**TRƯỜNG ĐẠI HỌC CẦN THƠ**

**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**————**🕮**————**



**QUẢN TRỊ HỆ THỐNG**

**Mã Học Phần: CT179**

**BÀI TẬP TỔNG HỢP CUỐI KỲ**

**Mã Lớp Học Phần: CT179-06**

**Sinh viên: Lê Trương Ngọc Duyên**

**MSSV: B2105569**

**Khóa: K47**

**Học Kỳ I, 2023 - 2024**

**MỤC LỤC**

**[MÔ TẢ BÀI TẬP TỔNG HỢP](#_Toc151847167)** [3](#_Toc151847167)

**[CÂU 1.1.](#_Toc151847168)** [3](#_Toc151847168)

**[CÂU 1.2.](#_Toc151847169)** [12](#_Toc151847169)

**[CÂU 1.3.](#_Toc151847170)** [14](#_Toc151847170)

**[CÂU 1.4.](#_Toc151847171)** [20](#_Toc151847171)

**[CÂU 1.5.](#_Toc151847172)** [24](#_Toc151847172)

**[CÂU 1.6.](#_Toc151847173)** [26](#_Toc151847173)

**[CÂU 1.7.](#_Toc151847174)** [28](#_Toc151847174)

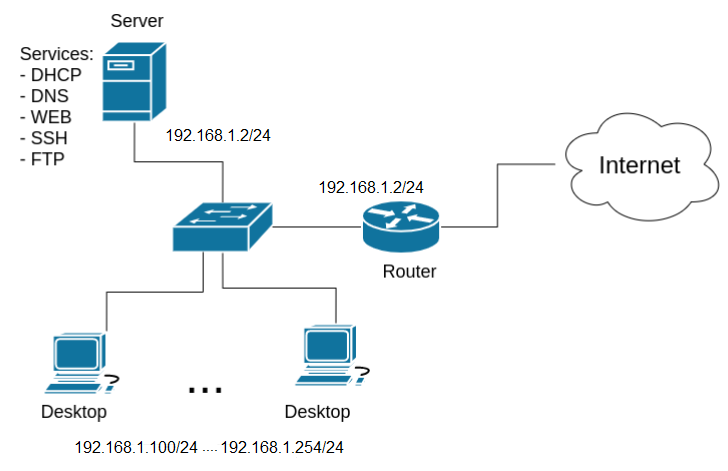
**[CÂU 1.8.](#_Toc151847175)** [33](#_Toc151847175)

**[CÂU 1.9.](#_Toc151847176)** [39](#_Toc151847176)

**[CÂU 1.10.](#_Toc151847177)** [43](#_Toc151847177)

## **MÔ TẢ BÀI TẬP TỔNG HỢP**

Công ty Straw Hat chuyên kinh doanh hải sản có nhu cầu xây dựng hệ thống mạng cục bộ phục vụ cho công việc của công ty như sau:



## **CÂU 1.1.**

**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).

- Tắt dịch vụ tường lửa trên Server.

**BÀI LÀM**

**\*Tạo 1 NAT Network tên "QTHT" có địa chỉ mạng là 192.168.1.0/24**

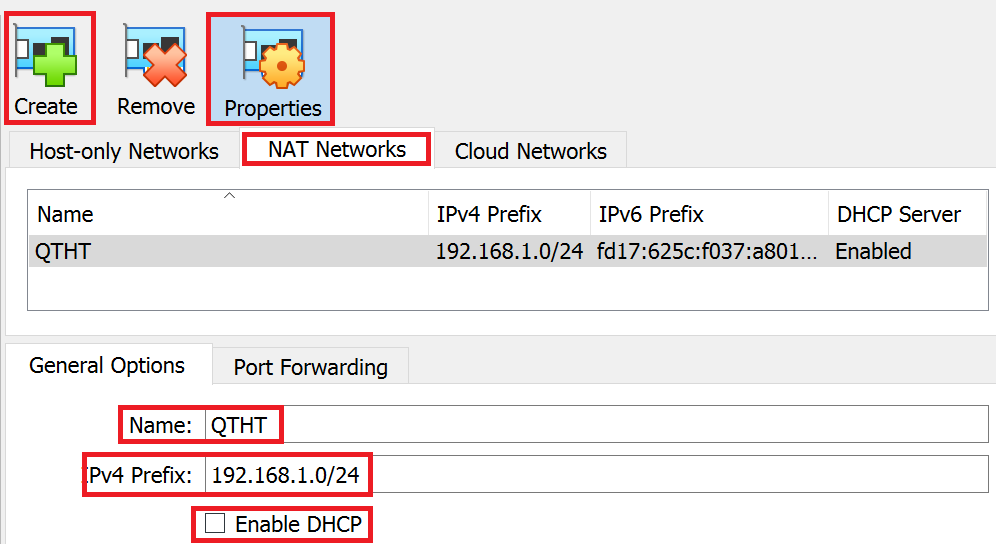
-Chọn Tools 🡪 Network

-Chọn NAT Networks 🡪 Create 🡪 Properties

-Trong General Options:

* Name: QTHT
* Ipv4 Prefix: 192.168.1.0/24
* Bỏ check ô Enable DHCP

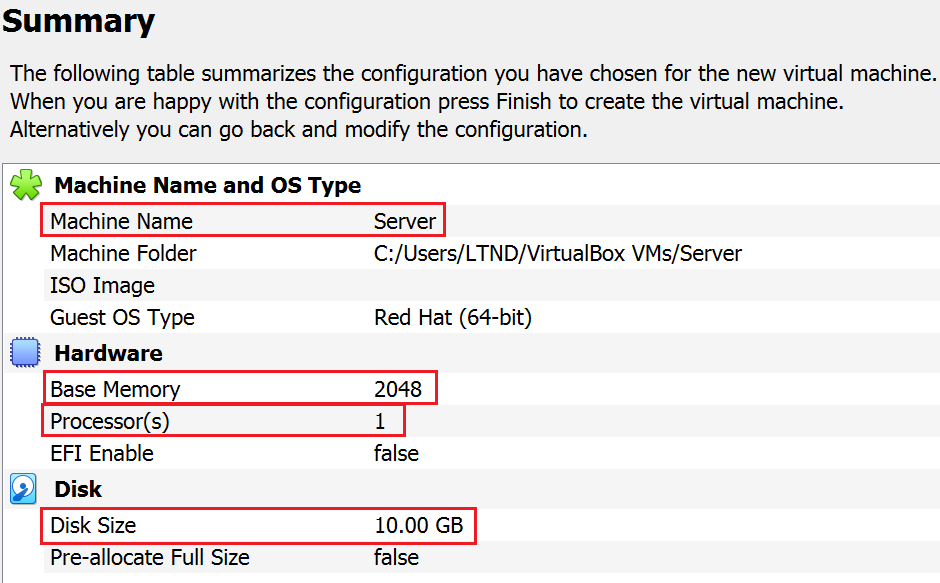
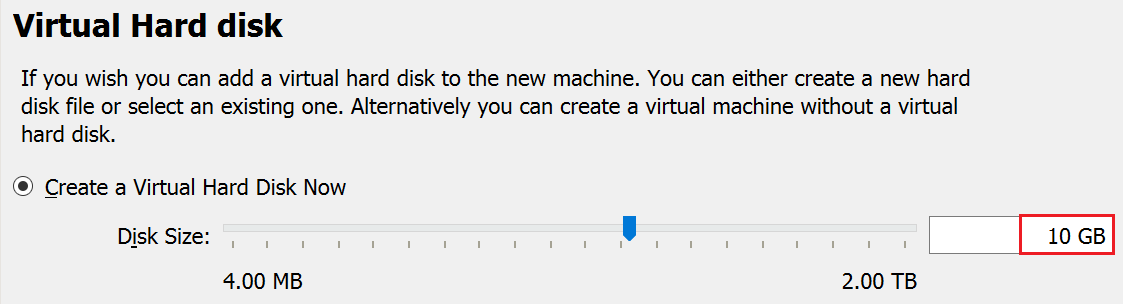
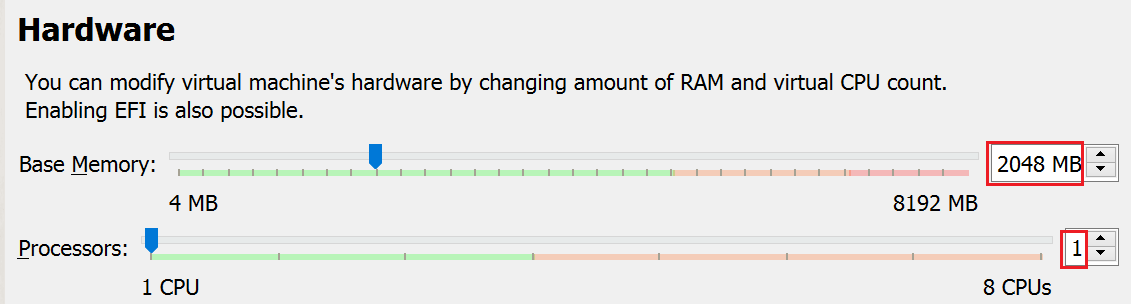
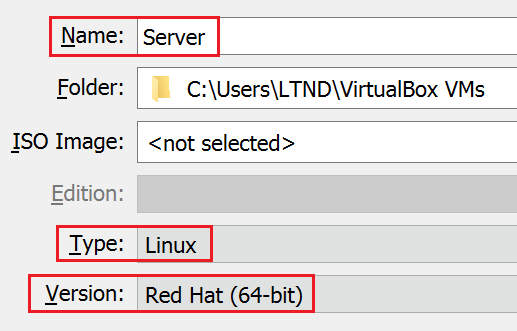
🡺Chọn Apply



**\*Tạo máy ảo Server:**

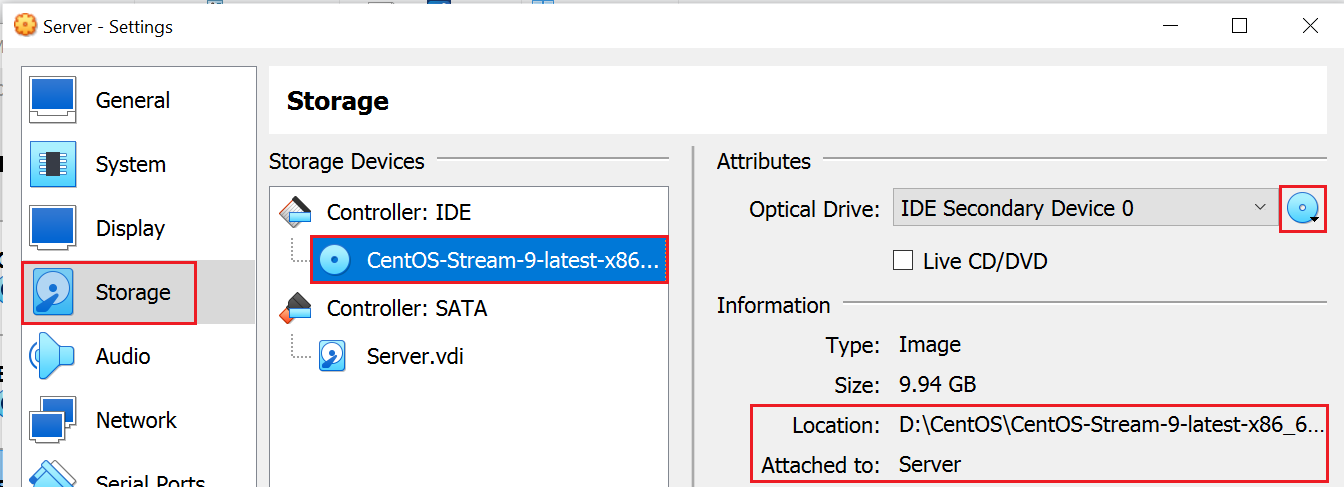
-Chọn New để tạo ra 1 máy ảo

* Name: Server
* Base Memory: 2GB ⬄ 2048MB
* Processors: 1 CPU
* Disk Size: 10GB

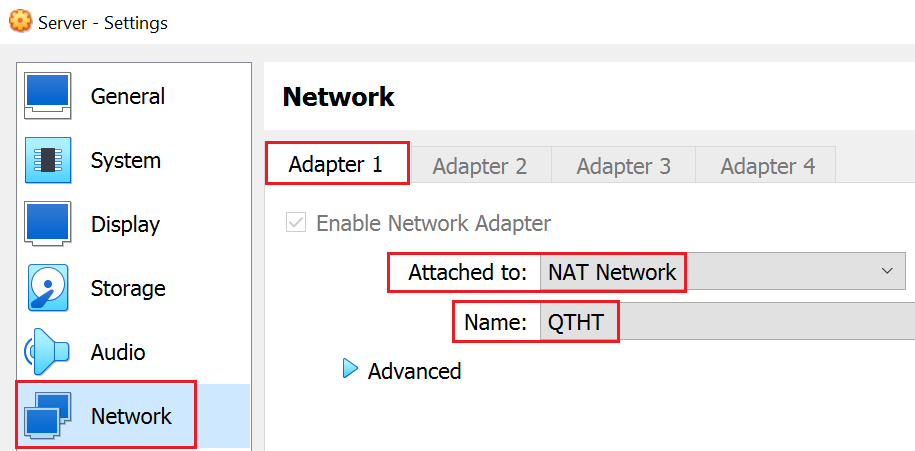


-Sau khi tạo xong thì chọn Settings

* Vào Storage 🡪 chọn file iso CentOS đã tải xuống và chọn OK

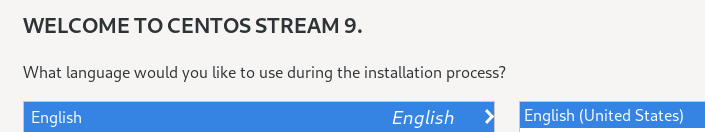


* Vào NetWork 🡪 Tại Adapter 1, chọn Attached to: NAT Network và Name QTHT

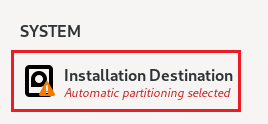
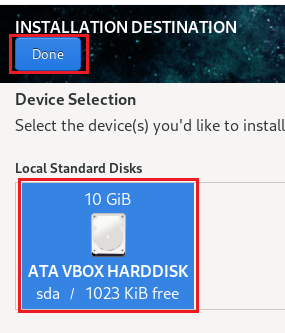


