**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC CẦN THƠ**

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

**KHOA KHOA HỌC MÁY TÍNH**

**🙞 🕮 🙜**



**MINI PROJECT**

**HỌC PHẦN: QUẢN TRỊ HỆ THỐNG**

**MÃ HỌC PHẦN: CT179**

**ĐỀ TÀI**

**BÀI TẬP TỔNG HỢP CUỐI KỲ**

|  |
| --- |
| **Sinh viên thực hiện** |
| **Họ tên: Lê Tuấn Đạt**  **MSSV: B2113328**  **Nhóm: 06** |

**Cần Thơ, ngày 31 tháng 10 năm 2024**

**MỤC LỤC**

**[MÔ TẢ BÀI TẬP TỔNG HỢP: 1](#_Toc18644)**

**[1. Sử dụng phần mềm VirtualBox để: 2](#_Toc18222)**

**[2. Tạo các nhóm người dùng (group) và người dùng (user) trên Server 15](#_Toc26525)**

**[3. Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server 18](#_Toc4492)**

**[4. Phân quyền truy cập: 25](#_Toc6392)**

**[5. Cài đặt và cấu hình tường lửa trên Server: 30](#_Toc15929)**

**[6. Cài đặt và cấu hình dịch vụ DHCP trên Server: 32](#_Toc31320)**

**[7. Cài đặt và cấu hình dịch vụ máy chủ Web trên Server sử dụng Docker 35](#_Toc26375)**

**[8. Cài đặt và cấu hình dịch vụ SAMBA trên Server. Cấu hình chỉ cho phép: 41](#_Toc4039)**

**[9. Cài đặt và cấu hình dịch vụ DNS trên Server để phân giải tên miền lautamquoc.com 47](#_Toc4944)**

**[10. Sử dụng dịch vụ cron và shell script tự động 52](#_Toc28873)**

# MÔ TẢ BÀI TẬP TỔNG HỢP:

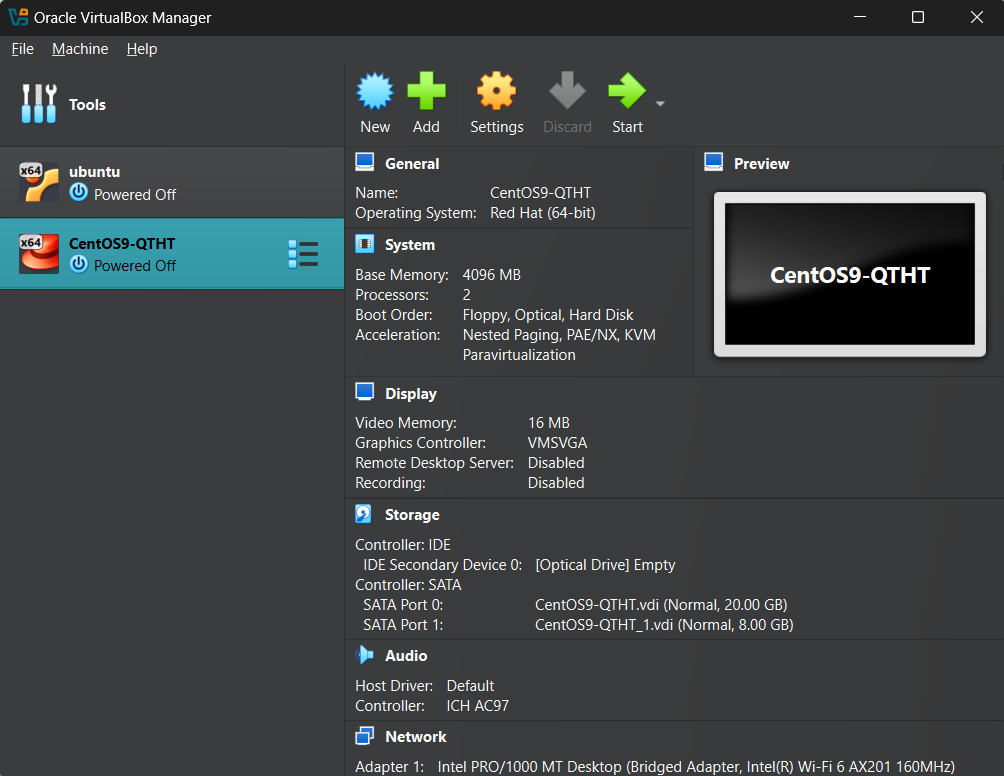
Công ty Tam Quốc chuyên kinh doanh buffet lẩu cay Tứ Xuyên có nhu cầu cài đặt các dịch vụ mạng phục vụ cho công việc của công ty như sau:

# 

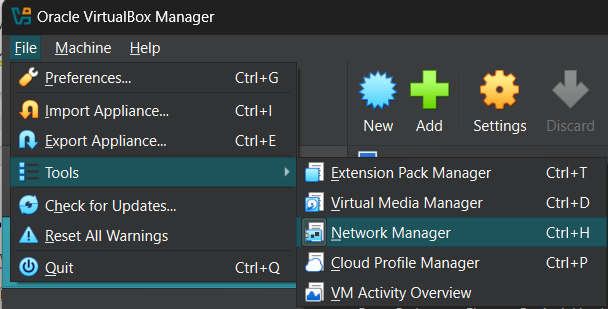
# Sử dụng phần mềm VirtualBox để:

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

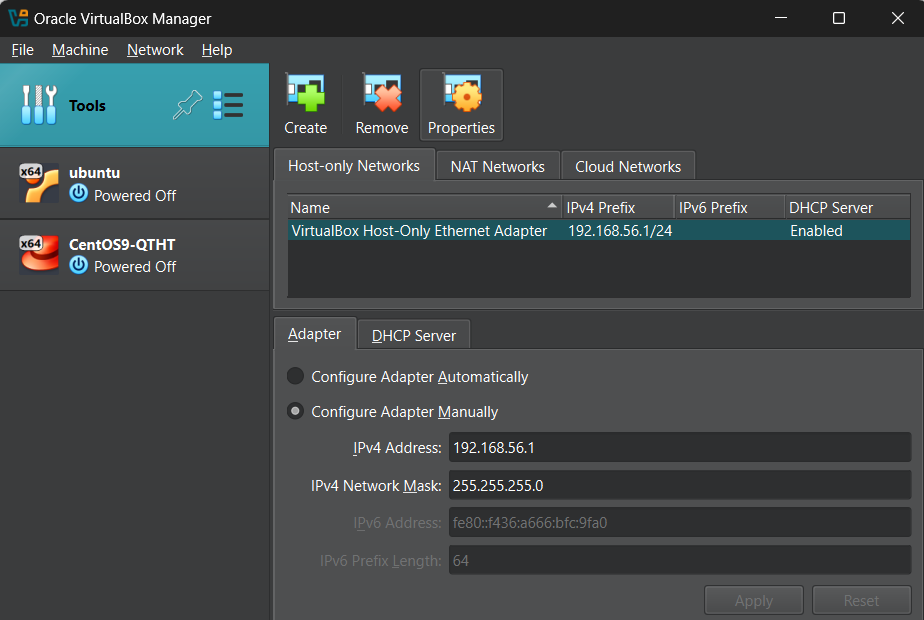
+ Phiên bản Virtual Box hiện tại được sử dụng là 7.1.4. Giao diện của hệ thống như sau:



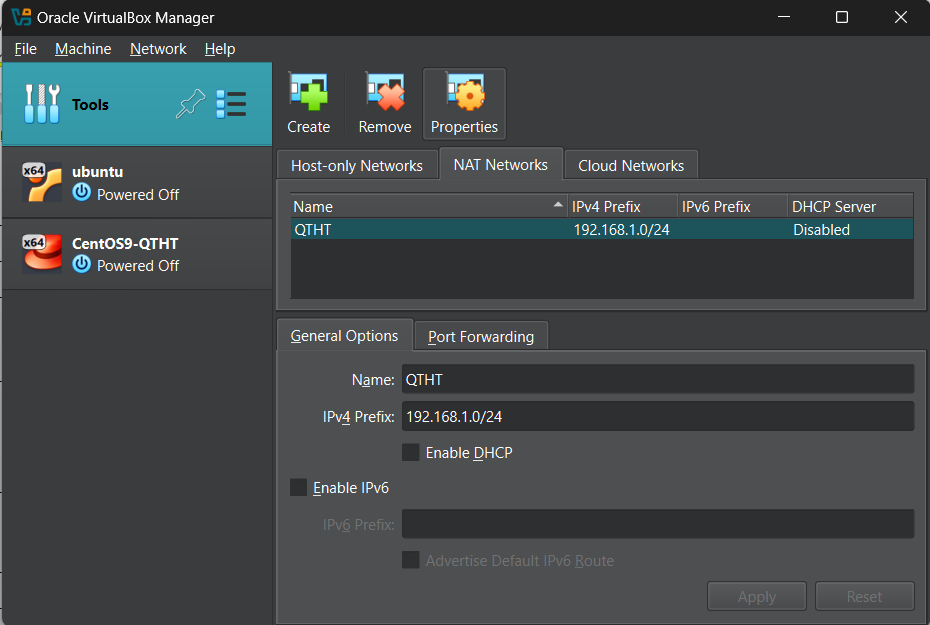
+ Chọn lần lượt: File Tools Network Manager (hoặc nhấn tổ hợp phím Ctrl + H để mở Network Manager):



+ Sau đó, giao diện sẽ hiển thị như sau:



+ Tại tab “NAT Networks”, nhấn *Create* để tạo một NAT Network. Sau đó, sửa tên thành “QTHT” và địa chỉ mạng là: 192.168.1.0/24. Tắt dịch vụ DHCP có sẵn.



