**BÀI TẬP NHÓM CUỐI KỲ**

Môn: **Quản Trị Hệ Thống**

**Học kỳ 1 - Năm học 2021-2022**

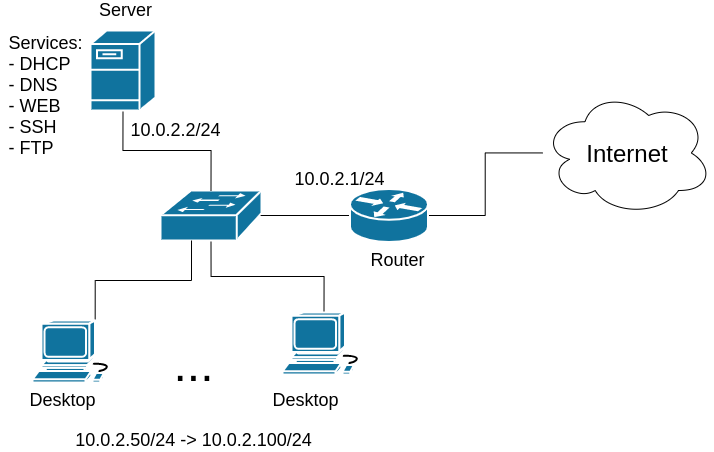
Nhóm báo cáo:  **23**

Nhóm học phần: **03**

Sinh viên thực hiện (1 sv): **Nguyễn Quang Thụy B1910306**

**Mô tả bài tập nhóm:**

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



**MỤC LỤC**

[1. Cài đặt và cấu hình server/desktop (80%) 6](#_Toc88937330)

[**1.1.** (10%) Sử dụng phần mềm VirtualBox/VMware: 6](#_Toc88937331)

[**1.2**. (10%) Tạo các nhóm người dùng (group) và người dùng (user) trên server 9](#_Toc88937332)

[**1.3.** (10%) Tạo thư mục /data trên server và phân quyền 12](#_Toc88937333)

[**1.4.** (10%) Cài đặt và cấu hình dịch vụ DHCP trên server 16](#_Toc88937334)

[**1.5.** (10%) Cài đặt và cấu hình tường lửa trên server 19](#_Toc88937335)

[**1.6.** (10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa server. 23](#_Toc88937336)

[**1.7.** (5%)Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền *trasualsb.com* 25](#_Toc88937337)

[**1.8.** (5%) Cài đặt và cấu hình dịch vụ máy chủ Web trên server sử dụng docker 30](#_Toc88937338)

[**1.9.** (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server 32](#_Toc88937339)

[**1.10.** (5%) Sử dụng dịch vụ cron và shell script thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng 34](#_Toc88937340)

[2. Hình thức bài báo cáo bài tập nhóm (20%) 37](#_Toc88937341)

**MỤC LỤC HÌNH**

[Hình 1: Tạo NAT Network tên "QTHT" có địa chỉ mạng là 10.0.2.0/24 6](#_Toc88937238)

[Hình 2: Cài đặt NAT Network cho máy Server 7](#_Toc88937239)

[Hình 3: Cấu hình kết nối Ethernet cho máy ảo Server 8](#_Toc88937240)

[Hình 4: Khởi động lại dịch vụ mạng 8](#_Toc88937241)

[Hình 5: Cấu hình của máy ảo Server 8](#_Toc88937242)

[Hình 6: Cài đặt NAT Network cho máy Desktop 9](#_Toc88937243)

[Hình 7: Tạo người dùng "tong.vo" và đặt mật khẩu cho người dùng đó 10](#_Toc88937244)

[Hình 8: Tạo nhóm người dùng "bangiamdoc" và thêm người dùng "giang.tong" vào nhóm 10](#_Toc88937245)

[Hình 9: Liệt kê tất cả người dùng trong nhóm 11](#_Toc88937246)

[Hình 10: Truy cập vào tập tin /etc/sudoers 11](#_Toc88937247)

[Hình 11: Thêm nhóm người dùng "bangiamdoc" vào nhóm người dùng có quyền sudo 11](#_Toc88937248)