-Tiếp theo, chọn Start để khởi động máy ảo Server

-Chọn ngôn ngữ: English

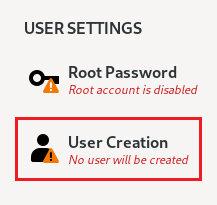
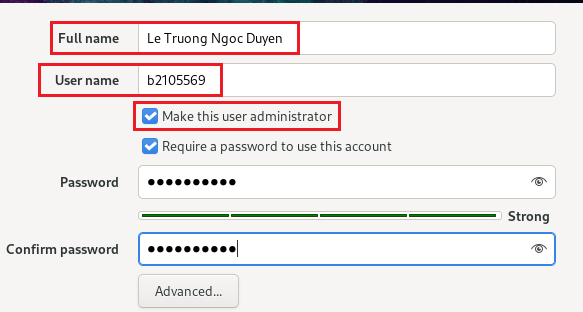


-Chọn Installation Destination 🡪 Chọn ổ cứng 10GB vừa tạo 🡪 Done

-Chọn User Creation để tạo tài khoản

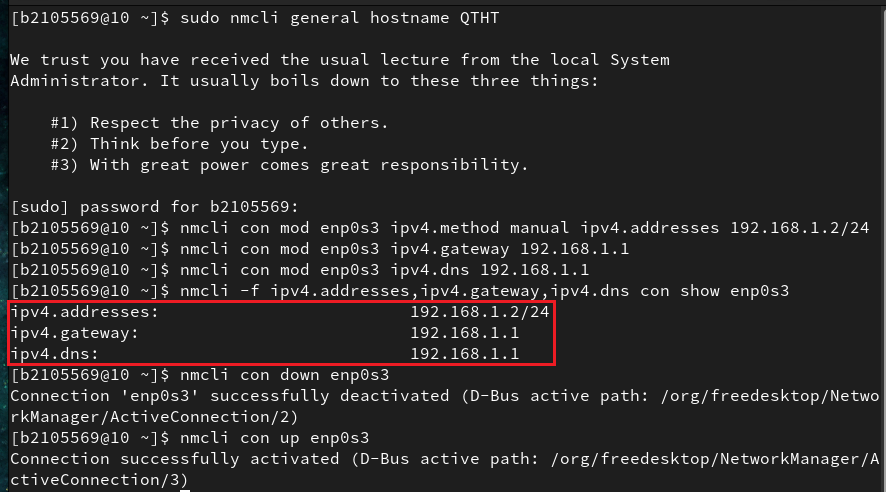
* Full name: Le Truong Ngoc Duyen
* User name: b2105569
* Check vào ô Make this user administrator để cấp quyền quản trị cho tài khoản
* Password

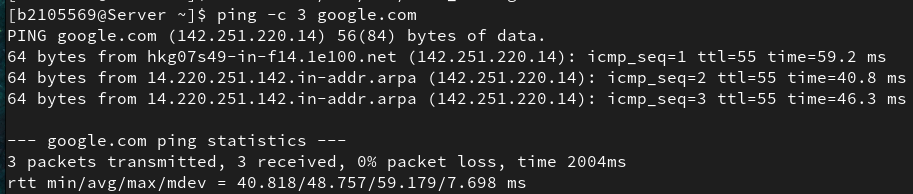
🡺 Chọn Begin Installation

-Sau khi cài đặt xong, chúng ta sẽ đăng nhập vào tài khoản vừa tạo để cấu hình mạng:

* Đổi tên hostname bằng lệnh $sudo nmcli general hostname Server
* Chuyển sang chế độ cấu hình tĩnh và cấu hình địa chỉ IPv4 bằng lệnh $nmcli con mod enp0s3 ipv4.method manual ipv4.addresses 192.168.1.2/24
* Cấu hình Gateway bằng lệnh $nmcli con mod enp0s3 ipv4.gateway 192.168.1.1
* Cấu hình DNS bằng lệnh $nmcli con mod enp0s3 ipv4.dns 192.168.1.1
* Xem lại các thông tin đã cấu hình bằng lệnh $nmcli -f ipv4.addresses,ipv4.gateway,ipv4.dns con show enp0s3
* Cập nhật các thay đổi bằng lệnh $nmcli con down enp0s3 và $nmcli con up enp0s3



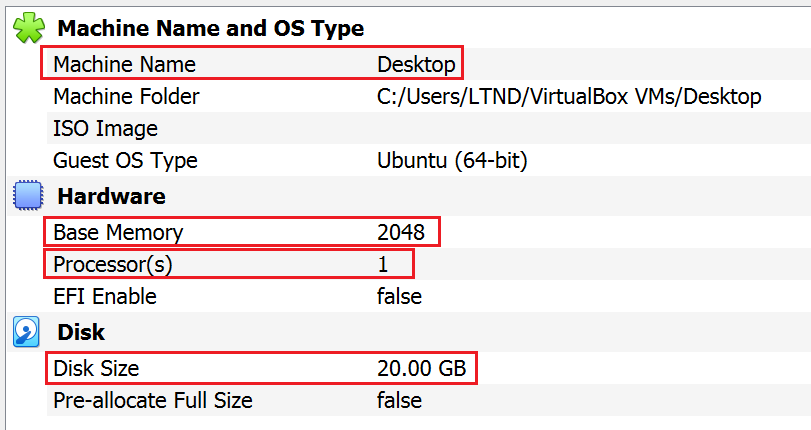
* Kiểm tra kết nối mạng bằng lệnh $ping –c 3 google.com



**\*Tạo máy ảo Desktop:**

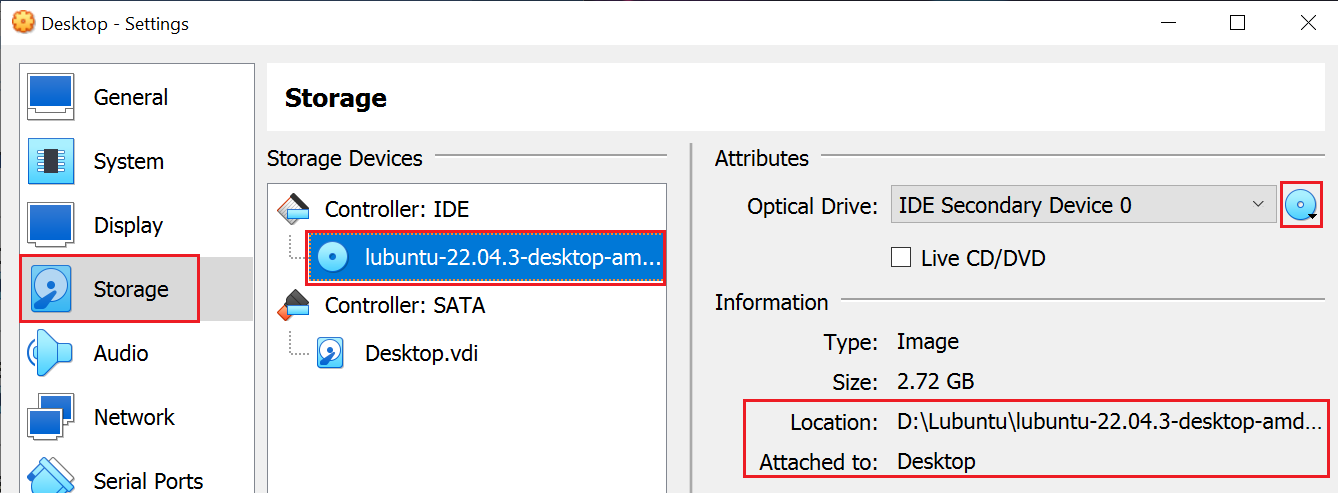
-Chọn New để tạo ra 1 máy ảo

* Name: Desktop
* Base Memory: 2GB ⬄ 2048MB
* Processors: 1 CPU
* Disk Size: 10GB

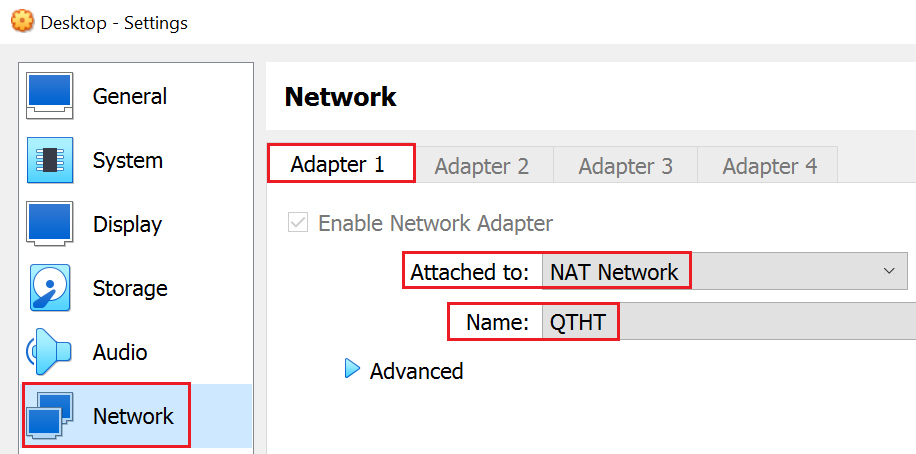


Sau khi tạo xong thì chọn Settings

* Vào Storage 🡪 Chọn file iso Lubuntu đã tải xuống và chọn OK



* Vào NetWork 🡪 Tại Adapter 1, chọn Attached to: NAT Network và Name QTHT

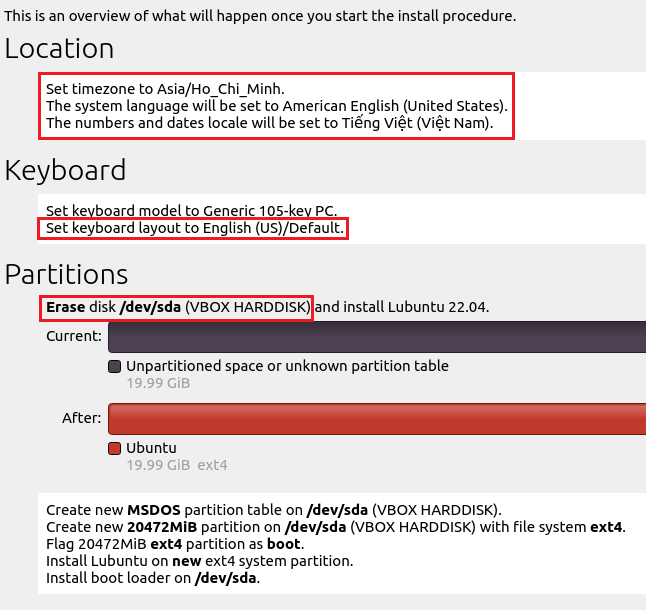


-Tiếp theo, chọn Start để khởi động máy ảo Desktop

-Sau khi khởi động xong, chọn Install Lubuntu 22.04 LTS

* Language: American English
* Location: Asia – Ho Chi Minh
* Keyboard: English (US) - Default
* Partition: Chọn ổ cứng 10GB vừa tạo – Erase disk
* Users: Nami