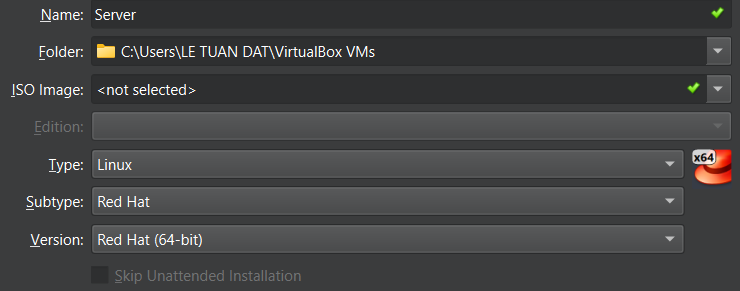
- Tạo 2 máy ảo với thông tin như sau:

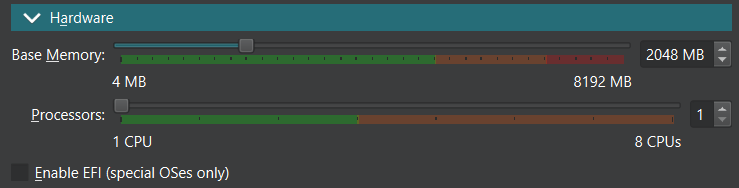
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | |  |  | **Desktop** | |
| **Host name** | Server |  |  | **Host name** | Desktop |
| **Hệ điều hành** | CentOS 9 |  |  | **Hệ điều hành** | Lubuntu 22.04,  hoặc bất kỳ hệ điều hành khác |
| **CPU/RAM/DISK** | 1core/2G/10G  Hoặc 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** |

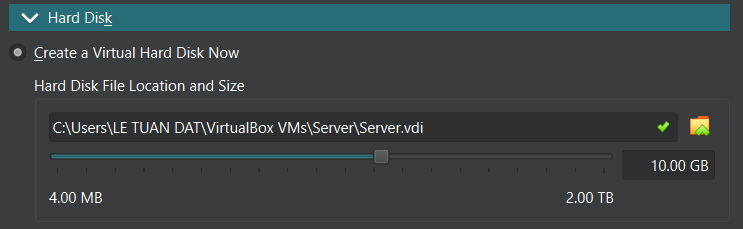
+ Máy ảo Server:

* Tại giao diện hệ thống, chọn New để tạo một máy ảo. Thông tin như sau:

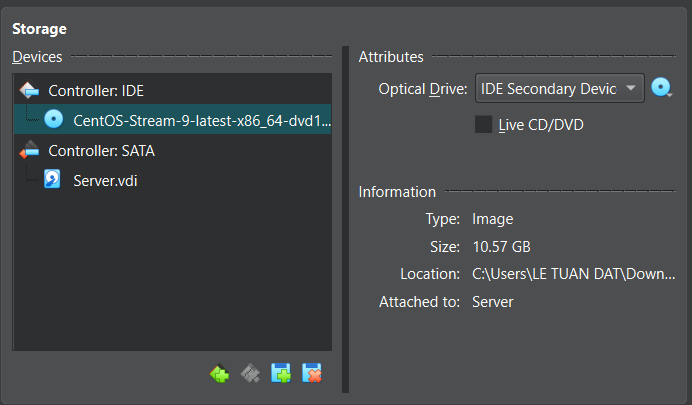
|  |
| --- |
| Name: Server  Base Memory: 2 GB = 2048MB  Processors: 1 CPU  Disk Size: 10GB |

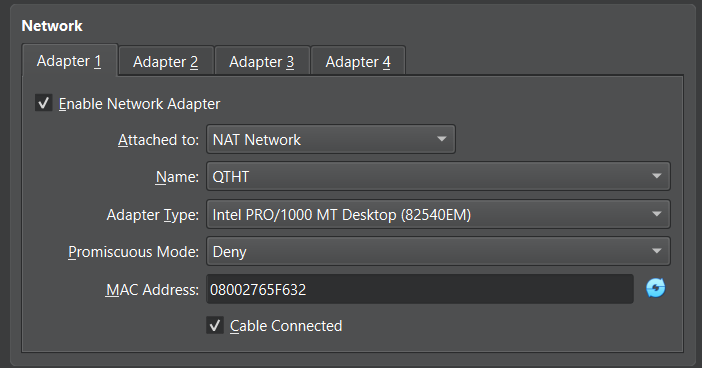




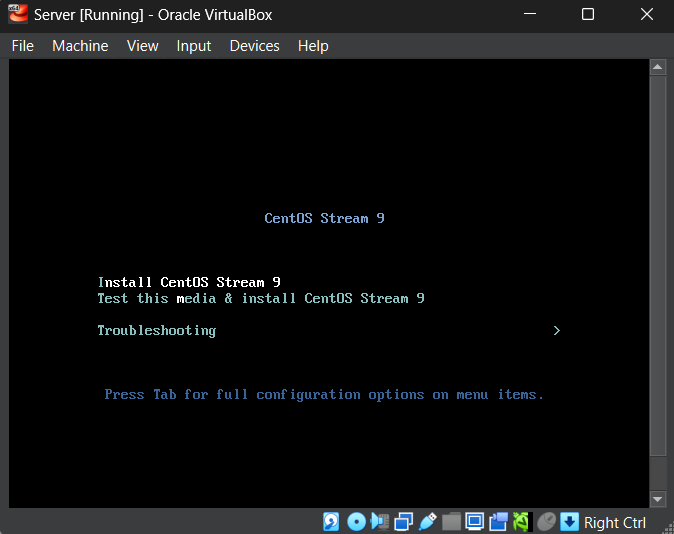


* Sau khi tạo, vào mục Settings của máy ảo Server để lấy file ISO CentOS đã tải, chọn NAT Network tại trường “Attached to” và chọn tên là “QTHT” tại trường “Name”. Các thông tin còn lại do hệ thống chọn.

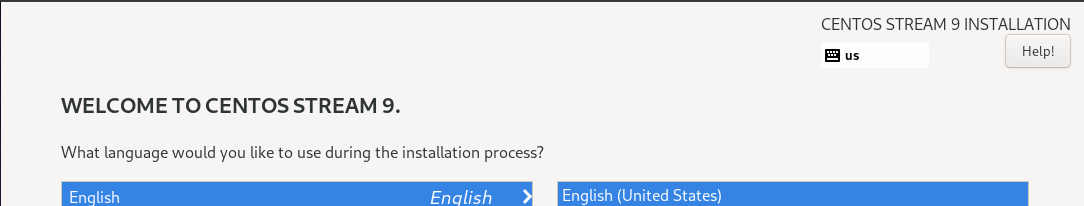




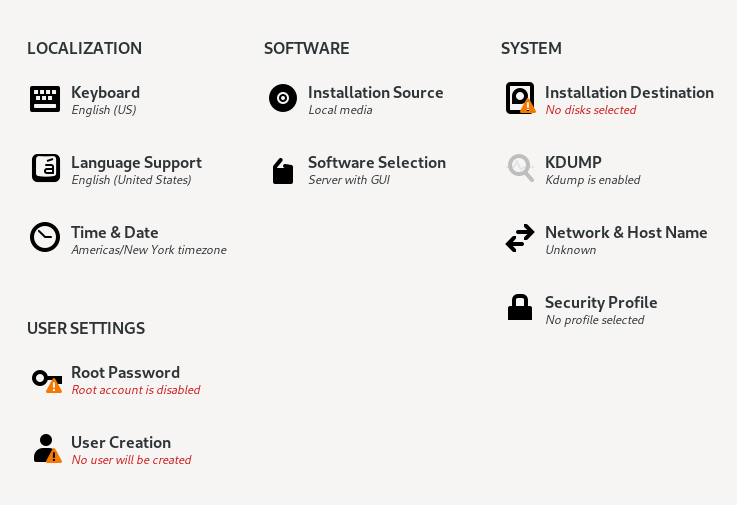
* Sau đó, chọn Start để khởi động máy ảo Server.
* Chọn “Install CentOS Stream 9”.



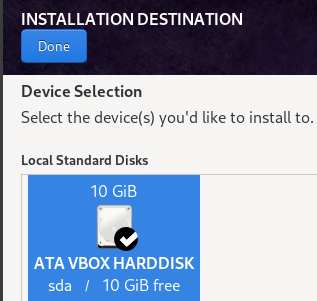
* Chọn ngôn ngữ: English.



* Tiếp theo, giao diện sẽ hiển thị như sau:

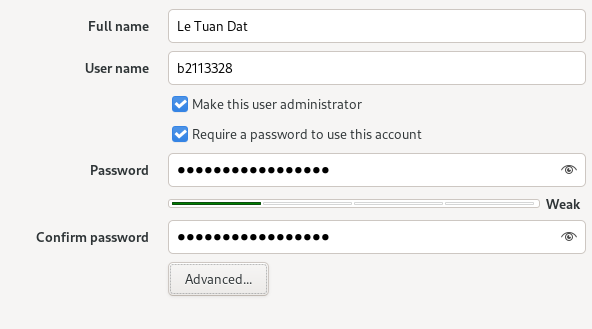


* Chọn Installation Destination, nhấn vào ổ đĩa 10GB và nhấn Done.

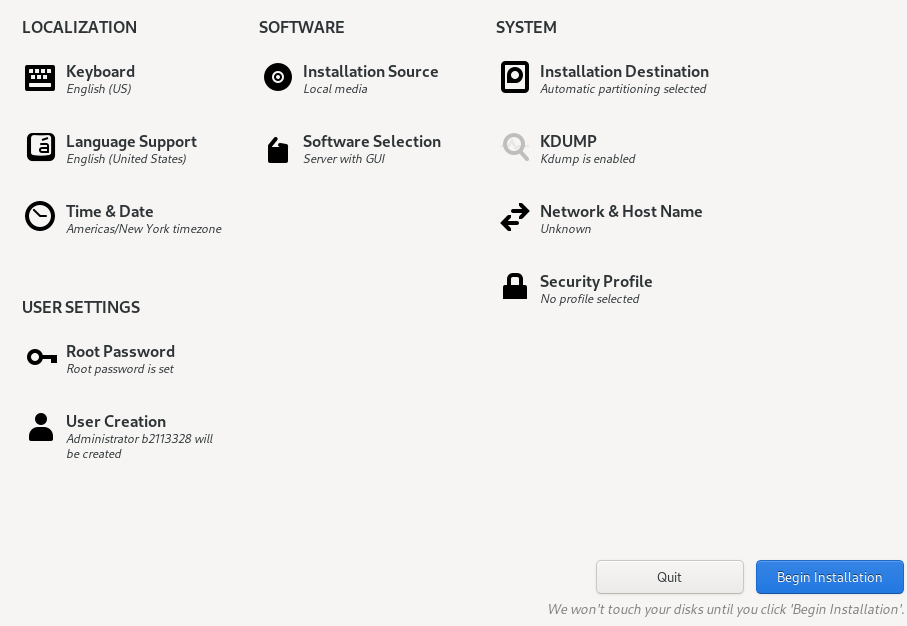


* Chọn User Creation và tạo tài khoản với thông tin như sau:

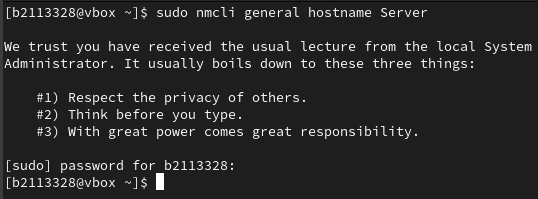
|  |
| --- |
| Full name: Le Tuan Dat  Username: b2113328  Cấp quyền quản trị => Make this user administrator  Password |



* Sau đó, màn hình sẽ trở lại như bên dưới và nhấn vào “Begin Installation” để cài đặt:



* Sau khi cài đặt, thực hiện cấu hình mạng cho máy. Đầu tiên, thực hiện đổi tên máy 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:

$nmcli con mod enp0s3 ipv4.gateway 192.168.1.1



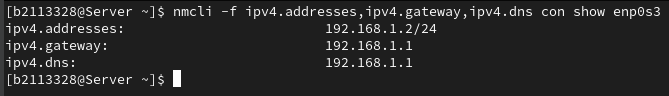
* Cấu hình DNS:

$nmcli con mod enp0s3 ipv4.dns 192.168.1.1



* Xem lại các thông tin đã cấu hình:

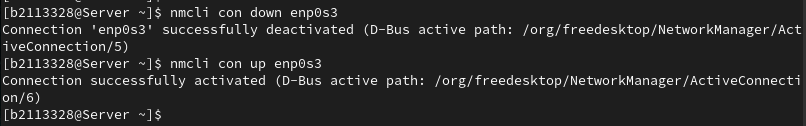
$nmcli -f ipv4.addresses,ipv4.gateway,ipv4.dns con show enp0s3