[Hình 12: Người dùng "giang.tong" có thể truy cập vào tập tin /etc/shadow thông qua lệnh **sudo** 11](#_Toc88937249)

[Hình 13: Người dùng "nghia.lu" có thể truy cập vào tập tin /etc/shadow thông qua lệnh **sudo** 12](#_Toc88937250)

[Hình 14: Người dùng "lam.xung" không thể truy cập vào tập tin /etc/shadow thông qua lệnh sudo 12](#_Toc88937251)

[Hình 15: Tạo thư mục /data và kiểm tra phân quyền 13](#_Toc88937252)

[Hình 16: Chuyển nhóm chủ sở hữu của thư mục /data sang nhóm "bangiamdoc" 13](#_Toc88937253)

[Hình 17: Phân quyền truy cập cho chủ sở hữu, nhóm chủ sở hữu và các người dùng khác 13](#_Toc88937254)

[Hình 18: Chuyển chủ sở hữu của thư mục /data từ "root" sang "giang.tong" 14](#_Toc88937255)

[Hình 19: Thêm quyền đọc và thực thi cho các người dùng là trưởng phòng 14](#_Toc88937256)

[Hình 20: Thay đổi quyền của thư mục để chỉ chủ sở hữu mới có thể xóa hoặc đổi tên tập tin trong thư mục 14](#_Toc88937257)

[Hình 21: Người dùng "giang.tong" có thể ghi và thực thi trên tập tin test.sh nằm trong thư mục /data 15](#_Toc88937258)

[Hình 22: Người dùng "giang.tong" có thể đọc tập tin test.sh nằm trong thư mục /data 15](#_Toc88937259)

[Hình 23: Người dùng "dung.ngo" có thể thực thi thư mục test.sh nằm trong thư mục /data 15](#_Toc88937260)

[Hình 24: Người dùng "dung.ngo" không thể ghi trên thư mục test.sh nằm trong thư mục /data 16](#_Toc88937261)

[Hình 25: Người dùng "tham.lo" không thể truy cập được vào thư mục /data 16](#_Toc88937262)

[Hình 26: Người dùng "nghia.lu" không thể thay đổi tên tập tin hoặc xóa tập tin trong thư mục /data 16](#_Toc88937263)

[Hình 27: Cài đặt dịch vụ DHCP trên server 17](#_Toc88937264)

[Hình 28: Cấu hình dịch vụ DHCP qua tập tin /etc/dhcp/dhcpd.conf 17](#_Toc88937265)

[Hình 29: Khởi động dịch vụ DHCP 18](#_Toc88937266)

[Hình 30: Kiểm tra địa chỉ IP trên máy Lubuntu 18](#_Toc88937267)

[Hình 31: Từ máy Lubuntu ping tới CentOS 18](#_Toc88937268)

[Hình 32: Cài đặt dịch vụ iptables 19](#_Toc88937269)

[Hình 33: Khởi động dịch vụ iptables 19](#_Toc88937270)

[Hình 34: Trạng thái của dịch vụ iptables 20](#_Toc88937271)

[Hình 35: Các rules hiện có trong iptables 20](#_Toc88937272)

[Hình 36: Thêm rule cho phép dịch vụ DNS truy cập được vào máy Server 20](#_Toc88937273)

[Hình 37: Thêm rule cho phép dịch vụ DHCP truy cập được vào máy Server 21](#_Toc88937274)

[Hình 38: Thêm rule cho phép dịch vụ FTP truy cập được vào máy Server 21](#_Toc88937275)

[Hình 39: Thêm rule cho phép dịch vụ Web truy cập được vào máy Server 22](#_Toc88937276)

[Hình 40: Thay đổi rule để chỉ Desktop có thể ping tới Server 22](#_Toc88937277)

[Hình 41: Từ máy Desktop ping tới Server 22](#_Toc88937278)

[Hình 42: Từ máy thực Windows ping tới máy ảo CentOS (Server) 23](#_Toc88937279)

[Hình 43: Sao lưu rules trong iptables 23](#_Toc88937280)

[Hình 44: Cài đặt dịch vụ SSH cho Server 23](#_Toc88937281)

[Hình 45: Khởi động dịch vụ SSH 24](#_Toc88937282)