🡺Chọn Install

-Sau khi cài đặt xong, chúng ta sẽ đăng nhập vào tài khoản vừa tạo để cấu hình mạng:

* Cấu hình động ở **câu 1.6**

**\*Tắt dịch vụ tường lửa trên Server**

-Dùng lệnh $sudo systemctl stop firewalld để tắt dịch vụ tường lửa:



## **CÂU 1.2.**

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

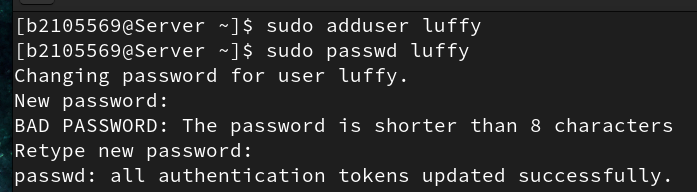
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Họ Tên** | **Nhóm** | **Username** | **Password** | **Mô tả** |
| 1 | Luffy | bangiamdoc | luffy | luffy | Giám đốc |
| 2 | Nami | bangiamdoc | nami | nami | Phó giám đốc |
| 3 | Zoro | banhang | zoro | zoro | Trưởng phòng |
| 4 | Usopp | banhang | usopp | usopp | Nhân viên |
| 5 | Robin | banhang | robin | robin | Nhân viên |
| 6 | Sanji | hanhchanh | sanji | sanji | Trưởng phòng |
| 7 | Chopper | hanhchanh | chopper | chopper | Nhân viên |

**BÀI LÀM**

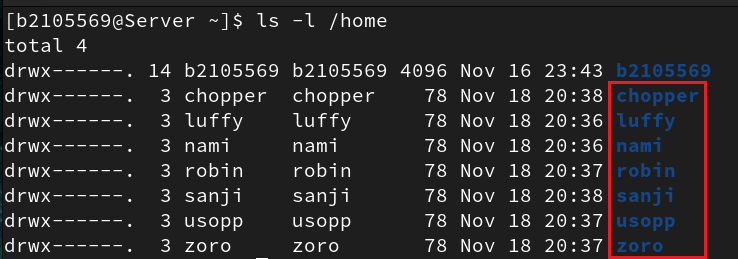
**\*Tạo người dùng (user)**

-Tạo ra user mới với lệnh $sudo adduser <username>

-Đặt mật khẩu cho tài khoản với lệnh $sudo passwd <username>

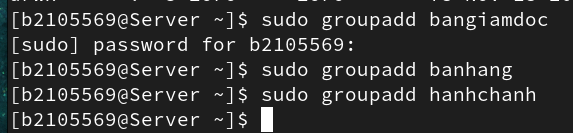


-Dùng lệnh $ls –l /home để xem lại các tài khoản đã được tạo



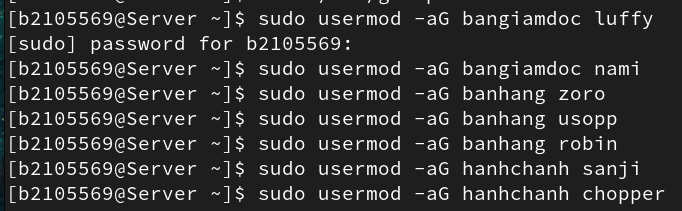
**\*Tạo nhóm người dùng (group)**

-Tạo nhóm mới với lệnh $sudo groupadd <group name>



**\*Thêm người dùng vào nhóm người dùng**

-Thêm tài khoản user vào nhóm nào đó với lệnh $sudo usermod –aG <group name> <username>

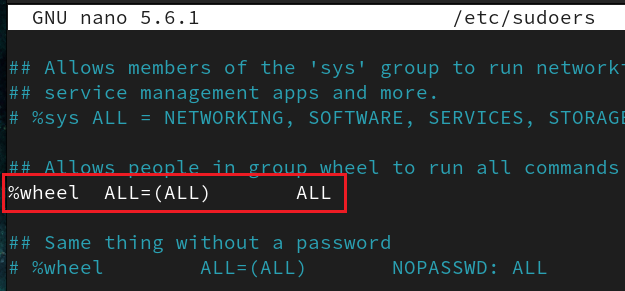


-Dùng lệnh $nano /etc/group mở tập tin group để kiểm tra:



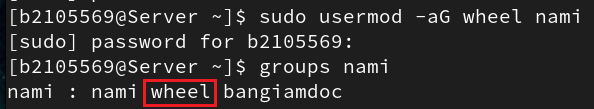
**\*Cấp quyền sudo cho người dùng Nami**

-Dùng lệnh $sudo nano /etc/sudoers để mở tập tin sudoers. Tập tin này dùng để quản lý các quyền sudo trên hệ thống



🡪Cho phép tất cả các người dùng ở trong nhóm wheel thực thi bất kỳ lệnh nào trên hệ thống

🡪Vậy để người dùng nami có quyền sudo thì thêm người dùng nami vào nhóm wheel. Sau đó dùng lệnh $groups <username> để kiểm tra tài khoản thuộc những nhóm nào.



## **CÂU 1.3.**

**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.

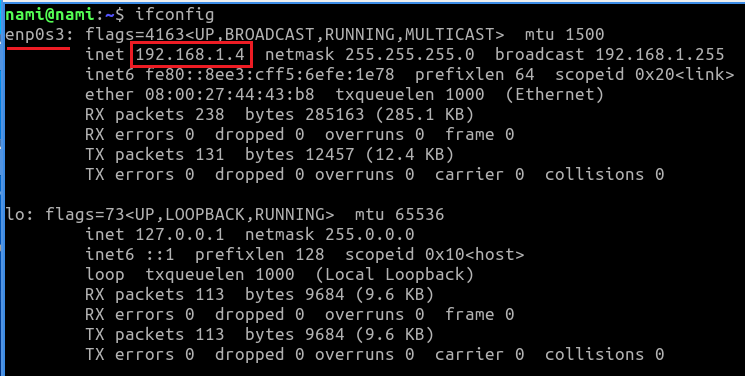
- Chỉ cho phép chứng thực bằng private key, không cho phép chứng thực bằng password. Tạo private/public key cho người dùng <Mã số sinh viên> để có thể SSH tới server.

**BÀI LÀM**

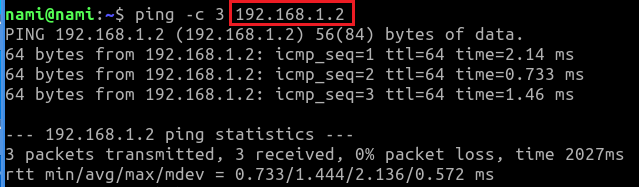
**\*Cài đặt dịch vụ SSH trên Server**

-Kiểm tra kết nối mạng giữa máy Server và máy Desktop:

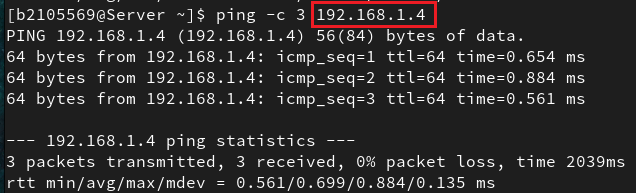
* Dùng lệnh $ifconfig trên máy Desktop để xem địa chỉ IP của máy Desktop:



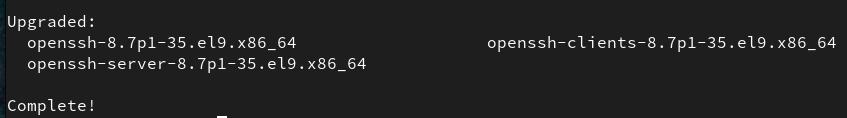
* Dùng lệnh $ping –c 3 192.168.1.2 từ máy Desktop để kiểm tra kết nối mạng đến máy Server



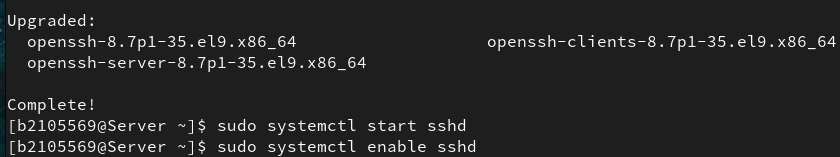
* Dùng lệnh $ping –c 3 192.168.1.2 từ máy Desktop để kiểm tra kết nối mạng đến máy Server



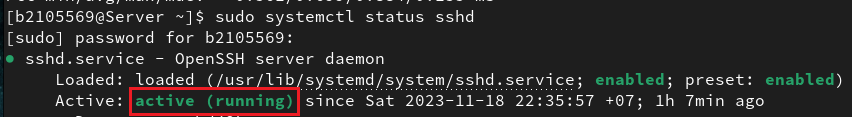
-Cài đặt Open SSH bằng lệnh $sudo dnf install openssh-server –y



-Khởi động và cho phép SSH tự động thực thi khi khởi động hệ điều hành bằng lệnh $sudo systemctl start sshd và $sudo systemctl enable sshd



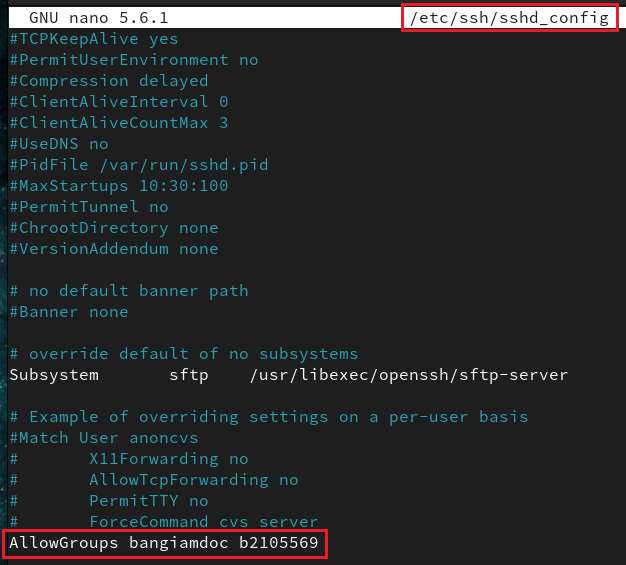
-Kiểm tra xem SSH Server có đang thực thi hay chưa bằng lệnh $sudo systemctl status sshd



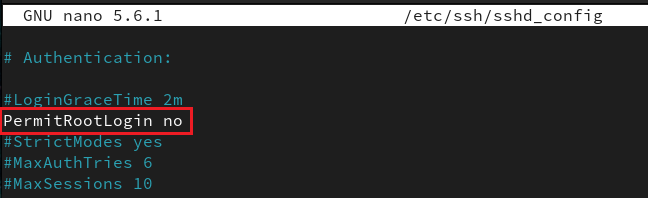
**\*Chỉ có thành viên ban giám đốc và tài khoản <Mã số sinh viên> mới có quyền điều khiển từ xa Server. Tài khoản root không được nối kết tới server từ xa.**

-Dùng lệnh $nano /etc/ssh/sshd\_config để mở tập tin sshd\_config

* Để cho phép chỉ có thành viên ban giám đốc và tài khoản b2105569 mới có quyền điều khiển từ xa Server, thêm vào file dòng AllowGroups bangiamdoc b2105569:

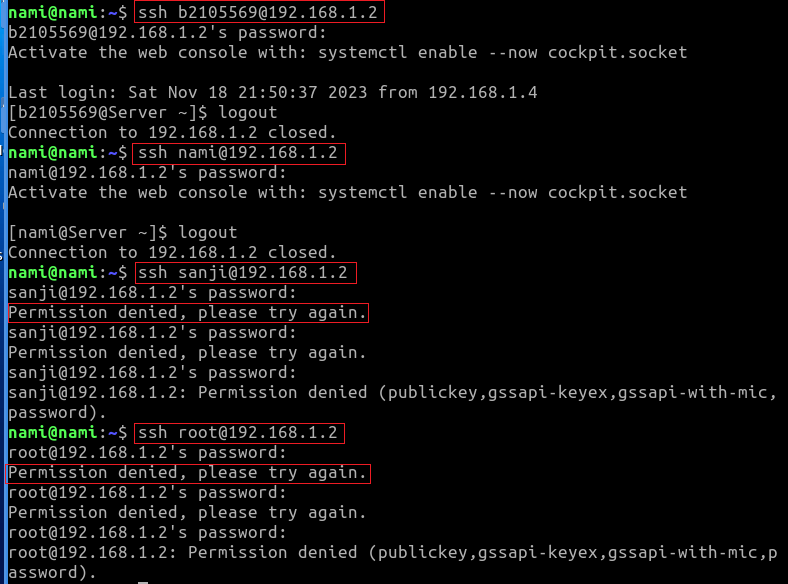


* Để tài khoản root không được nối kết tới server từ xa, thay đổi dòng PermitRootLogin no