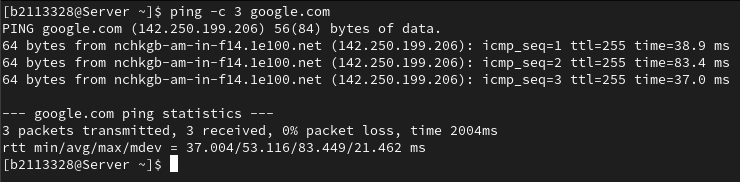
* Cập nhật các thay đổi bằng lệnh:

$nmcli con down enp0s3

$nmcli con up enp0s3



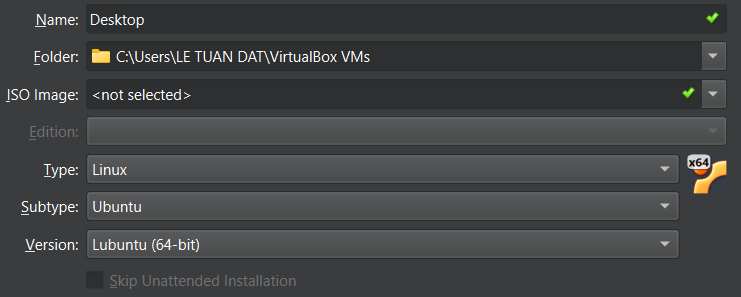
* Kiểm tra kết nối mạng bằng lệnh: $ping -c 3 google.com

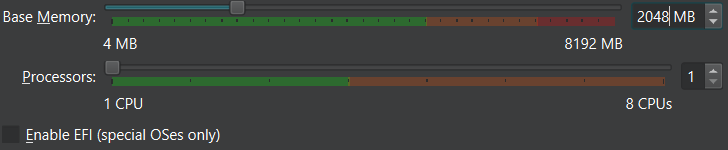


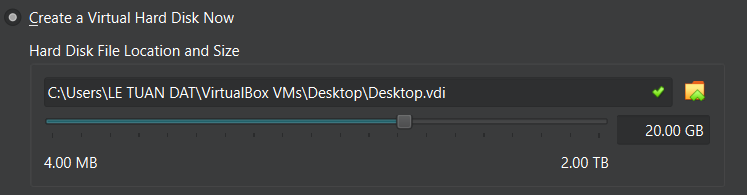
+ Máy ảo Desktop:

* Tại giao diện hệ thống, chọn New để tạo một máy ảo. Thông tin như sau:

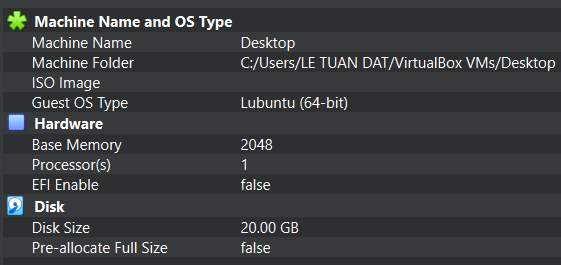
|  |
| --- |
| Name: Desktop  RAM: 2 GB = 2048MB  Processors: 1 CPU  Disk Size: 20GB |



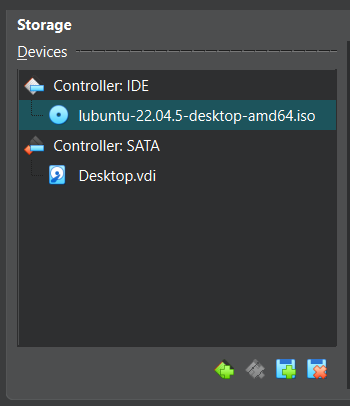


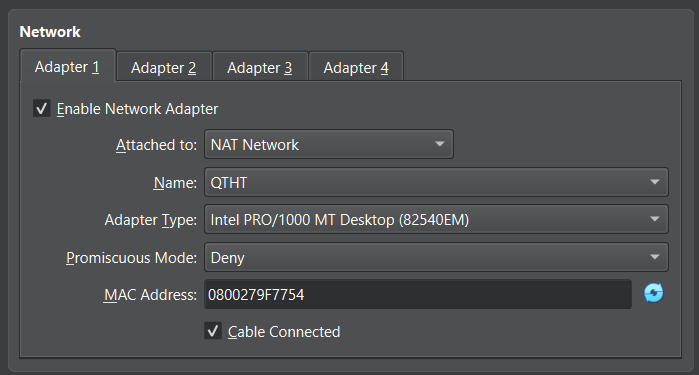


* Thông tin máy ảo Desktop vừa tạo:

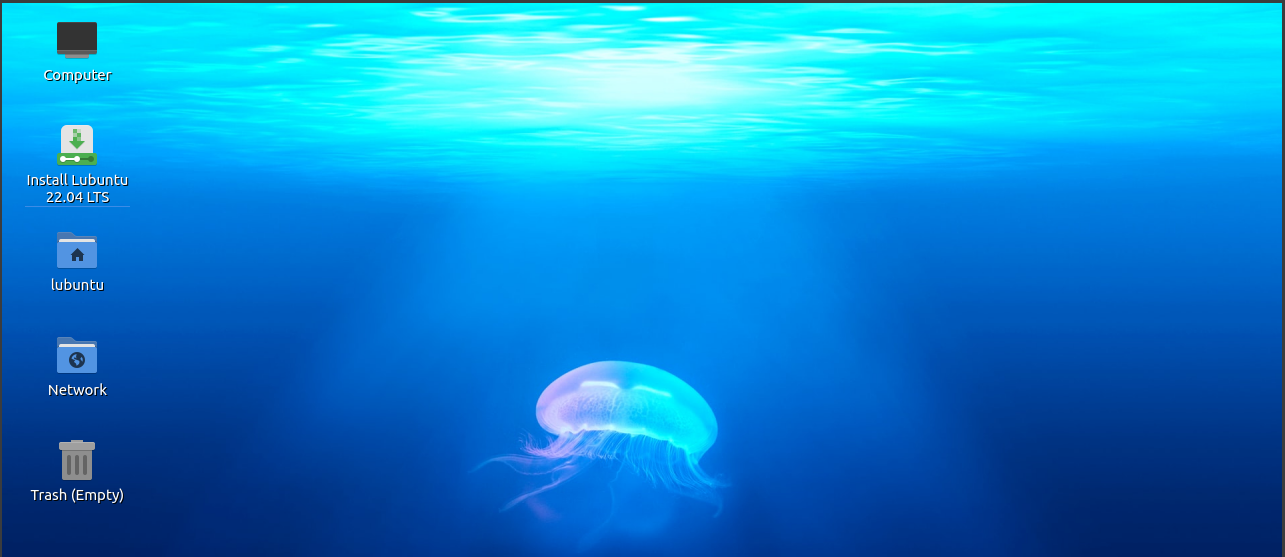


* Sau khi tạo, vào mục Settings của máy ảo Desktop để lấy file ISO Lubuntu đã tải, chọn NAT Network tại trường “Attached to” và chọn tên là “QTHT” tại trường “Name”.



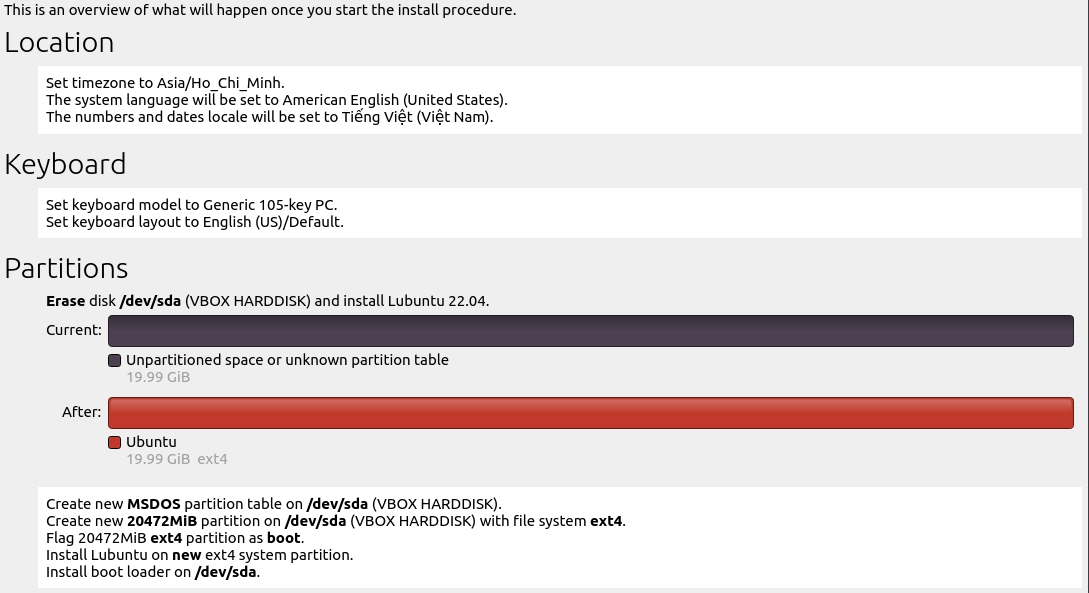


* Sau đó, khởi động máy ảo Desktop.
* Sau khi khởi động, giao diện sẽ được hiển thị như bên dưới:



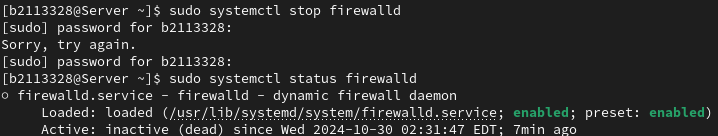
* Nhấn vào Install Lubuntu 22.04 LTS. Thông tin cài đặt như sau:

|  |
| --- |
| Language: American English  Region: Asia - Zone: Ho Chi Minh  Keyboard: English (US) - Default  Partition: Erase disk  Users: giacatluong |



* Sau khi cài đặt, tiến hành đăng nhập vào tài khoản vừa tạo. Việc cấu hình mạng động sẽ được thực hiện ở **câu** **6.**

- Tắt dịch vụ tường lửa trên Server bằng: $sudo systemctl stop firewalld



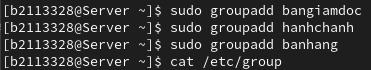
# Tạo các nhóm người dùng (group) và người dùng (user) trên Server

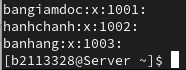
- Để quản lý các bộ phận và người dùng trong công ty, hãy tạo các nhóm người dùng (group) và người dùng (user) trên server như bảng bên dưới. Cấp quyền sudo cho người dùng Gia Cát Lượng.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Họ Tên** | **Nhóm** | **Username** | **Password** | **Mô tả** |
| 1 | Lưu Bị | bangiamdoc | bi.luu | luubi | Giám đốc |
| 2 | Gia Cát Lượng | bangiamdoc | luong.giacat | giacatluong | Phó giám đốc |
| 3 | Quan Vũ | hanhchanh | vu.quan | quanvu | Trưởng phòng |
| 4 | Trương Phi | hanhchanh | phi.truong | truongphi | Nhân viên |
| 5 | Triệu Vân | banhang | van.trieu | trieuvan | Trưởng phòng |
| 6 | Mã Siêu | banhang | sieu.ma | masieu | Nhân viên |
| 7 | Hoàng Trung | banhang | trung.hoang | hoangtrung | Nhân viên |

+ Tạo các nhóm người dùng *bangiamdoc, hanhchanh, banhang*.

