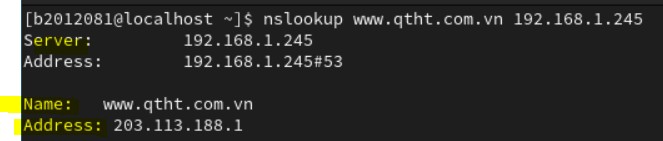
* Tắt tường lửa:

$sudo systemctl stop firewalld

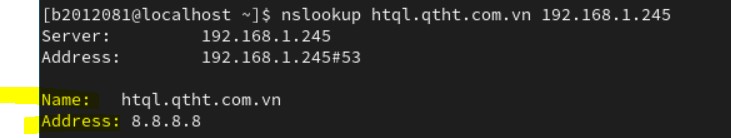
* Khởi động dịch vụ DNS:

$sudo systemctl start named

* Kiểm tra kết quả:

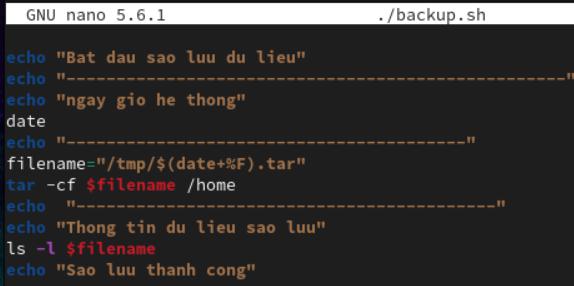
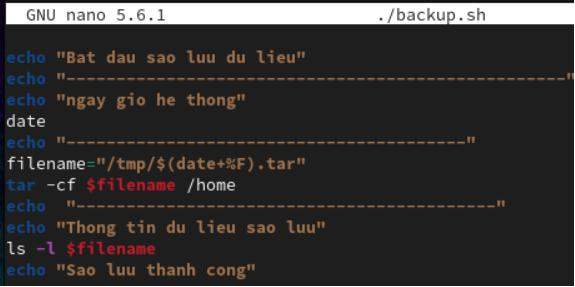
nslookup [www.qtht.com.vn](http://www.qtht.com.vn/) <địa chỉ IP máy ảo>

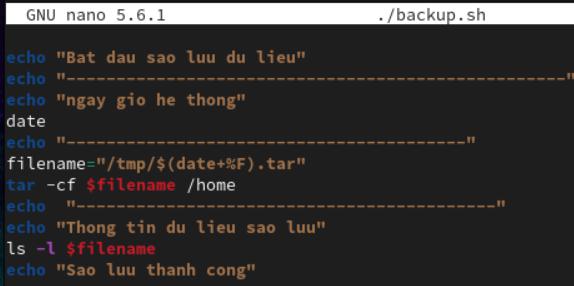


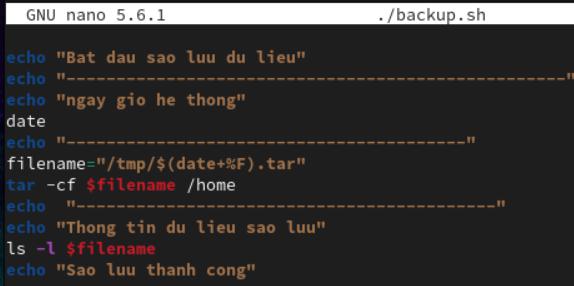
nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>

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

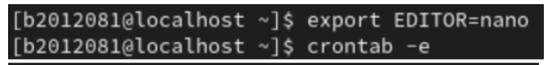
- Sao lưu mỗi tuần: thực hiện vào lúc 23:59 ngày chủ nhật hàng tuần, dữ liệu sẽ được nén lại và lưu với tên như sau: backup\_week<thứ tự tuần> (ví dụ: backup\_week1).

- 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.

Cron là một tiện ích trong Linux cho phép máy tính thiết lập thời gian biểu để thực hiện

công việc một cách định kỳ. Một crontab file chứa danh sách các lệnh sẽ được thực thi, kèm theo thông tin về thời điểm lặp lại việc thực thi. Để hiệu chỉnh file crontab với trình soạn thảo nano, ta dùng các lệnh sau:

**lệnh export EDITOR=nano cho phép chuyển đổi giao diện sang nano crontab -e**









**2. Hình thức bài báo cáo bài tập tổng hợp (30%)**

* Viết báo cáo trình bày các bước thực hiện công việc 1.1 đến 1.10.
* Trình bày rõ ràng đầy đủ từng bước thực hiện và có hình ảnh minh hoạ. Báo cáo ít lỗi chính tả, trình bày đẹp; có hình ảnh minh họa rõ, chi tiết, có mục lục, …

--- Hết ---