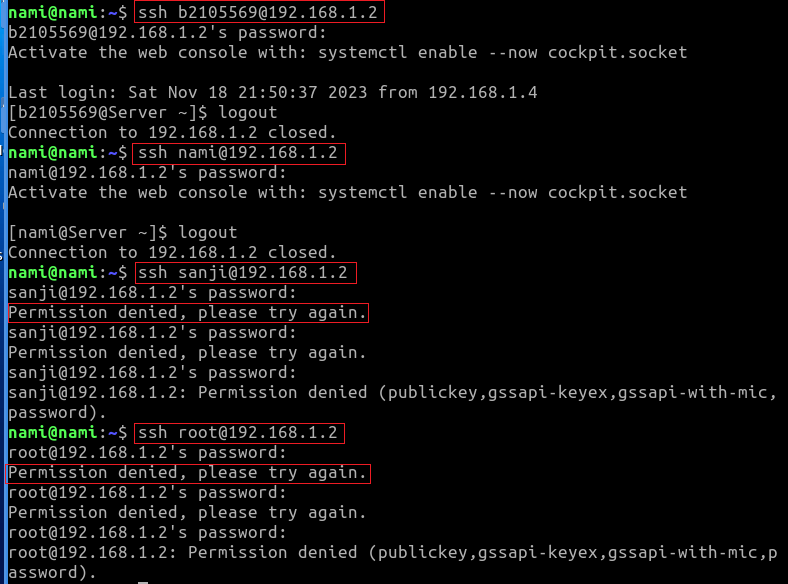


-Kiểm tra trên máy Desktop

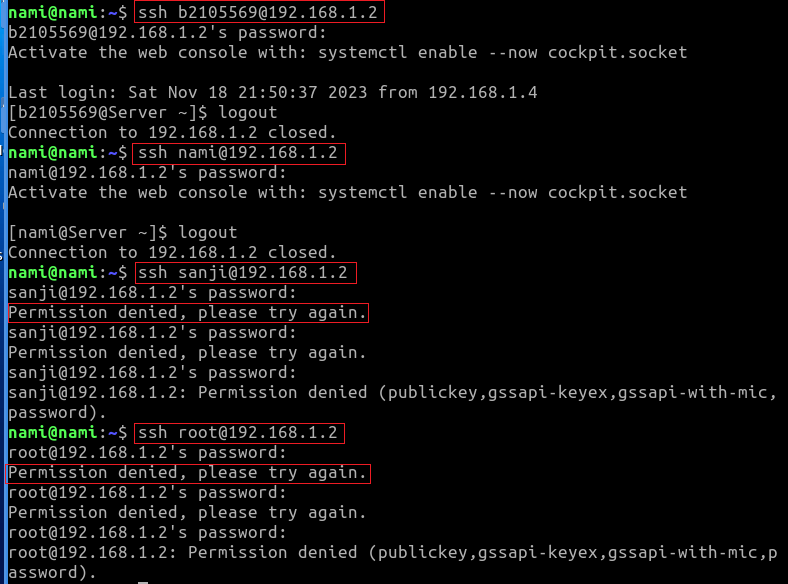
* Để kiểm tra kết nối tới SSH trên Lubuntu này, em dùng lệnh $ssh <username>@<địa chỉ server>
  + Kiểm tra với tài khoản b2105569: 🡺Kết nối thành công



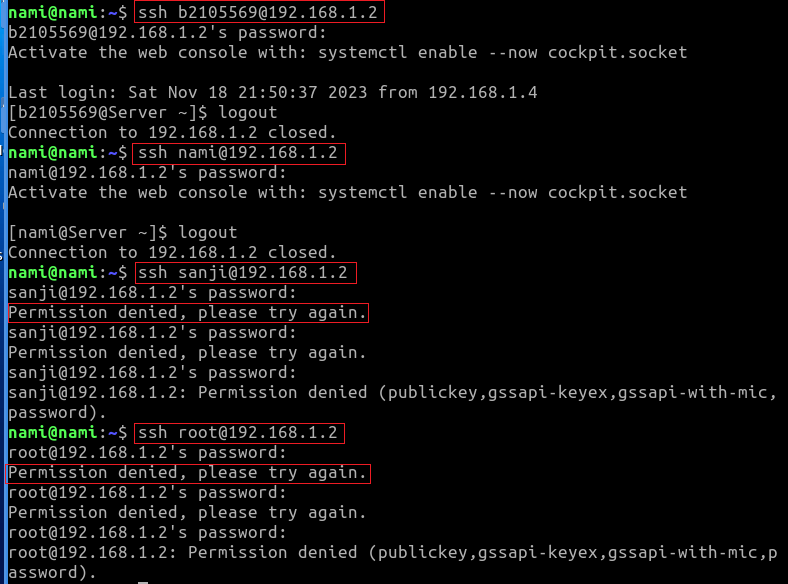
* + Kiểm tra với thành viên trong ban giám đốc, dưới đây em lấy người dùng nami để kiểm tra: 🡺 Kết nối thành công



* + Kiểm tra với tài khoản root: 🡺 Kết nối thất bại



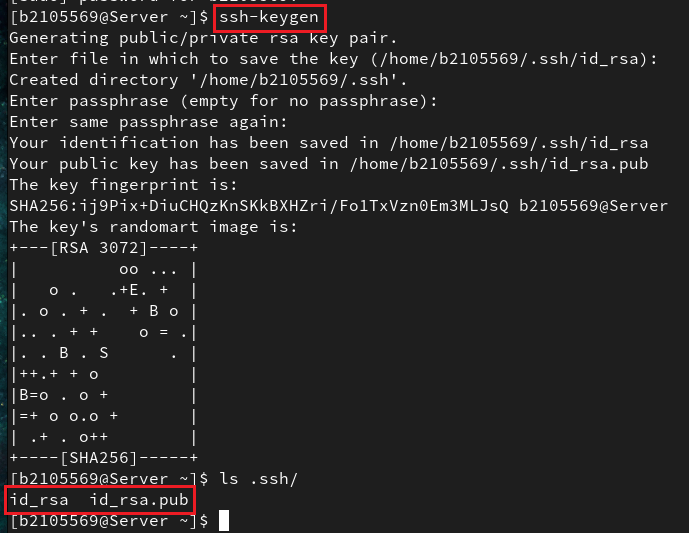
* + Kiểm tra với tài khoản khác, dưới đây em lấy người dùng sanji để kiểm tra (người dùng sanji không thuộc ban giám đốc): 🡺 Kết nối thất bại



**\*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.**

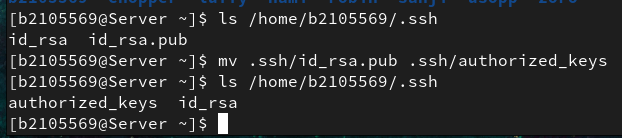
-Tạo private/public keys:

* Để tạo ra cặp khóa dùng lệnh $ssh-keygen, chọn các thông tin mặc định khi được hỏi. Sau khi tạo xong cặp khóa, dùng lệnh $ls .ssh/ thì thấy trong /home/b2105569/.ssh/ sinh ra 2 tập tin id\_rsa và id\_rsa.pub lần lượt là private key và public key:

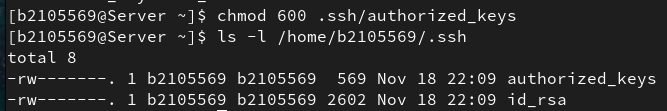


-Cho phép người dùng b2105569 có thể SSH tới Server chỉ với chứng thực bằng private key

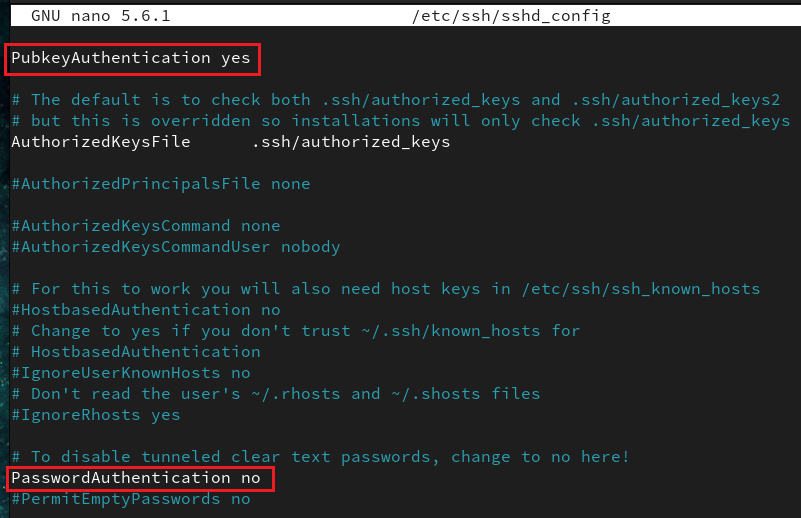
* Di chuyển public key đến vị trí mặc định là .ssh/authorized\_keys bằng lệnh $mv .ssh/id\_rsa.pub .ssh/authorized\_keys



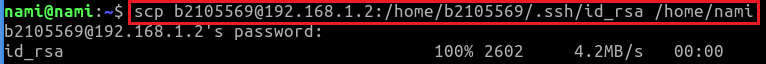
* Phân quyền lại (read, write) cho file chứa public key:



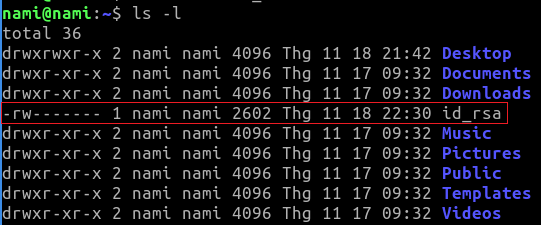
* Dùng lệnh nano mở tập tin /etc/ssh/sshd\_config để tắt chức năng chứng thực bằng password và mở chứng thực bằng public key:
* Thay đổi dòng PubkeyAuthentication yes và dòng PubkeyAuthentication yes



* Trên máy Desktop, dùng lệnh $scp <username>@<địa chỉ server>:</đường dẫn tập tin cần tải xuống> <đường dẫn đích để tải xuống> để download file private key (.ssh/id\_rsa)



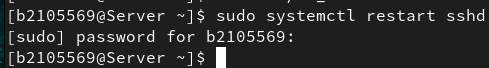
* + Dùng lệnh $ls –l để kiểm tra lại:



* Sau đó, xóa file private key trên máy Server:

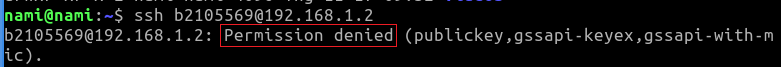


* Khởi động lại SSH Server:

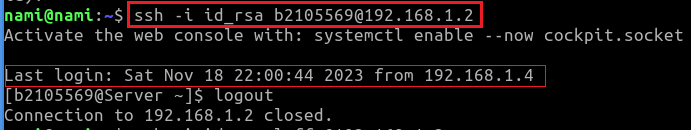


-Kiểm tra kết nối trên máy Desktop

* Nếu tạo kết nối SSH tới máy Server sử dụng chứng thực bằng password thì thì sẽ bị từ chối vì đã tắt chức năng chứng thực bằng mật khẩu:



* Nhưng nếu tạo kết nối SSH tới máy Server sử dụng chứng thực bằng private key bằng lệnh $ssh -i id\_rsa <username>@<địa chỉ server> thì kết nối thành công:



## **CÂU 1.4.**

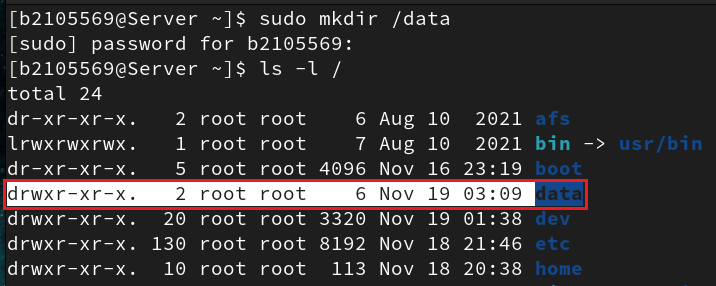
**Tạo thư mục /data trên server và phân quyền sao cho thành viên ban giám đốc có toàn quyền (read, write và execute), các trưởng phòng có quyền read và execute, các nhân viên không có bất cứ quyền gì. Ngoài ra chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên tập tin trong thư mục /data.**