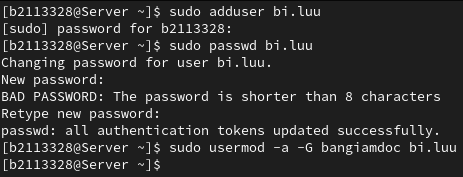
|  |
| --- |
| Tạo nhóm người dùng mới: $sudo groupadd <tên nhóm>  Xem lại các nhóm đã tạo: $cat /etc/group |

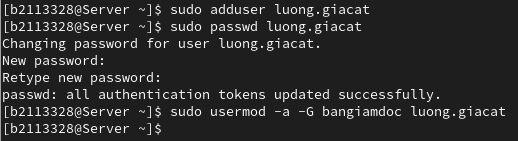


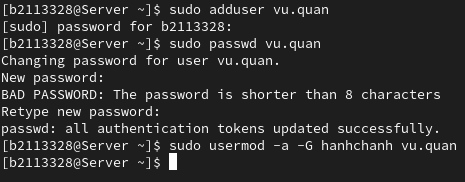


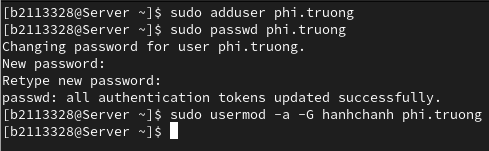
+ Tạo các người dùng Lưu Bị, Gia Cát Lượng, Quan Vũ, Trương Phi, Triệu Vân, Mã Siêu, Hoàng Trung với username và password như bảng phía trên và thêm người dùng vào nhóm tương ứng.

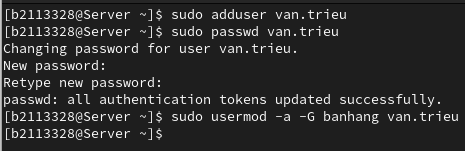
|  |
| --- |
| Tạo người dùng mới: $sudo adduser <tên người dùng>  Đặt mật khẩu cho người dùng: $sudo passwd <tên người dùng>  Thêm người dùng vào nhóm: $sudo usermod -a -G <tên nhóm> <tên người dùng> |

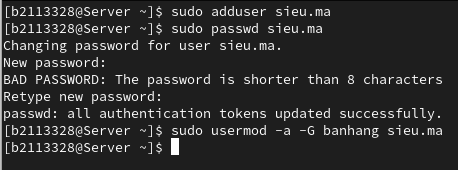


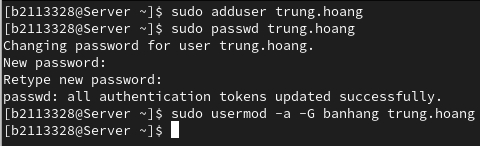








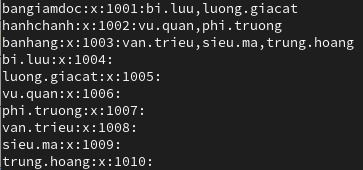




+ Xem các nhóm người dùng và những người dùng có trong nhóm đó bằng lệnh:

$cat /etc/group





+ Cấp quyền sudo cho người dùng Gia Cát Lượng.

|  |
| --- |
| Cấp quyền sudo: $sudo usermod -aG wheel <tên người dùng>  Kiểm tra người dùng thuộc những nhóm nào: $groups <tên người dùng> |

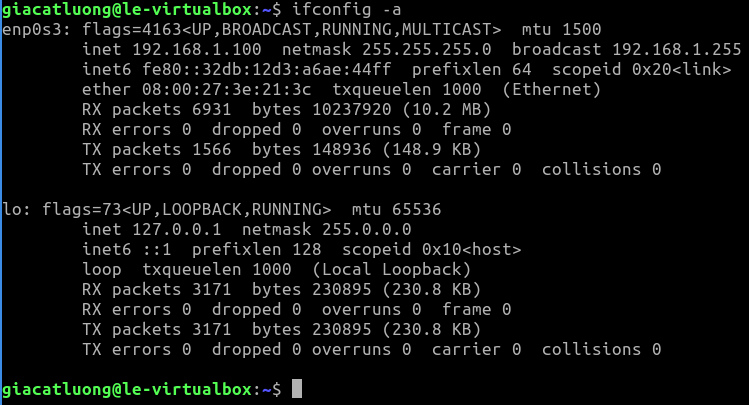


=> Nhóm wheel cho phép tất cả người dùng trong nhóm này thực thi bất kỳ lệnh nào trên hệ thống. Nên để người dùng *luong.giacat* có quyền sudo thì thêm người dùng *luong.giacat* vào nhóm wheel.

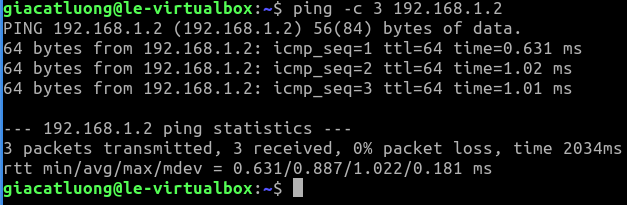
# Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa Server

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

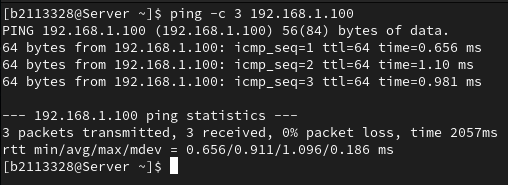
+ Xem địa chỉ IP trên máy Desktop: $ifconfig -a



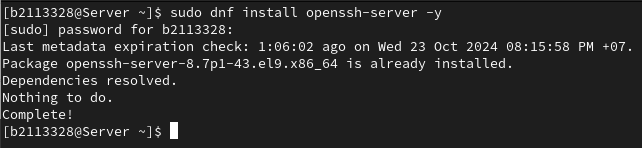
+ Ping từ máy Desktop sang máy Server: $ping -c 3 192.168.1.2



+ Ping từ máy Server sang máy Desktop: $ping -c 3 192.168.1.100



- Cài đặt OpenSSH: $sudo dnf install openssh-server -y



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

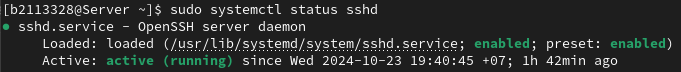
$sudo systemctl start sshd

$sudo systemctl enable sshd



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

$sudo systemctl status sshd

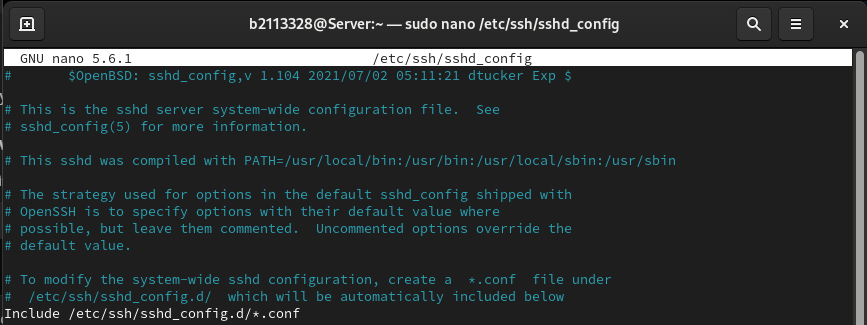


- Chỉ có thành viên ban giám đốc và tài khoản *b2113328*mới có quyền điều khiển từ xa Server. Tài khoản root không được nối kết tới Server từ xa.

+ Mở tệp cấu hình SSH /etc/ssh/sshd\_config để chỉnh sửa file cấu hình:

$sudo nano /etc/ssh/sshd\_config





+ Chỉ cho phép thành viên nhóm ban giám đốc và tài khoản *b2113328* có quyền điều khiển từ xa bằng cách thêm dòng sau: AllowGroups bangiamdoc b2113328



+ Chặn tài khoản root kết nối qua SSH bằng cách tìm dòng *PermitRootLogin* và sửa từ “yes” thành “no”.



+ Khởi động lại dịch vụ SSH để lưu các thay đổi:

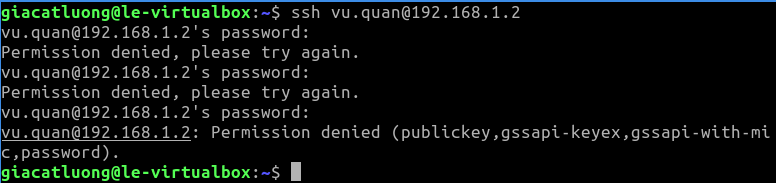
$sudo systemctl restart sshd



+ Kiểm tra quyền truy cập ở máy Desktop bằng lệnh:

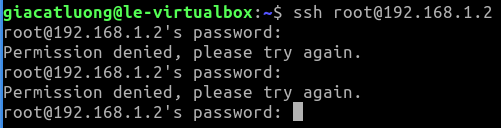
$ssh <username>@<địa chỉ server>

* Kiểm tra bằng tài khoản không thuộc nhóm bangiamdoc. Trường hợp này sử dụng tài khoản của người dùng Quan Vũ (vu.quan).



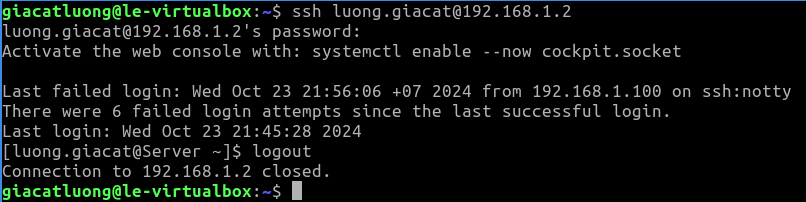
=> Kết nối thất bại.

* Kiểm tra bằng tài khoản root.



=> Kết nối thất bại.

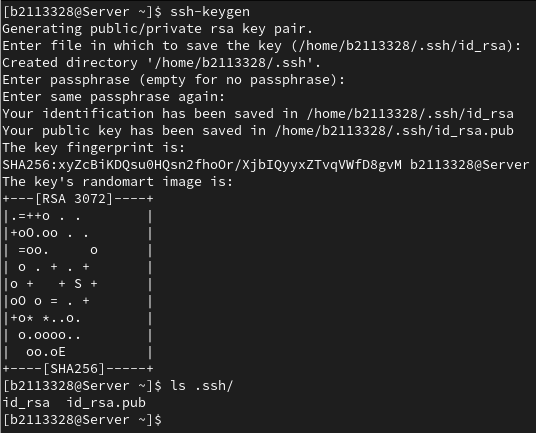
* Kiểm tra với tài khoản thuộc nhóm bangiamdoc. Trường hợp này sử dụng tài khoản Gia Cát Lượng (luong.giacat).