**BÀI LÀM**

**\*Tạo thư mục /data trên server**

-Dùng lệnh $sudo mkdir /data để tạo thư mục /data trên server

-Kiểm tra thư mục /data mới tạo với lệnh $ls –l /



**\*Chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên tập tin trong thư mục /data**

-Đặt sticky bit trên thư mục /data với lệnh $sudo chmod 1750 /data



**\*Phân quyền cho thành viên ban giám đốc có toàn quyền (read, write và execute) trên thư mục /data**

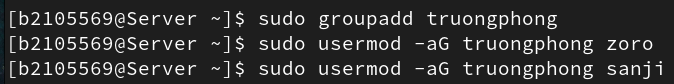
**-**Phân quyền phức tạp cho nhiều nhóm người dùng trên 1 thư mục hay tập tin với kỹ thuật ***ACL (Access Control List)***

-Lệnh $setfacl dùng để thay đổi quyền truy cập của tập tin, thư mục



**\*Phân quyền cho các trưởng phòng có quyền read và execute trên thư mục /data**

-Tạo nhóm truongphong và thêm người dùng zoro và sanji vào nhóm này:

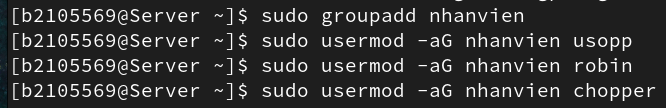


-Phân quyền cho các trưởng phòng có quyền read và execute:



**\*Phân quyền cho các nhân viên không có bất cứ quyền gì trên thư mục /data**

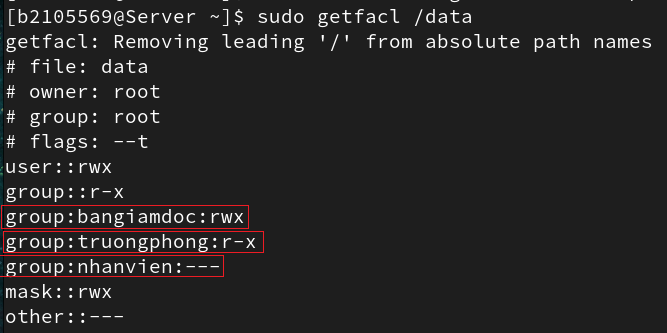
-Tạo nhóm nhanvien và thêm người dùng usopp, robin và choppper vào nhóm này:



-Phân quyền cho các nhân viên không có bất cứ quyền gì trên thư mục /data:



🡺Xem lại các quyền truy cập đầy đủ của thư mục /data với lệnh $sudo getfacl /data:

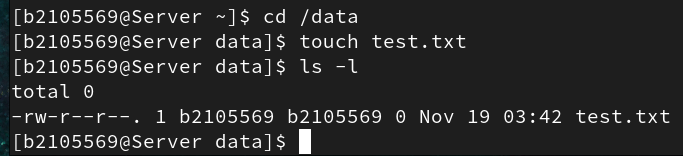


**\*Kiểm tra**

-Thay đổi chủ sở hữu của /data thành b2105569 với lệnh $sudo chown b2105569 /data để thuận tiện cho việc kiểm tra hơn

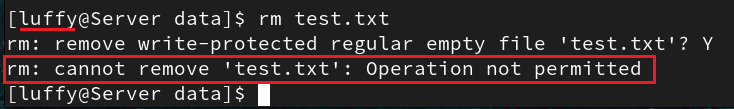


-Tạo 1 file rỗng test.txt trong /data với lệnh $touch test.txt



-Chuyển sang người dùng luffy thuộc nhóm bangiamdoc và thử xóa test.txt

* Chuyển sang người dùng luffy với lệnh $su luffy
* Xóa file test.txt với lệnh $rm test.txt

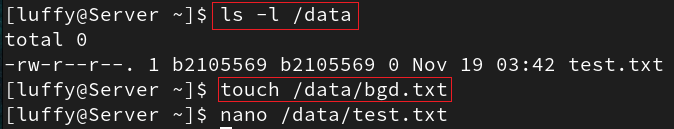


🡺 Mặc dù người dùng luffy thuộc nhóm bangiamdoc có đủ cả 3 quyền read, write và execute trên /data nhưng không thể xóa được file test.txt. Vì chỉ có chủ sở hữu (b2105569) mới có quyền xóa hoặc đổi tên tập tin trong thư mục /data.

**\*Kiểm tra các quyền của bangiamdoc**

-Chuyển qua tài khoản người dùng luffy thuộc bangiamdoc với lệnh $su luffy

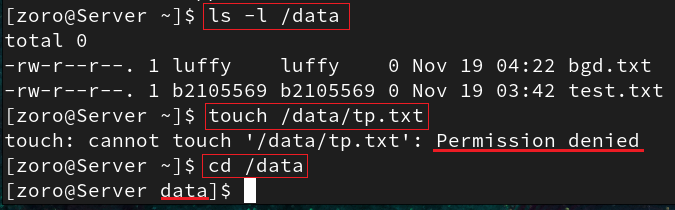
* Quyền read: xem bên trong thư mục /data có gì với lệnh $ls –l /data 🡺 Thành công
* Quyền write: tạo file bgd.txt trong thư mục /data với lệnh touch /data/bgd.txt 🡺 Thành công
* Quyền execute: đi xuyên qua thư mục /data với lệnh $cd /data 🡺 Thành công



**\*Kiểm tra các quyền của truongphong**

-Chuyển qua tài khoản người dùng zoro thuộc truongphong với lệnh $su zoro

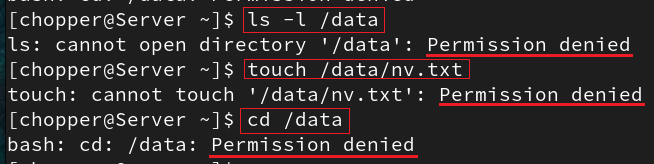
* Quyền read: xem bên trong thư mục /data có gì 🡺 Thành công
* Quyền write: tạo file tp.txt trong thư mục /data 🡺 Thất bại
* Quyền execute: đi xuyên qua thư mục /data 🡺 Thành công



**\*Kiểm tra các quyền của nhanvien**

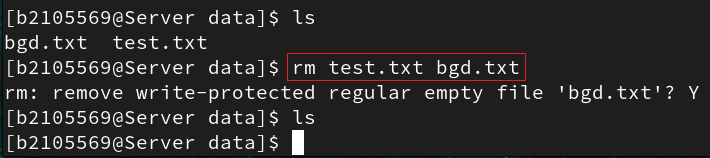
-Chuyển qua tài khoản người dùng chopper thuộc nhanvien với lệnh $su chopper

* Quyền read: xem bên trong thư mục /data có gì 🡺 Thất bại
* Quyền write: tạo file nv.txt trong thư mục /data 🡺 Thất bại
* Quyền execute: đi xuyên qua thư mục /data 🡺 Thất bại



**\*Kiểm tra người dùng b2105569**

-Xóa tất cả các file trong data 🡺 Thành công vì chỉ có duy nhất người dùng b2105569 mới có quyền xóa hoặc đổi tên tập tin trong thư mục /data



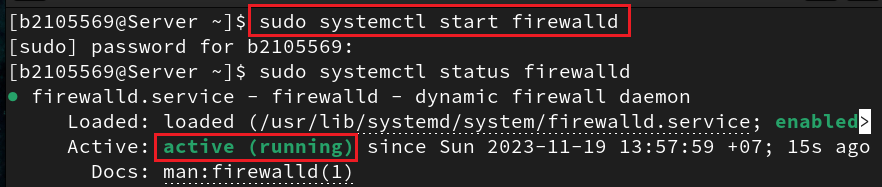
## **CÂU 1.5.**

**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.

**BÀI LÀM**

**\*Khởi động tường lửa**

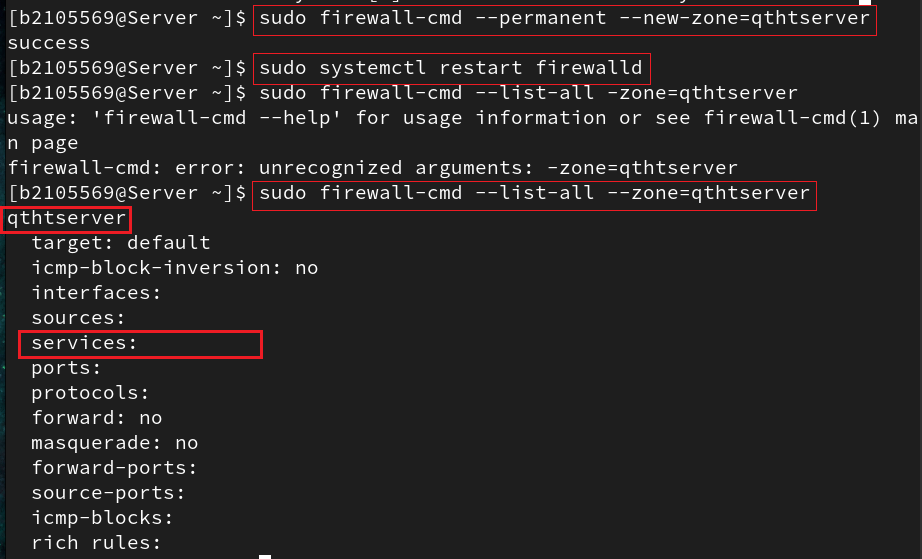


**\*Tạo zone mới có tên qthtserver**

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

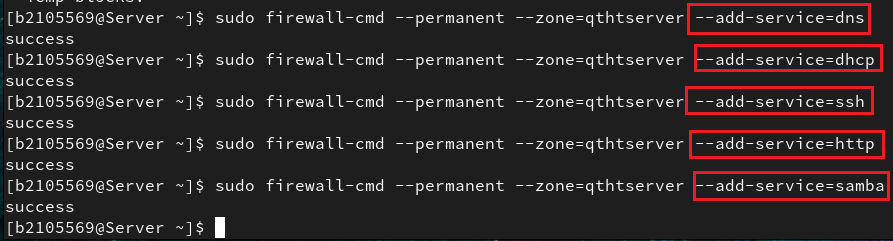
-$sudo systemctl restart firewalld

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

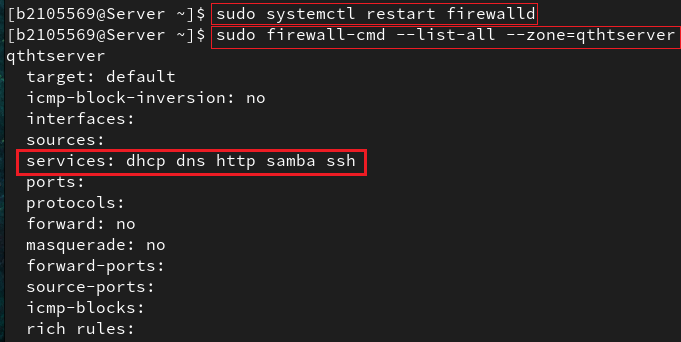


**\*Cho phép các dịch vụ DNS, DHCP, SSH, Web, SAMBA hoạt động trên zone qthtserver**

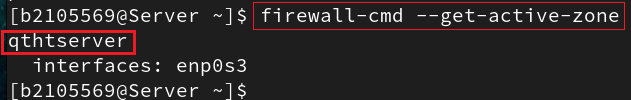
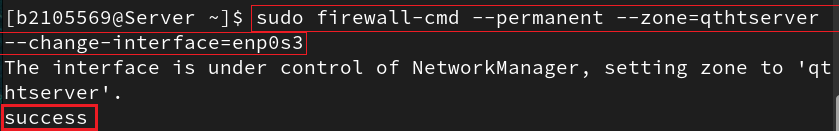
-Lệnh $sudo firewall-cmd –permanent --zone=<tên zone> --add-service=<tên dịch vụ> : cho phép dịch vụ hoạt động trên zone



**\*** **Khởi động lại tường lửa và kiểm tra các dịch vụ đã thêm vào zone chưa**

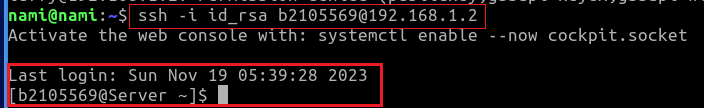


**\*** **Đổi qua zone mới tạo (qthtserver) và kiểm tra zone nào đang hoạt động**



**\*Kiểm tra**

-Thử SSH bên máy Desktop



🡺 Kết nối SSH tới máy Server thành công

## **CÂU 1.6.**

**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

**BÀI LÀM**

**\*** **Cài đặt dịch vụ DHCP trên Server**

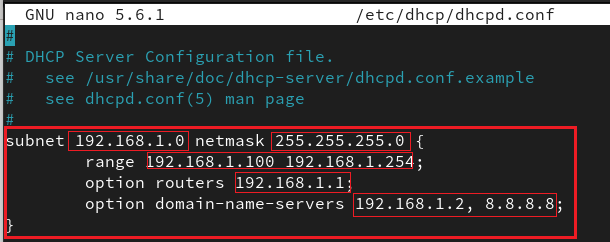
-Dùng lệnh $sudo dnf install dhcp-server -y



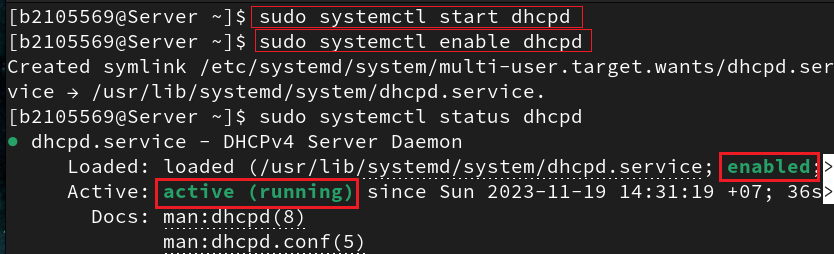
**\*Cấu hình dịch vụ DHCP**

-Dùng lệnh $sudo nano /etc/dhcp/dhcpd.conf

* Địa chỉ mạng 192.168.1.0
* Netmask 255.255.255.0 (/24)
* Địa chỉIP của Desktop có có range từ 192.168.1.100 đến 192.168.1.254
* Địa chỉ gateway: 192.168.1.1
* DNS server: 192.168.1.2 và 8.8.8.8



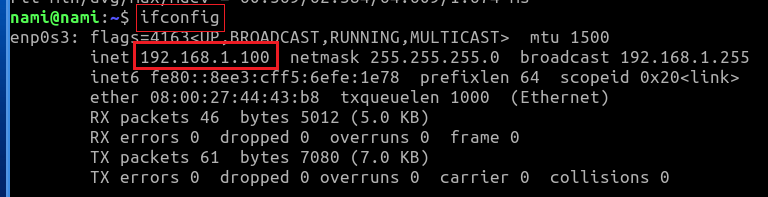
**\*Khởi động và cho phép dịch vụ DHCP tự động thực thi khi khởi động hệ điều hành:**



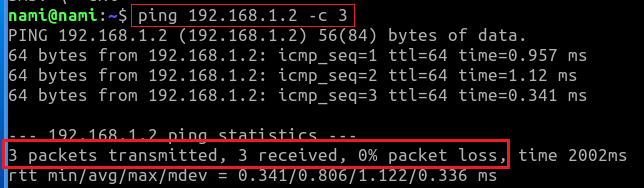
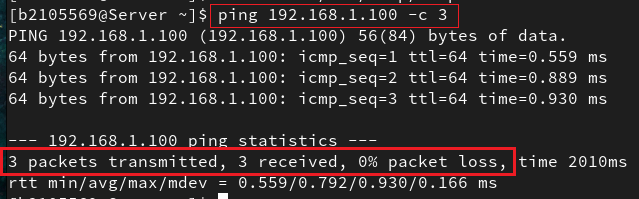
**\*** **Kiểm tra**

-Khởi động lại dịch vụ mạng trên máy Desktop với lệnh $systemctl restart NetworkManager

-Kiểm tra cấu hình mạng của Desktop với lệnh $ifconfig



-Kiểm tra nối kết từ máy Server đến Desktop và ngược lại với lệnh $ping <địa chỉ IP của máy kia> -c 3



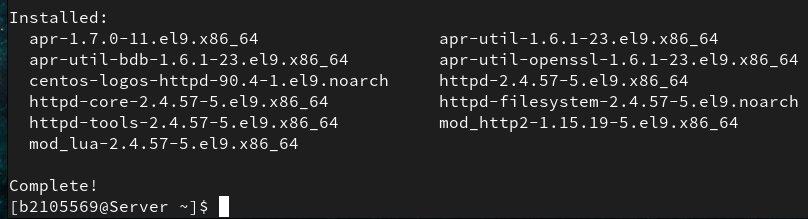
## **CÂU 1.7.**

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

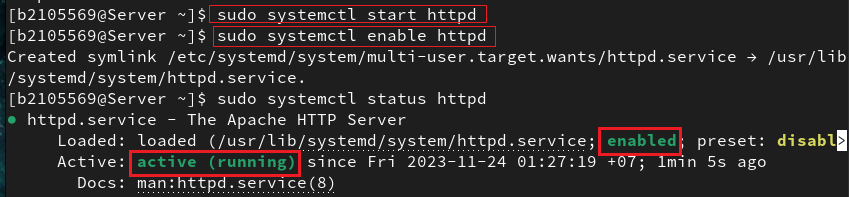
**BÀI LÀM**

**\*Cài đặt Apache web serever**

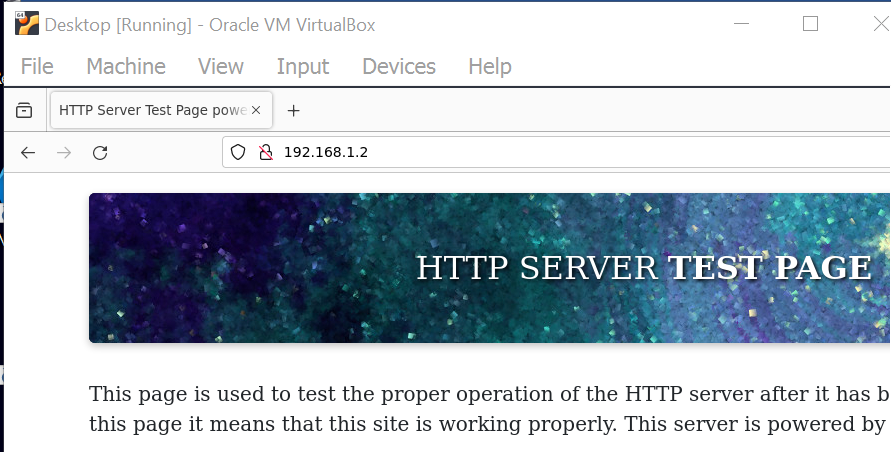
-Dùng lệnh $sudo dnf –y install httpd



-Khởi động và cho phép Apache tự động thực thi khi khởi hành hệ điều hành



- Trên máy Desktop, mở trình duyệt web và truy cập vào địa chỉ http://192.168.1.2 để kiểm tra



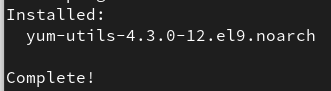
**\*** **Gỡ bỏ PodMan *(do sẽ đụng độ với Docker)***

-Dùng lệnh $sudo dnf -y remove podman runc



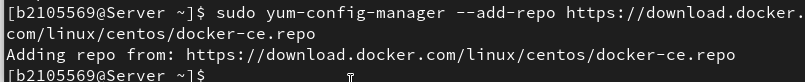
**\*Cài đặt công cụ yum-utils**

-Dùng lệnh $sudo dnf install -y yum-utils



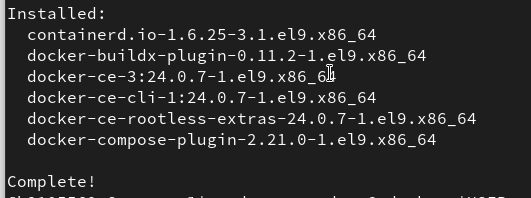
-Thêm địa repo của Docker vào công cụ yum

$sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo



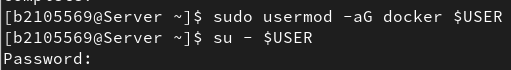
**\*Cài đặt Docker**

-Dùng lệnh $sudo dnf install docker-ce -y



- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà ko cần quyền sudo với lệnh $sudo usermod –aG docker $USER

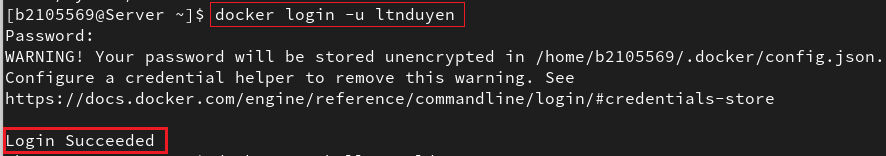
-Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng với lệnh $su - $USER



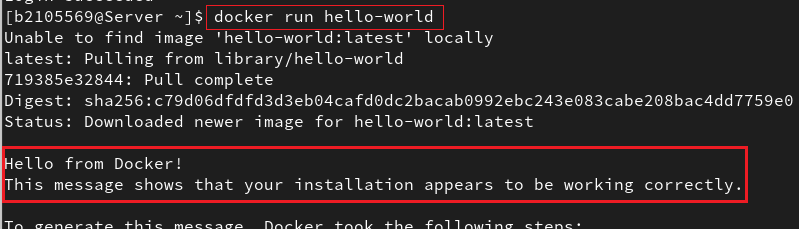
-Khởi động và cho phép dịch vụ Docker thực thi khi khởi động hệ điều hành



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

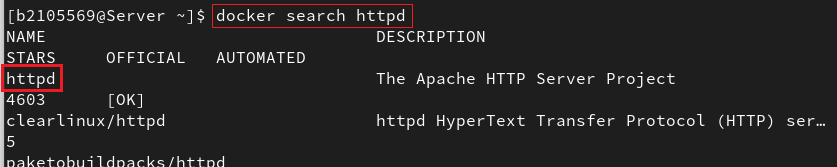


-Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.



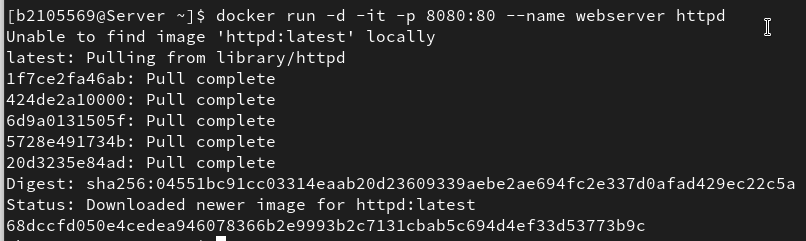
**\*Triển khai dịch vụ web server lên máy ảo CentOS 9 sử dụng một Docker container**

-Dùng lệnh $docker search httpd để tìm kiếm image với từ khóa httpd, kết quả sẽ thấy 1 image tên httpd ở dòng đầu tiên.

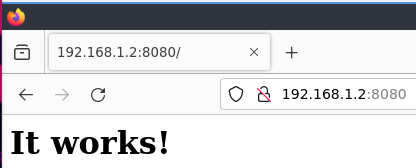


- Tạo container từ image httpd với lệnh $docker run -d -it -p 8080:80 --name webserver httpd

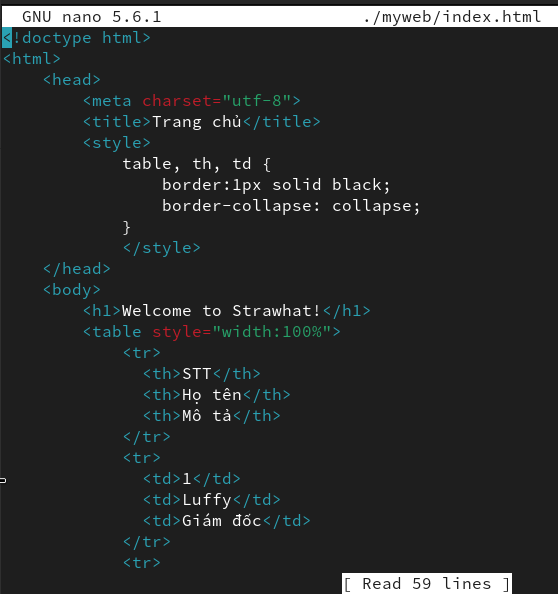
* -d: chạy container ở chế độ background
* -it: tạo shell để tương tác với container
* --name webserver: đặt tên container là webserver
* -p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container



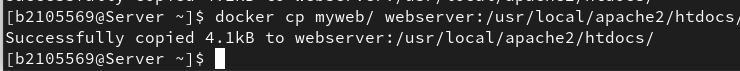
-Kiểm tra bằng cách dùng máy Desktop truy cập đến cổng 8080 của máy Server.