=> Kết nối thành công.

- 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: $ssh-keygen. Sau đó, sử dụng lệnh $ls .ssh/ thì xuất hiện 2 file là id\_rsa và id\_rsa.pub lần lượt là private key và public key.



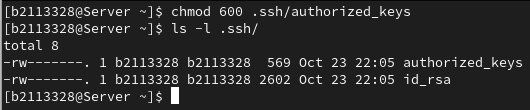
+ Di chuyển public key đến vị trí mặc định (.ssh/authorized\_keys) bằng lệnh:

$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 chức năng bằng public key:

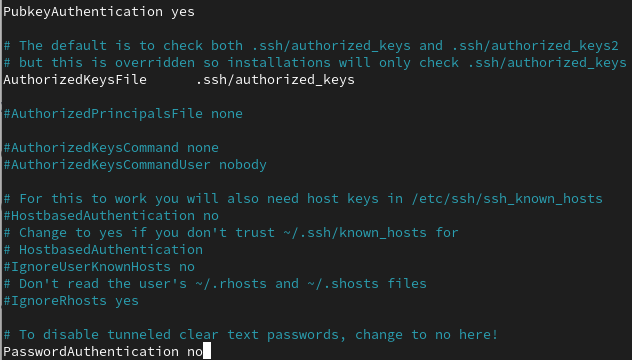
$sudo nano /etc/ssh/sshd\_config

# Thay đổi

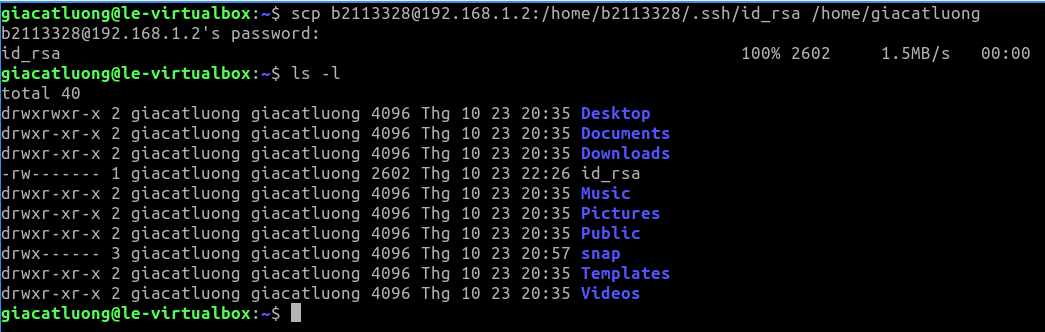
PubkeyAuthentication **yes**

PasswordAuthentication **no**

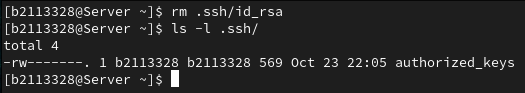




+ Ở máy Desktop, dùng lệnh $scp <username>@<địa chỉ server>:</đường dẫn tập tin cần tải> <đường dẫn đích để tải xuống> để download file private key (.ssh/id\_rsa).

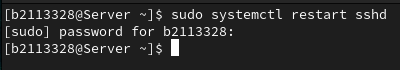


+ Thực hiện xóa file id\_rsa trên máy Server: $rm .ssh/id\_rsa



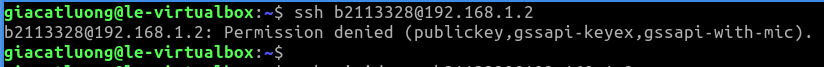
+ Khởi động lại SSH Server để lưu thay đổi:

$sudo systemctl restart sshd



+ Kiểm tra:

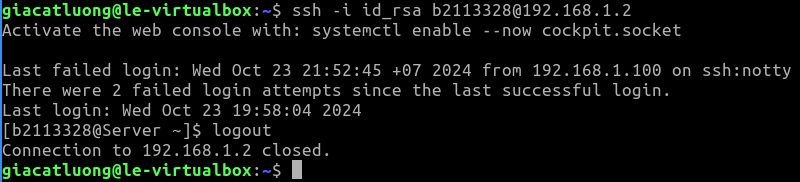
* Do tắt chức năng chứng thực bằng mật khẩu nên không thể nhập mật khẩu để kết nối vào máy Server.



=> Kết nối thất bại.

* Kết nối bằng tập tin private key vừa tải:

$ssh -i id\_rsa <username>@<địa chỉ server>

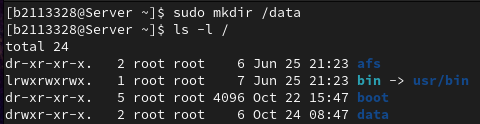


=> Kết nối thành công.

# Phân quyền truy cập:

- 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 chủ sở hữu tập tin có quyền xóa hoặc đổi tên tệp trong thư mục /data.

+ Sử dụng lệnh $sudo mkdir /data để tạo thư mục data trên Server.



=> Để phân quyền cho nhiều nhóm người dùng trên một thư mục hay tập tin, kỹ thuật được sử dụng ở đây là: **ACL (Access Control List).**

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

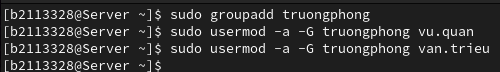
$sudo setfacl -m g:bangiamdoc:rwx /data



+ Phân quyền cho các trưởng phòng có quyền read và execute trên thư mục /data:

$sudo setfacl -m g:truongphong:r-x /data

* Tạo nhóm **truongphong** gồm: Quan Vũ và Triệu Vân.



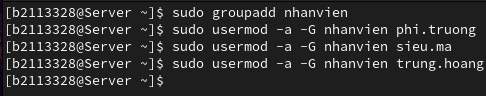
* Phân quyền cho các trưởng phòng có quyền trên thư mục /data.



+ Phân quyền cho các nhân viên không có quyền gì trên thư mục /data.

$sudo setfacl -m g:nhanvien:--- /data

* Tạo nhóm **nhanvien** gồm: Trương Phi, Mã Siêu và Hoàng Trung.



* Phân quyền cho các nhân viên không có quyền gì trên thư mục /data.

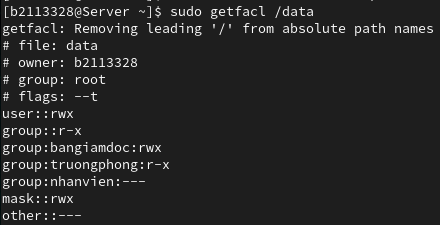


+ Chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên trên thư mục /data bằng cách: Đặt sticky bit trên thư mục /data với lệnh: $sudo chmod 1750 /data



+ Xem lại các quyền truy cập của các nhóm người dùng trên thư mục /data:

$sudo getfacl /data

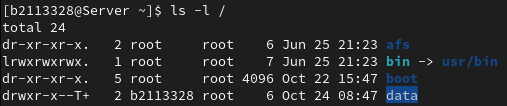


- Kiểm tra các quyền truy cập:

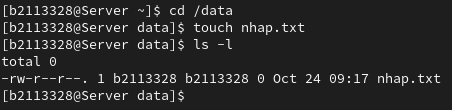
+ Đối với người dùng *b2113328*:

* Để dễ dàng trong việc kiểm tra, thay đổi chủ sở hữu của thư mục /data thành b2113328 bằng lệnh: $sudo chown b2113328 /data.



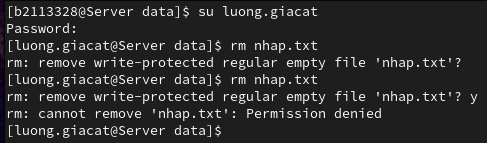


* Sử dụng lệnh $touch nhap.txt trong thư mục /data để tạo một file rỗng.



* Chuyển sang người dùng Gia Cát Lượng (luong,giacat) thuộc nhóm *bangiamdoc* và xóa file nhap.txt

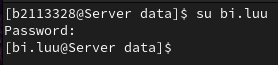
|  |
| --- |
| Chuyển sang người dùng khác: $su <tên người dùng>  Xóa tập tin: $rm <tên tập tin> |



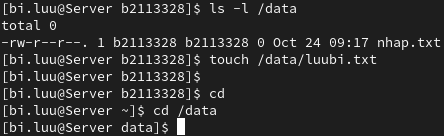
=> Người dùng Gia Cát Lượng thuộc nhóm bangiamdoc với toàn quyền (read, write và execute) trên thư mục /data nhưng không thể xóa do đã phân quyền chỉ có chủ sở hữu mới có quyền xóa hoặc đổi tên tập tin trong thư mục /data.

+ Đối với nhóm người dùng *bangiamdoc*:

* Chuyển sang người dùng Lưu Bị (bi.luu) thuộc nhóm người dùng *bangiamdoc*.



* Thực hiện kiểm tra các quyền của người dùng bi.luu trên thư mục /data.



=> Quyền read: Xem được bên trong thư mục /data bằng $ls -l /data.

Quyền write: Tạo được tập tin mới *luubi.txt* trong /data bằng lệnh:

$touch /data/luubi.txt

Quyền execute: Có thể đi xuyên qua thư mục /data bằng lệnh:

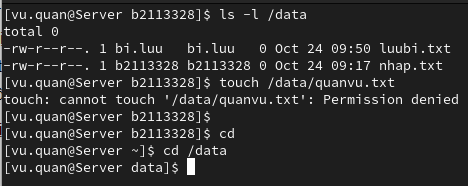
$cd /data

+ Đối với nhóm người dùng *truongphong*:

* Chuyển sang người dùng Quan Vũ (vu.quan) thuộc nhóm người dùng *truongphong*.



* Thực hiện kiểm tra các quyền của người dùng vu.quan trên thư mục /data



=> Quyền read: Xem được bên trong thư mục /data bằng $ls -l /data.

Quyền write: Không tạo được tập tin mới bằng lệnh

$touch /data/quanvu.txt.

Quyền execute: Có thể đi xuyên qua được thư mục /data bằng lệnh:

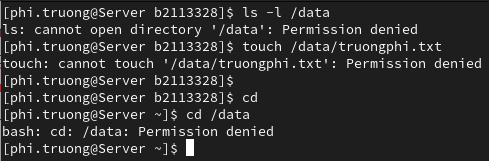
$cd /data

+ Đối với nhóm người dùng *nhanvien*:

* Chuyển sang người dùng Trương Phi (phi.truong) thuộc nhóm người dùng *nhanvien*.



* Thực hiện kiểm tra các quyền của người dùng phi.truong trên thư mục /data.



=> Quyền read: Không thể xem được bên trong thư mục /data bằng lệnh

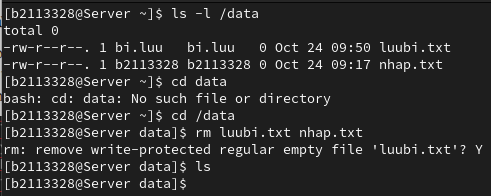
$ls -l /data.

Quyền write: Không thể tạo được tập tin mới bằng lệnh $touch /data/truongphi.txt.

Quyền execute: Không thể đi xuyên qua thư mục data bằng lệnh:

$cd /data.