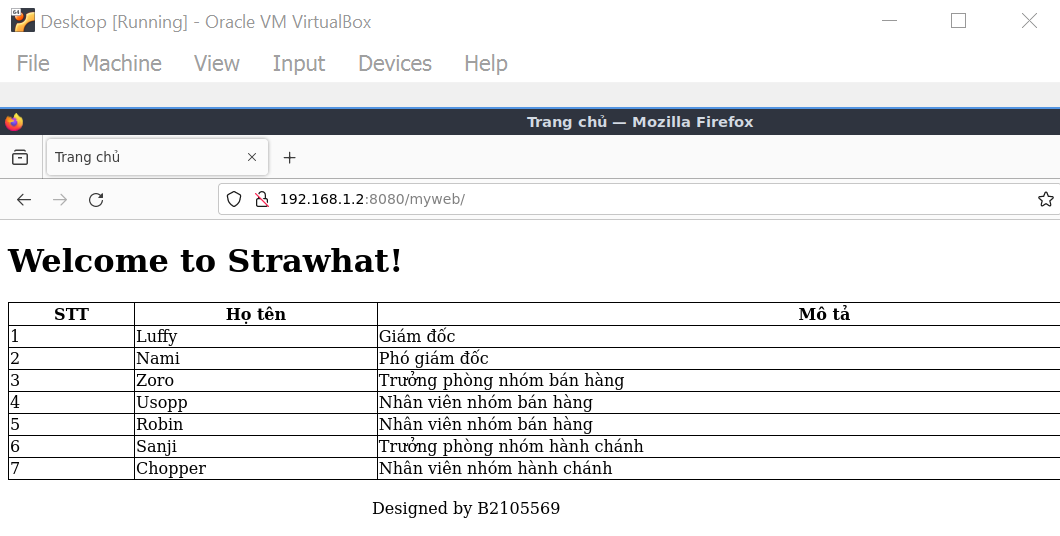
-Tạo thư mục ./myweb và tạo file ./myweb/index.html với nội dung trang chủ giới thiệu về các thành viên trong công ty.



-Sao chép thư mục /myweb vào thư mục gốc của dịch vụ của web trên Docker container với lệnh $docker cp myweb/ webserver:/usr/local/apache2/htdocs/



**\*Kiểm tra trên máy Desktop:**



## **CÂU 1.8.**

**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.

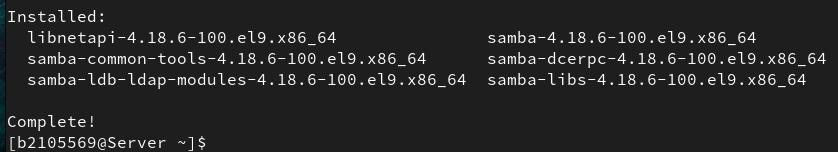
- Tất cả người dùng có thể truy cập vào thư mục cá nhân của họ (/home/<username>) trên Server.

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

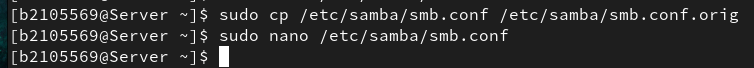
**BÀI LÀM**

**\*Cài đặt dịch vụ SAMBA**

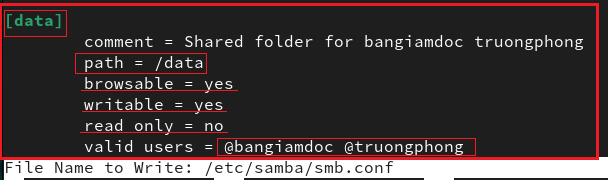
-Dùng lệnh $sudo dnf install –y samba



**\*Cấu hình dịch vụ SAMBA để thành viên ban giám đốc và trưởng phòng có thể truy cập vào thư mục /data trên Server.**



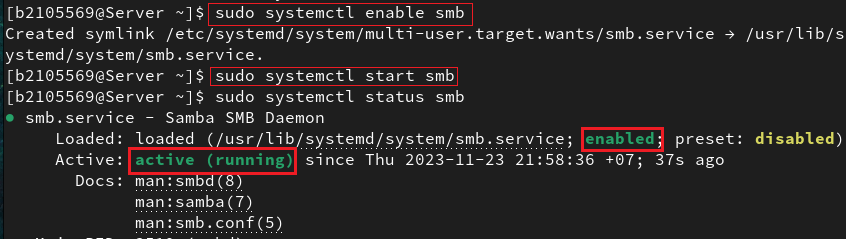
-Thêm đoạn cấu hình vào cuối file /etc/samba/smb.conf:



-Cấu hình SELINUX cho phép SAMBA với 2 lệnh:

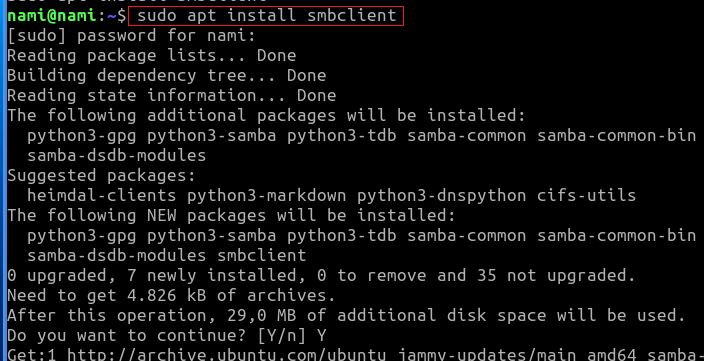


-Khởi động và cho phép dịch vụ SAMBA tự động thực thi khi khởi động hệ điều hành



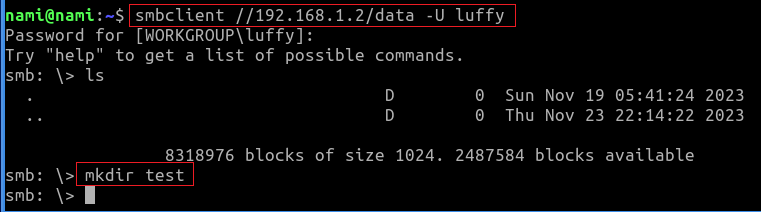
**\*Kiểm tra trên máy Desktop**

-Cài SAMBA vào máy Desktop với lệnh $sudo apt install smbclient

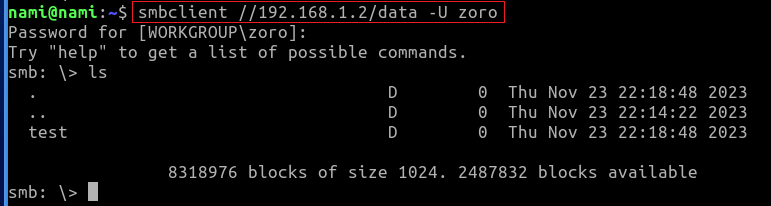


-Kết nối SAMBA thành công từ máy Desktop đến máy Server và vào thư mục /data bằng tài khoản luffy (thuộc bangiamdoc) với lệnh $smbclient //192.168.1.2/data –U luffy

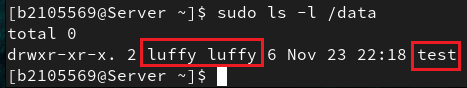
* Thử tạo thư mục test trong /data



-Kết nối SAMBA thành công từ máy Desktop đến máy Server và vào thư mục /data bằng tài khoản zoro thuộc truongphong với lệnh $smbclient //192.168.1.2/data –U zoro

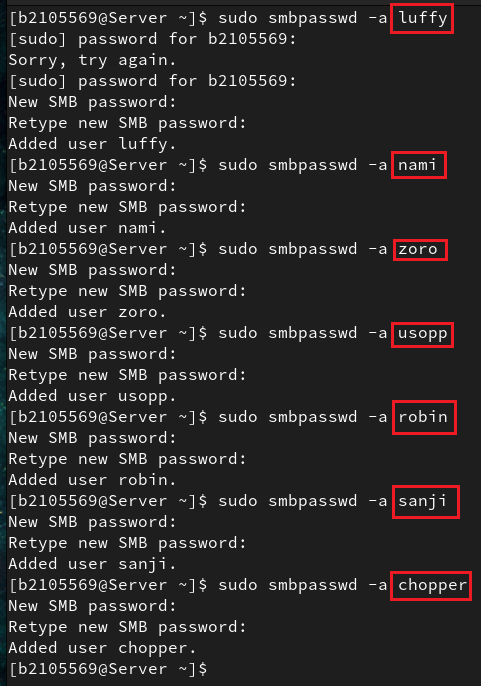


-Bên máy Server, kiểm tra trong /data có thư mục test do luffy vừa tạo không bằng lệnh $sudo ls –l /data

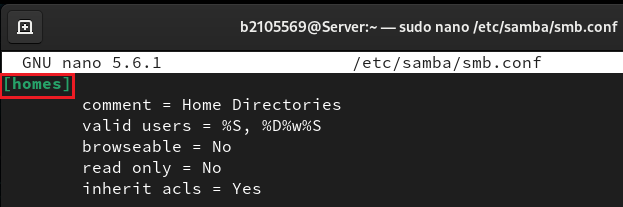


**\*Cấu hình dịch vụ SAMBA để tất cả người dùng có thể truy cập vào thư mục cá nhân của họ (/home/<username>) trên Server.**

-Thêm tất cả người dùng cho dịch vụ Samba với lệnh $sudo smbpasswd –a <người dùng>



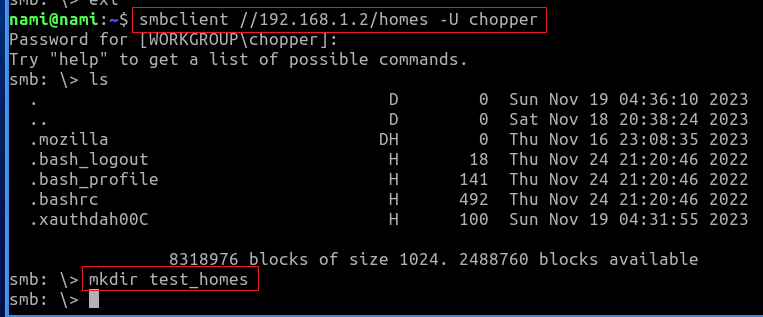
-Trong file /etc/samba/smb.conf đã có cấu hình sẵn cho phép tất cả người dùng có thể truy cập vào thư mục cá nhân:



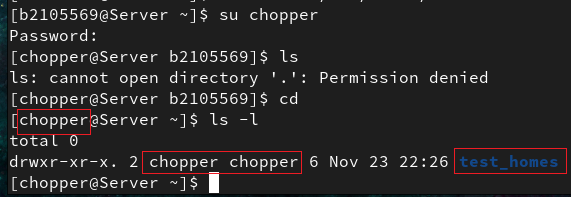
**\*Kiểm tra trên máy Desktop**

-Kết nối SAMBA thành công từ máy Desktop đến máy Server và vào thư mục /homes bằng tài khoản bất kỳ với lệnh $smbclient //192.168.1.2/homes –U chopper

* Tạo thư mục test\_homes trong thư mục cá nhân bằng người dùng chopper



-Bên máy Server, chuyển sang người dùng chopper với lệnh $su chopper và kiểm tra trong /home/chopper có thư mục test\_homes vừa tạo hay không



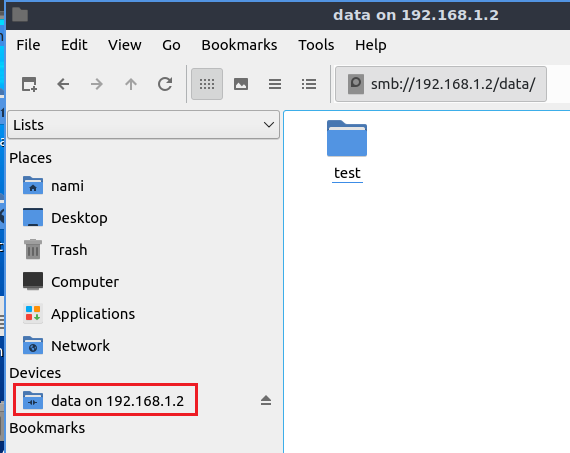
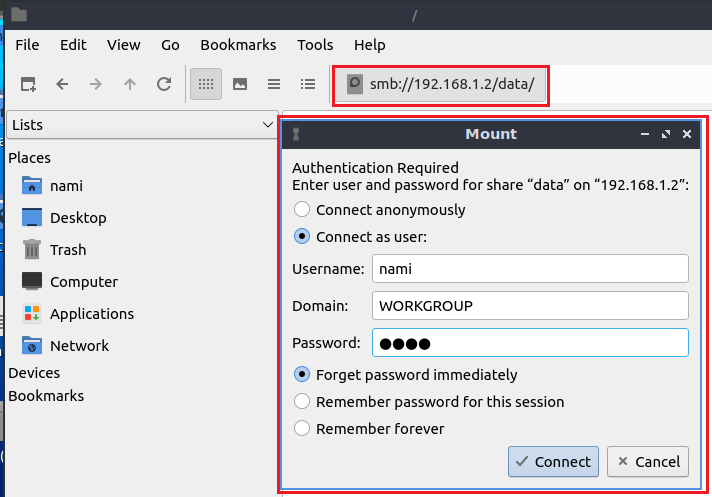
**\*Trên Desktop tạo ổ cứng ảo nối kết tới dịch vụ SAMBA trên Server.**