+ Kiểm tra quyền xóa của người dùng *b2113328* trong thư mục /data.

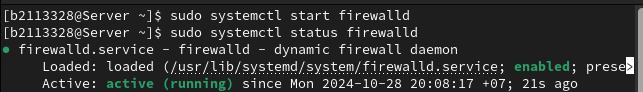


=> Sau khi kiểm tra các quyền với các nhóm người dùng, trong thư mục /data gồm hai tập tin luubi.txt và nhap.txt. Người dùng *b2113328* có thể thực hiện xóa hai tập tin này do *b2113328* là chủ sở hữu của /data và chủ sở hữu có thể xóa hoặc đổi tên tập tin trong /data.

# Cài đặt và cấu hình tường lửa trên Server:

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

+ Khởi động tường lửa firewalld: $sudo systemctl start firewalld

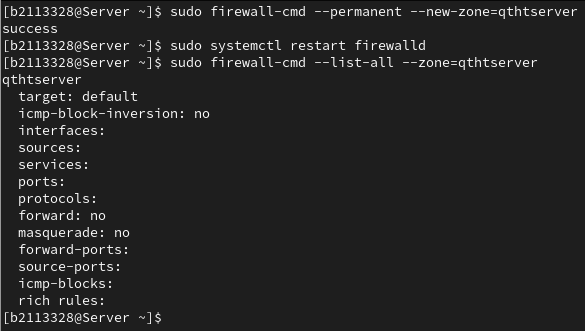


+ Tạo zone mới có tên là *qthtserver*:

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

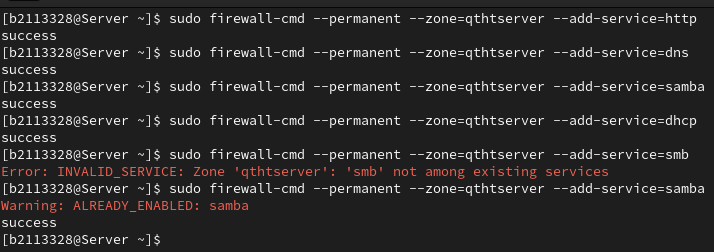
$sudo systemctl restart firewalld

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



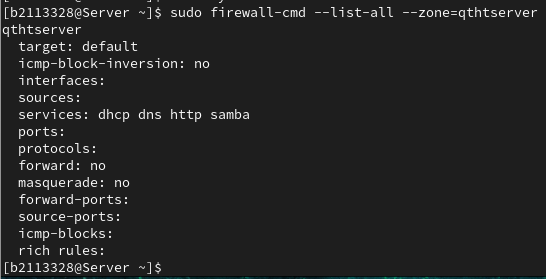
+ Cho phép các dịch vụ DNS, DHCP, SSH, Web, SAMBA trên zone *qthtserver*:

$sudo firewall-cmd --permanent --zone=qthtserver --add-service=<tên dịch vụ>



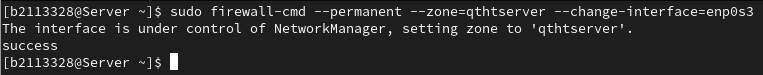
+ Khởi động lại tường lửa: $sudo systemctl restart firewalld



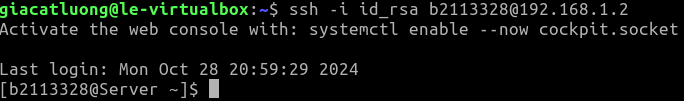


+ Chuyển giao diện mạng sang zone *qthtserver*.

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



+ Kiểm tra máy ảo Desktop có thể truy cập được tới các dịch vụ trên máy Server hay không?



=> Kết nối thành công.

# Cài đặt và cấu hình dịch vụ DHCP trên Server:

- 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: 192.168.1.100/24 => 192.168.1.254/24  Địa chỉ gateway: 192.168.1.1  DNS server: 192.168.1.1 và 8.8.8.8 |

+ Cài đặt dịch vụ DHCP trên Server: $sudo dnf install dhcp-server -y

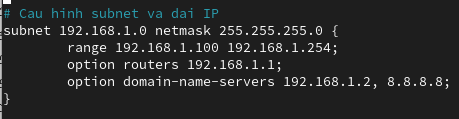




+ Tệp cấu hình chính của DHCP Server nằm ở /etc/dhcp/dhcpd.conf. Sử dụng lệnh $sudo nano /etc/dhcp/dhcpd.conf để cung cấp phạm vi địa chỉ IP cho các máy desktop.

|  |
| --- |
| Địa chỉ mạng: 192.168.1.0/24  Netmask: 255.255.255.0  Địa chỉ IP của desktop: 192.168.1.100/24 => 192.168.1.254/24  Gateway (Routers): 192.168.1.1  DNS Server: 192.168.1.2,8.8.8.8 |

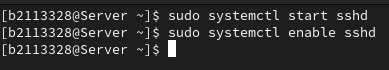




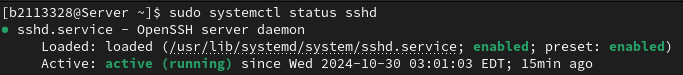
+ Khởi động và cho phép SSH tự động thực thi khi khởi động hệ điều hành:

$sudo systemctl start sshd

$sudo systemctl enable sshd



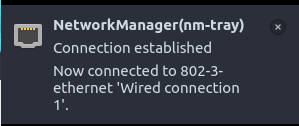
+ Kiểm tra xem SSH Server có đang thực thi hay chưa?



+ Khởi động lại dịch vụ mạng trên máy ảo Desktop bằng lệnh:

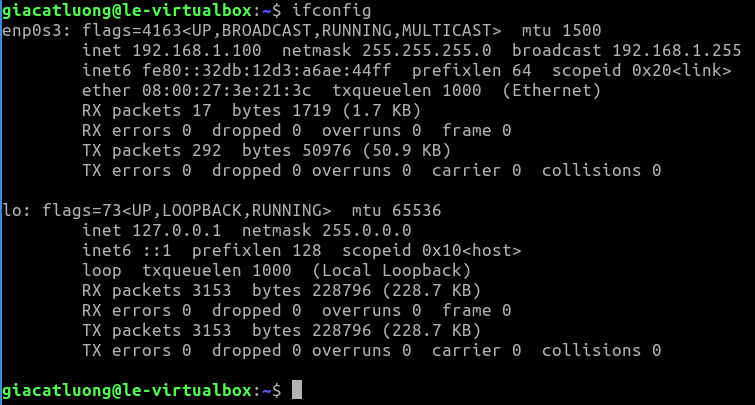
$sudo systemctl restart NetworkManager





=> Kết nối mạng thành công.

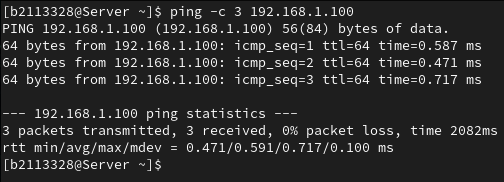
+ Kiểm tra máy Desktop đã nhận được IP từ DHCP hay chưa: $ifconfig



=> Máy Desktop đã nhận IP từ DHCP với địa chỉ mạng là: 192.168.1.100.

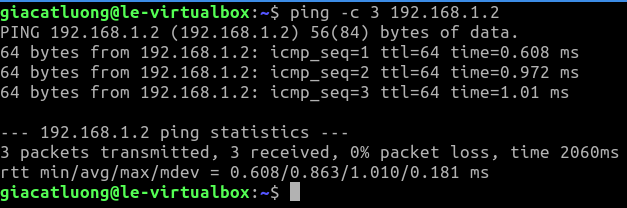
+ Kiểm tra nối kết từ máy Server đến máy Desktop:

$ping -c 3 192.168.1.100



+ Kiểm tra nối kết từ máy Desktop đến máy Server:

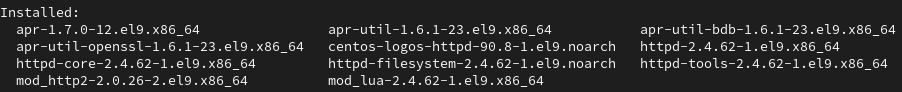
$ping -c 3 192.168.1.2



# Cài đặt và cấu hình dịch vụ máy chủ Web trên Server sử dụng Docker

- Cài đặt Apache Web Server: $sudo dnf install httpd -y

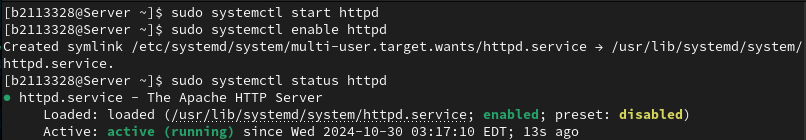




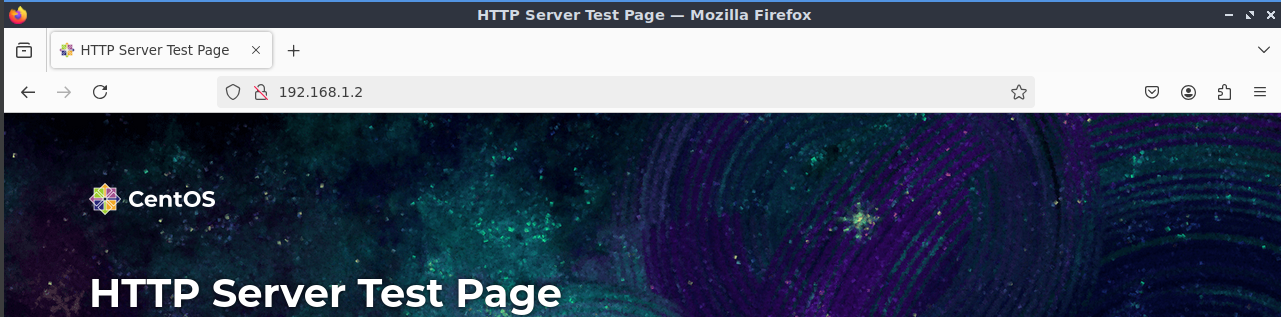
- Khởi động và cho phép Apache tự động thực thi khi khởi động hệ điều hành:

$sudo systemctl start httpd

$sudo systemctl enable httpd



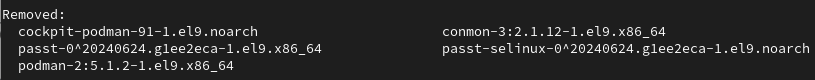
- Mở trình duyệt Web ở máy chủ Desktop và truy cập vào địa chỉ IP của máy Server để kiểm tra:



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

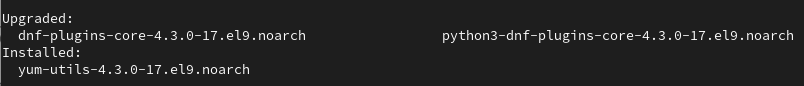
$sudo dnf remove podman runc -y





- Cài đặt công cụ yum-utils: $sudo dnf install yum-utils -y



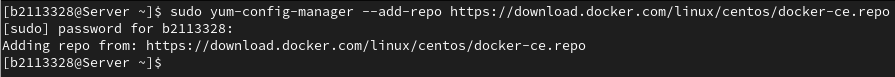


- Thêm địa chỉ repo của Docker vào công cụ yum:

$sudo yum-config-manager \

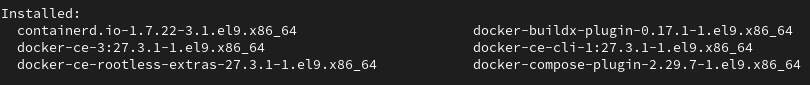
--add-repo \

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



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



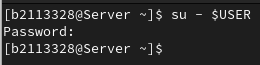


- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo: $sudo usermod -aG docker $USER.