-Mở Computer trên máy Desktop 🡪 Nhập trên thanh tìm kiếm smb://192.168.1.2/data/

-Tiếp theo sẽ hiện ra hộp thoại:

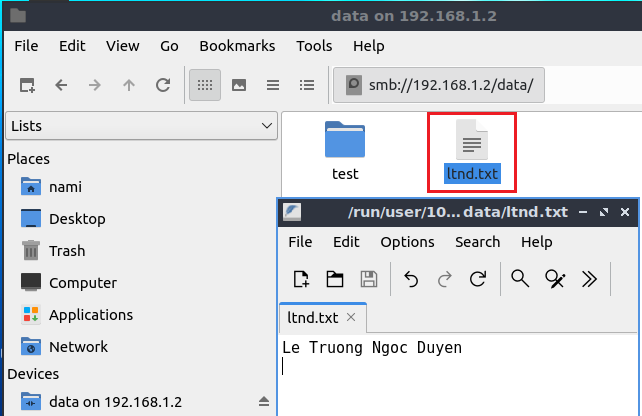
* Chọn Connect as user
* Username: nhập 1 người dùng bất kỳ mà đã thêm vào SAMBA
* Domain: WORKGROUP
* Password: nhập mật khẩu Samba tương ứng với người dùng

🡺Chọn Connect

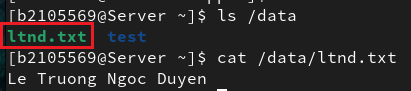


**\*Kiểm tra**

-Tạo 1 tập tin văn bản mới trong ổ ảo của thư mục data:



-Quay lại với máy Server để kiểm tra xem tập tin ltnd.txt vừa tạo trên Desktop có không:



## **CÂU 1.9.**

**Cài đặt và cấu hình dịch vụ DNS trên Server để phân giải tên miền strawhat.com**

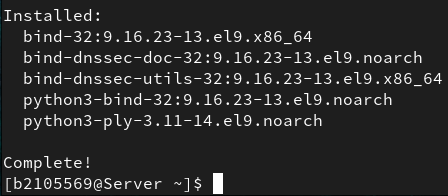
Tên miền: *www.strawhat.com* <----> IP: 192.168.1.2 (Server IP)

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

**BÀI LÀM**

**\*Cài đặt bind và các công cụ cần thiết**

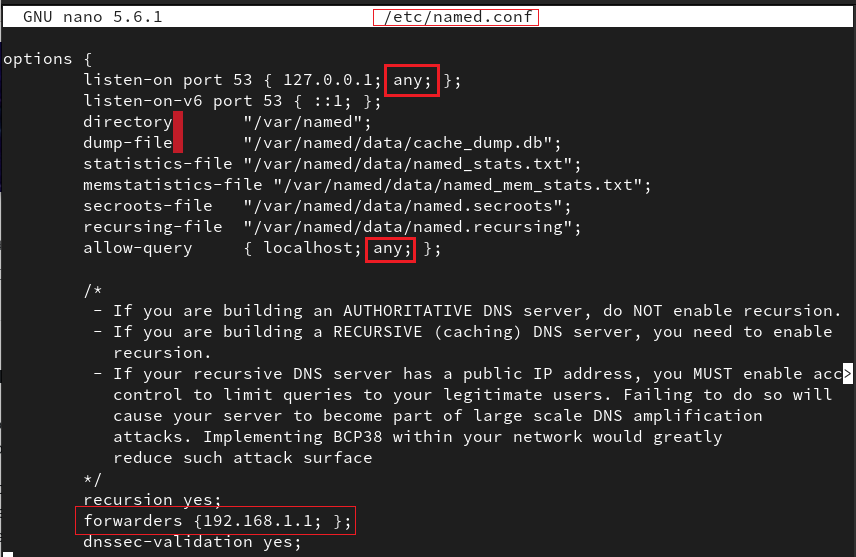
-Dùng lệnh $sudo dnf install bind bind-utils –y



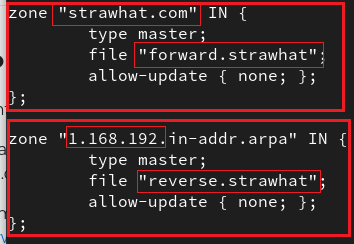
**\*Cấu hình DNS server**

-Dùng lệnh $sudo nano /etc/named.conf

* Thêm any vào listen-on port 53 để có thể lắng nghe từ mọi IP
* Thêm any vào allow-query để cho phép truy vấn từ mọi IP
* Thêm forwarders {192.168.1.1};



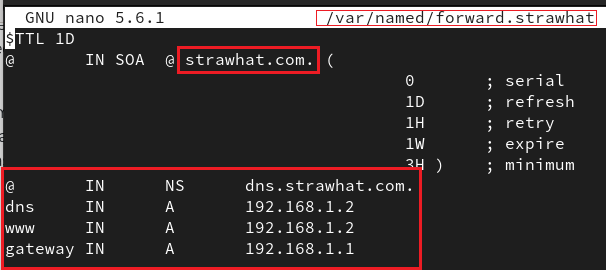
* Phân giải xuôi với forward.strawhat
* Phân giải ngược với reverse.strawhat



**\*Tạo tập tin cấu hình phân giải xuôi:**



-Mở tập tin phân giải xuôi với lệnh $sudo nano /var/named/forward.strawhat



**\*Tạo tập tin cấu hình phân giải ngược:**



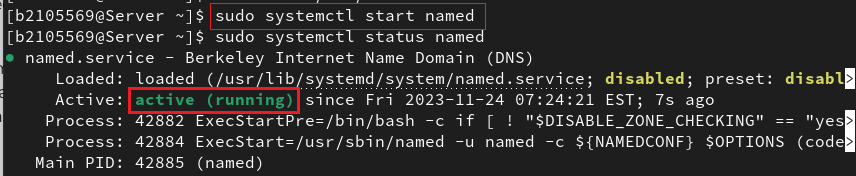
-Mở tập tin phân giải ngược với lệnh $sudo nano /var/named/reverse.strawhat



**\*Chạy dịch vụ DNS**

- Tắt tường lửa $sudo systemctl stop firewalld

-Khởi động dịch vụ DNS với lệnh $sudo systemctl start named



**\*Kiểm tra**

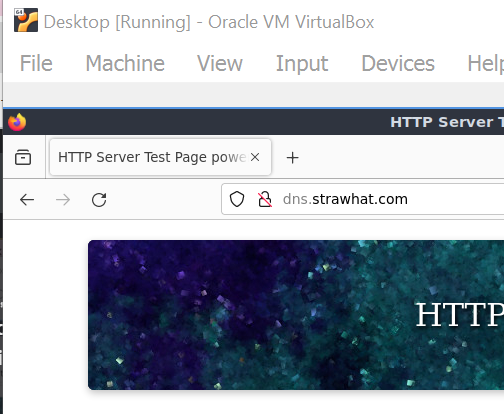
-Kiểm tra phân giải xuôi với lệnh $nslookup



-Kiểm tra phân giải ngược với lệnh $nslookup



-Kiểm tra trên máy Desktop



## **CÂU 1.10.**

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

+ Các thư mục cần sao lưu sao lưu: /home, /data, /etc

+ Nơi lưu dữ liệu sao lưu: /mnt/backup

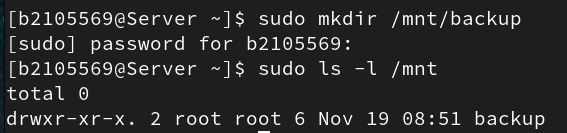
- Sao lưu mỗi ngày: thực hiện vào lúc 23:59 từ thứ 2 đến thứ 7, dữ liệu sẽ được nén lại và lưu với tên như sau: backup\_<thứ> (ví dụ: backup\_monday).

- 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.

**BÀI LÀM**

**\*Tạo nơi lưu dữ liệu sao lưu: /mnt/backup**

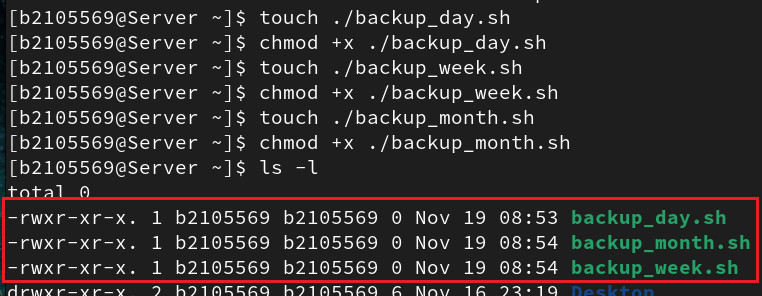


**\*Tạo 3 shell script sao lưu**

-Tạo 3 shell script rỗng ./backup\_day.sh, ./backup\_week.sh và ./backup\_month.sh tương ứng sao lưu ngày, sao lưu tuần và sao lưu tháng với lệnh $touch <file>

-Cấp quyền thực thi (execute) cho chúng để chạy trực tiếp mà không cần lệnh bash với lệnh $chmod +x <file>

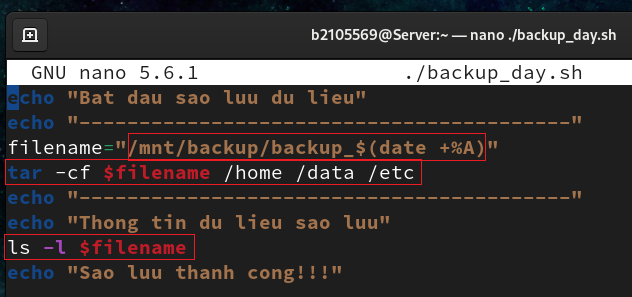
-Dùng lệnh $ls –l để kiểm tra



**\*Tập tin sao lưu backup\_day.sh**

-Dùng lệnh $nano ./backup\_day.sh để mở tập tin lên. Trong đó:

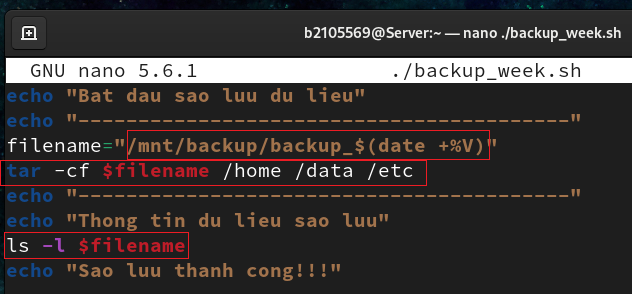
* date +%A để lấy thứ trong tuần *(Sunday, Monday, ...)*
* Lệnh $tar –cf $filename /home /data /etc : nén toàn bộ thư mục /home, /data và /etc thành tập tin /mnt/backup/backup\_<thứ>
* In thông tin đầy đủ của tập tin /mnt/backup/backup\_<thứ> với lệnh $ls –l $filename
* In ra thông báo “Sao lưu thành công!!!”



**\*Tập tin sao lưu backup\_week.sh**

-Dùng lệnh $nano ./backup\_week.sh để mở tập tin lên. Trong đó:

* date +%V để lấy thứ tự tuần trong năm *(01, 02, ..., 52, 53)*
* Lệnh $tar –cf $filename /home /data /etc : nén toàn bộ thư mục /home, /data và /etc thành tập tin /mnt/backup/backup\_<thứ tự tuần>
* In thông tin đầy đủ của tập tin /mnt/backup/backup\_<thứ tự tuần> với lệnh $ls –l $filename
* In ra thông báo “Sao lưu thành công!!!”



**\*Tập tin sao lưu backup\_month.sh**

-Dùng lệnh $nano ./backup\_month.sh để mở tập tin lên. Trong đó:

* date +%m để lấy tháng trong năm *(01, 02, ..., 11, 12)*
* Lệnh $tar –cf $filename /home /data /etc : nén toàn bộ thư mục /home, /data và /etc thành tập tin /mnt/backup/backup\_<thứ tự tuần>
* In thông tin đầy đủ của tập tin /mnt/backup/backup\_<thứ tự tuần> với lệnh $ls –l $filename
* In ra thông báo “Sao lưu thành công!!!”

-------------------- Hết --------------------