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

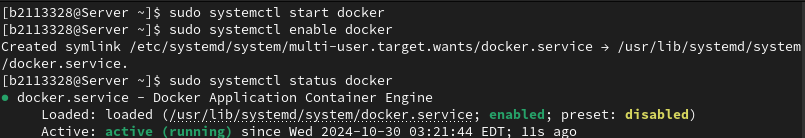
$su - $USER



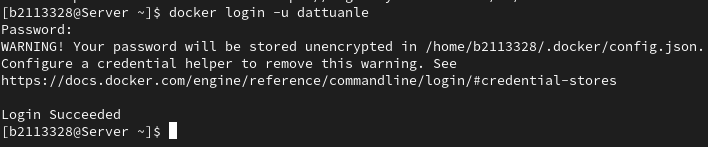
- Khởi động và cho phép dịch vụ Docker thực thi khi khởi động hệ điều hành:

$sudo systemctl start docker

$sudo systemctl enable docker

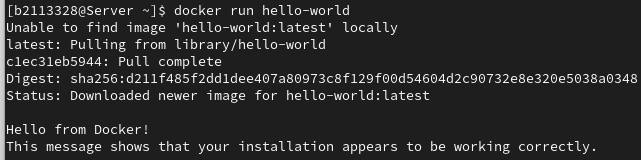


- Tạo một tài khoản trên DockerHub (https://hub.docker.com/), sau đó đăng nhập sử dụng lệnh: $docker login -u <docker-usename>



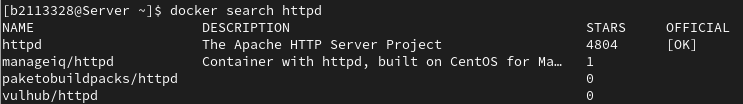
- Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.

$docker run hello-world



- Triển khai dịch vụ web server lên máy Server sử dụng một Docker:

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



+ Tạo container từ image httpd:

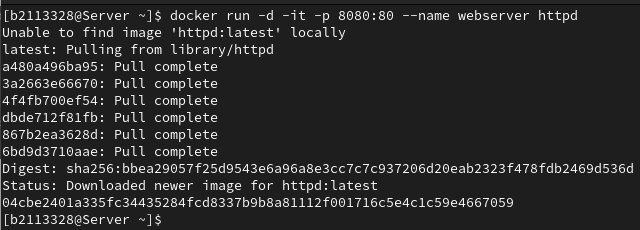
$docker run -d -it -p 8080:80 --name webserver httpd

-d: Chạy container ở chể độ background

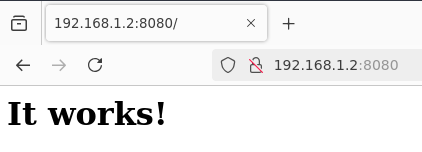
-it: Tạo shell để tương tác với container

--name webserver: Đặt tên container là webserver

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



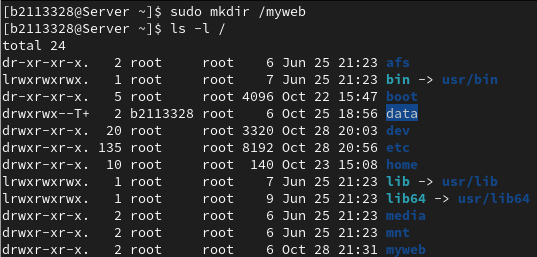
+ Kiểm tra trên máy Desktop bằng cách truy cập đến cổng 8080 của máy Server:



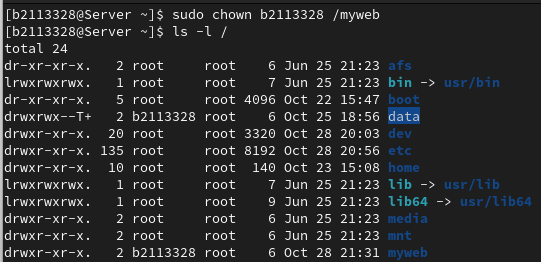
- Tạo một trang web cho công ty có tên miền *www.lautamquoc.com* với nội dung trang chủ giới thiệu về các thành viên trong công ty.

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

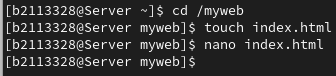
* Tạo thư mục /myweb: $sudo mkdir /myweb



* Chuyển chủ sở hữu của thư mục /myweb thành người dùng *b2113328* để có thể thao tác trên thư mục.



* Vào thư mục /myweb, tạo file index.html với nội dung là thành viên trong công ty.





+ Sao chép thư mục /myweb vào thư mục gốc của dịch vụ của web trên Docker container bằng lệnh:

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



+ Kiểm tra trên máy Desktop với đường dẫn: <http://192.168.1.2:8080/myweb>

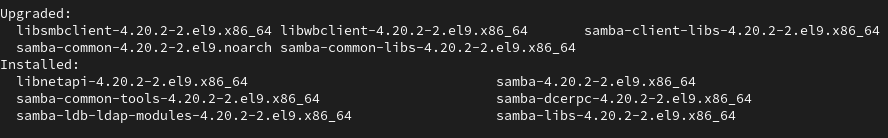


+ Tên miền www.lautamquoc.com sẽ được thực hiện ở câu **9**.

# Cài đặt và cấu hình dịch vụ SAMBA trên Server. Cấu hình chỉ cho phép:

- Cài đặt dịch vụ SAMBA: $sudo dnf install samba -y





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

+ 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 sau:

[data]

comment = Shared folder for bangiamdoc truongphong

path = /data

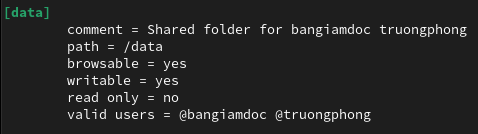
browsable = yes

writable = yes

read only = no

valid users = @bangiamdoc @truongphong





+ Cấu hình SELINUX cho phép SAMBA với hai lệnh:

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

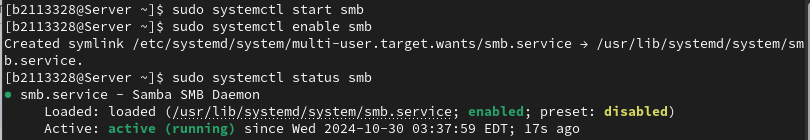
$sudo setsebool -P samba\_enable\_home\_dirs on



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

$sudo systemctl start smb

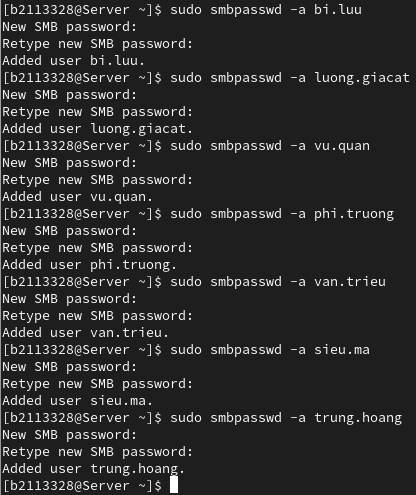
$sudo systemctl enable smb



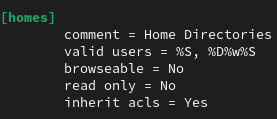
- Tất cả người dùng có thể truy cập vào thư mục cá nhân trên họ (/home/<username>) trên Server.

+ Thêm tất cả người dùng cho dịch vụ SAMBA bằng lệnh:

$sudo smbpasswd -a <user>



+ 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:

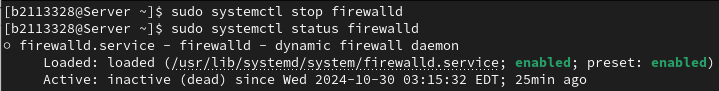


- Kiểm tra trên máy Desktop:

+ Cài SAMBA vào máy Desktop: $sudo apt install smbclient

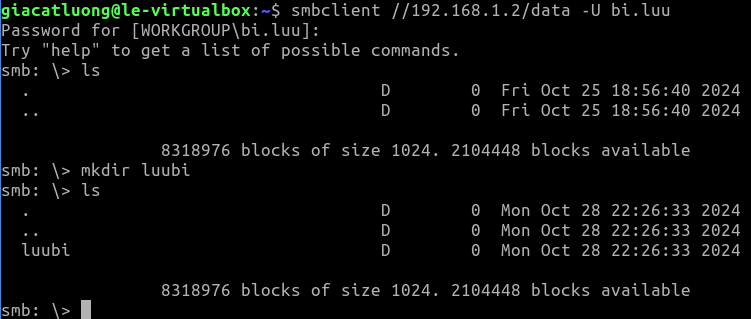


+ Tắt tường lửa trên máy Server:



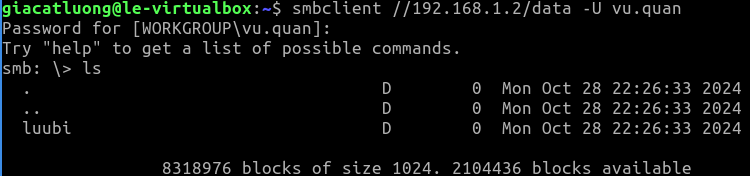
+ Kết nối SAMBA từ máy Desktop đến máy Server vào thư mục /data với tài khoản Lưu Bị thuộc bangiamdoc và tạo thư mục luubi:

$smbclient //192.168.1.2/data -U bi.luu

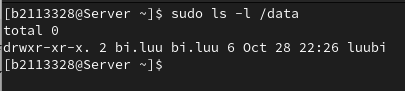


+ Kết nối SAMBA từ máy Desktop đến máy Server vào thư mục /data với tài khoản Quan Vũ thuộc truongphong:

$smbclient //192.168.1.2/data -U vu.quan

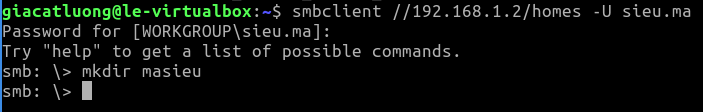


+ Đến đây, khi vào xem thư mục /data trên máy Server, sẽ có thư mục luubi vừa được tạo:

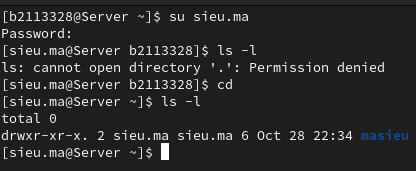


+ Kết nối SAMBA từ máy Desktop đến máy Server vào thư mục /homes với tài khoản Mã Siêu thuộc nhanvien và tạo thư mục masieu:

$smbclient //192.168.1.2/data -U sieu.ma

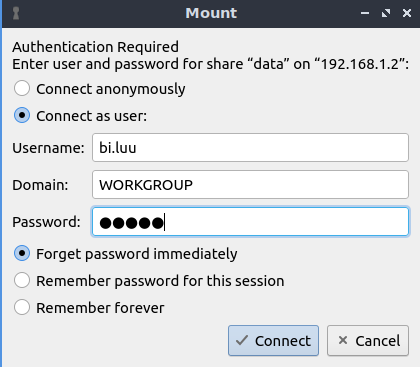


+ Chuyển sang người dùng Mã Siêu ở máy Server để kiểm tra liệu thư mục masieu có được tạo:



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

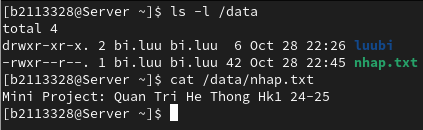
+ Nhập smb://192.168.1.2/data/ trên thanh tìm kiếm ở Computer của máy Desktop. Sau đó, một hộp thoại sẽ được hiện ra và các thông tin được cấu hình như hình sau:



+ Tạo một tập tin mới trong ổ ảo của thư mục /data:



+ Kiểm tra ở phía máy Server:

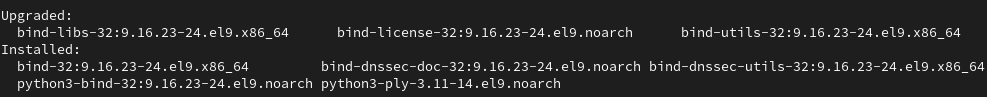


# Cài đặt và cấu hình dịch vụ DNS trên Server để phân giải tên miền lautamquoc.com

- Cài đặt BIND và các công cụ cần thiết:

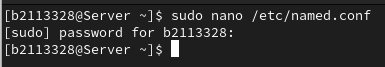
$sudo dnf install bind bind-utils -y





- Cấu hình DNS Server: $sudo nano /etc/named.conf

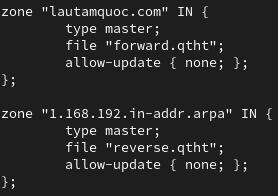
=> Bên dưới là các thay đổi so với những cài đặt trước đó của file cấu hình DNS Server, những cài đặt còn lại được giữ như cũ.











=> Thêm *any* vào *listen-on-port 53* để lắng nghe từ mọi IP.

Thêm *any* vào *allow-query* để cho phép truy vấn từ mọi IP.

Thêm *forwarders {192.168.1.1; };*

Tập tin phân giải xuôi: *forward.lautamquoc*.

Tập tin phân giải ngược: *reverse.lautamquoc*.

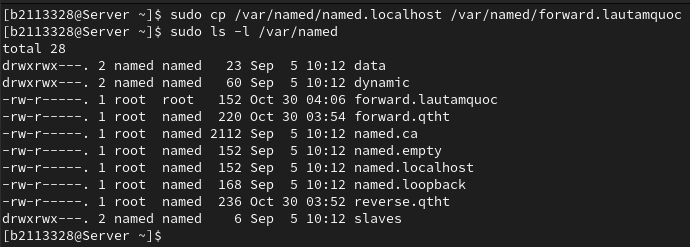
- Tên miền: *[www.lautamquoc.com](http://www.lautamquoc.com)* <----> IP: 192.168.1.2 (Server IP).

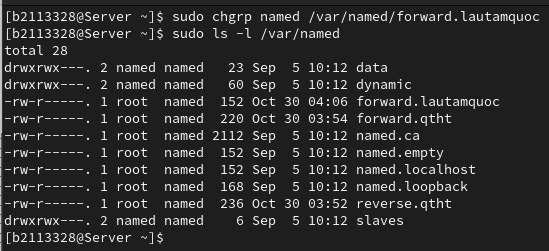
Tạo tập tin cấu hình phân giải xuôi:

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

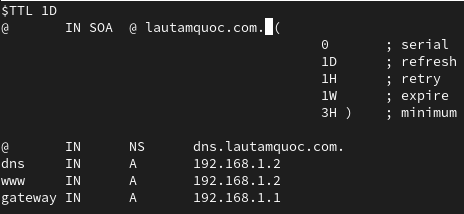
$sudo chgrp named /var/named/forward.lautamquoc

$sudo nano /var/named/forward.lautamquoc









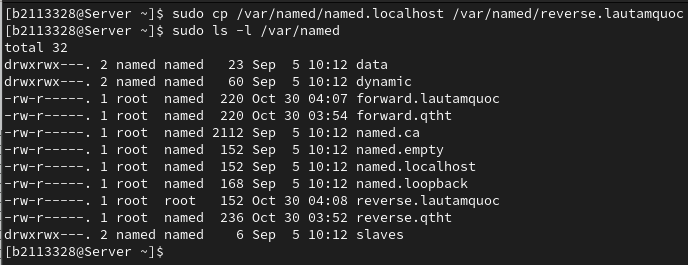
- Tên miền: *gateway.lautamquoc.com* <----> IP: 192.168.1.1

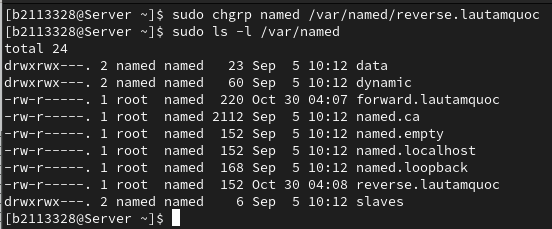
Tạo tập tin cấu hình phân giải ngược:

$sudo cp /var/named/named.localhost /var/named/reverse.lautamquoc

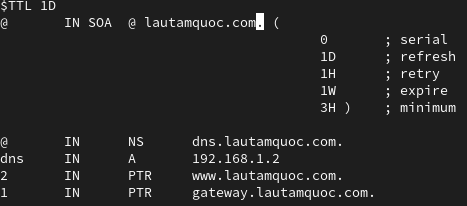
$sudo chgrp named /var/named/reverse.lautamquoc

$sudo nano /var/named/reverse.lautamquoc



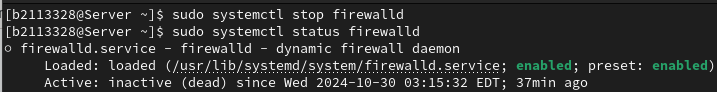




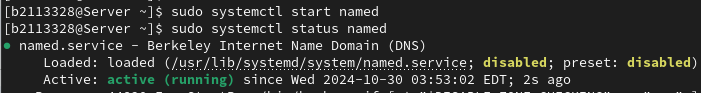


- Kiểm tra và sử dụng dịch vụ DNS:

+ Tắt tường lửa: $sudo systemctl stop firewalld



+ Khởi động dịch vụ DNS: $sudo systemctl start named



+ Kiểm tra kết quả:

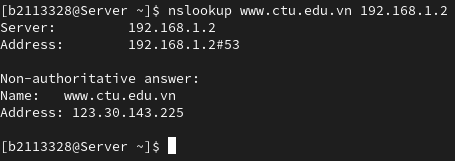
* nslookup [www.lautamquoc.com](http://www.lautamquoc.com) <địa chỉ IP máy Server>



* nslookup gateway.lautamquoc.com <địa chỉ IP máy Server>



* nslookup [www.ctu.edu.vn](http://www.ctu.edu.vn) <địa chỉ Ip máy Server>



* nslookup 192.168.1.2 192.168.1.2



* nslookup 192.168.1.1 192.168.1.2



* Trên máy Desktop, thêm tên miền [www.lautamquoc.com](http://www.lautamquoc.com) hướng đến địa chỉ IP của máy Server tại /etc/hosts. Sau đó, mở trình duyệt web và truy cập vào địa chỉ <http://www.lautamquoc.com/myweb>



# Sử dụng dịch vụ cron và shell script tự động

- Để hiệu chỉnh file crontab với trình soạn thảo nano, ta dùng câu lệnh sau:

$export EDITOR=nano

- Thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng trên Server:

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

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





- Lệnh $tar -cf <tên file nén> <các thư mục cần nén>:

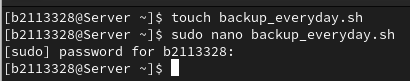
+ -c: Tạo tập tin nén mới.

+ -f: Chỉ định tên của tập tin nén.

+ Các thư mục cần nén cần nhau một khoảng trắng.

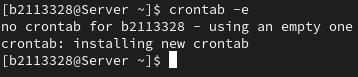
- Sao lưu mỗi ngày: Thực hiện vào lúc 23:59 từ thứ 2 đến thứ 7, dữ liệu sẽ được nén lại và lưu với tên như sau: backup\_<thứ> (ví dụ: backup\_monday).

+ Tạo một shell script *backup\_everyday.sh* để nén file. Chỗ *data +%A* được sử dụng để lấy ra các ngày trong tuần:





+ Hiệu chỉnh file crontab bằng lệnh: $crontab -e





- 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).

+ Tạo một shell script *backup\_everyweek.sh* để nén file. Chỗ *data +%V* được sử dụng để lấy thứ tự tuần trong năm.





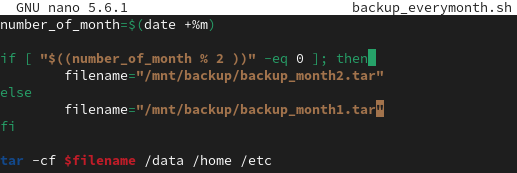
+ Hiệu chỉnh file crontab:



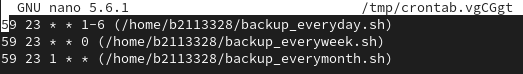
- Sao lưu mỗi tháng: Thực hiện vào lúc 23:59 ngày 1 hằng tháng, dữ liệu sẽ được nén lại và lưu với tên backup\_month1 nếu là tháng lẻ, backup\_month2 nếu là tháng chẵn.

+ Tạo một shell script *backup\_everymonth.sh* để nén file. Chỗ *data +%m* được sử dụng để lấy thứ tự tuần trong năm.

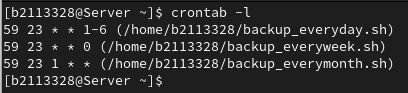




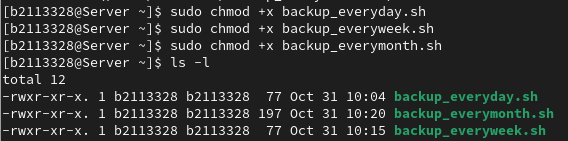
+ Hiệu chỉnh crontab:



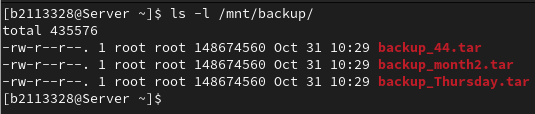
- Xem lại các shell script bằng lệnh: $crontab -l



- Cấp quyền thực thi cho các shell script: $sudo chmod +x <tên file>.sh



- Kiểm tra các crontab hoạt động bằng cách chạy các shell script và xem kết quả trong thư mục sao lưu:



**--- HẾT ---**