[Hình 46: Không cho phép tài khoản root đăng nhập 24](#_Toc88937283)

[Hình 47: Cho phép group "bangiamdoc" và các trưởng phòng đăng nhập 24](#_Toc88937284)

[Hình 48: Tài khoản root bị từ chối đăng nhập 24](#_Toc88937285)

[Hình 49: Tài khoản giang.tong đăng nhập thành công 25](#_Toc88937286)

[Hình 50: Tài khoản dung.ngo đăng nhập thành công 25](#_Toc88937287)

[Hình 51: Tài khoản nhân viên bị từ chối đăng nhập 25](#_Toc88937288)

[Hình 52: Cài đặt BIND và các công cụ cần thiết 26](#_Toc88937289)

[Hình 53: Thêm vào file /etc/named.conf các câu lệnh 27](#_Toc88937290)

[Hình 54: Thêm vào file /etc/named.conf các câu lệnh 27](#_Toc88937291)

[Hình 55: Tạo tập tin cấu hình phân giải xuôi 28](#_Toc88937292)

[Hình 56: Tạo tập tin cấu hình phân giải ngược 29](#_Toc88937293)

[Hình 57: Khởi động dịch vụ DNS 29](#_Toc88937294)

[Hình 58: Kiểm tra phân giải tên miền xuôi 29](#_Toc88937295)

[Hình 59: Kiểm tra phân giải tên miền ngược 30](#_Toc88937296)

[Hình 60: Liệt kê danh sách các container 30](#_Toc88937297)

[Hình 61: Lấy shell container loving\_mclaren đang chạy dịch vụ httpd 30](#_Toc88937298)

[Hình 62: Chỉnh sửa nội dung trang chủ 31](#_Toc88937299)

[Hình 63: Nội dung website trang chủ của công ty 31](#_Toc88937300)

[Hình 64: Cài đặt dịch vụ FTP cho máy Server 32](#_Toc88937301)

[Hình 65: Cấu hình dịch vụ FTP 32](#_Toc88937302)

[Hình 66: Cấu hình dịch vụ FTP 32](#_Toc88937303)

[Hình 67: Cấu hình dịch vụ FTP 33](#_Toc88937304)

[Hình 68: Khởi động dịch vụ FTP 33](#_Toc88937305)

[Hình 69: Kết nối đến Server bằng tài khoản “giang.tong” 33](#_Toc88937306)

[Hình 70: Các tập tin có trong thư mục /data 34](#_Toc88937307)

[Hình 71: Upload tập tin “abc.txt” lên Server và nhận được phản hồi “Permission denined” 34](#_Toc88937308)

[Hình 72: Tải tập tin “test.sh” từ Server về Desktop 34](#_Toc88937309)

[Hình 73: Script sao lưu mỗi ngày 35](#_Toc88937310)

[Hình 74: Shell script sao lưu mỗi ngày khi được thực thi 35](#_Toc88937311)

[Hình 75: Script sao lưu mỗi tuần 35](#_Toc88937312)

[Hình 76: Shell script sao lưu mỗi tuần khi được thực thi 36](#_Toc88937313)

[Hình 77: Script sao lưu mỗi tháng 36](#_Toc88937314)

[Hình 78: Shell script sao lưu mỗi tháng khi được thực thi 36](#_Toc88937315)

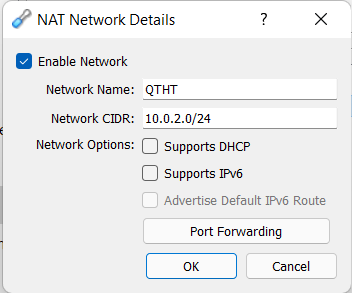
[Hình 79: Các file nén sau khi sao lưu được thực thi 37](#_Toc88937316)

[Hình 80: Lên lịch sao lưu định kỳ với Cron 37](#_Toc88937317)

# 1. Cài đặt và cấu hình server/desktop (80%)

## **1.1.** (10%) Sử dụng phần mềm VirtualBox/VMware:

- Tạo 1 NAT Network tên "QTHT" có địa chỉ mạng là 10.0.2.0/24. Tắt dịch vụ DHCP có sẵn trên NAT Network "QTHT".

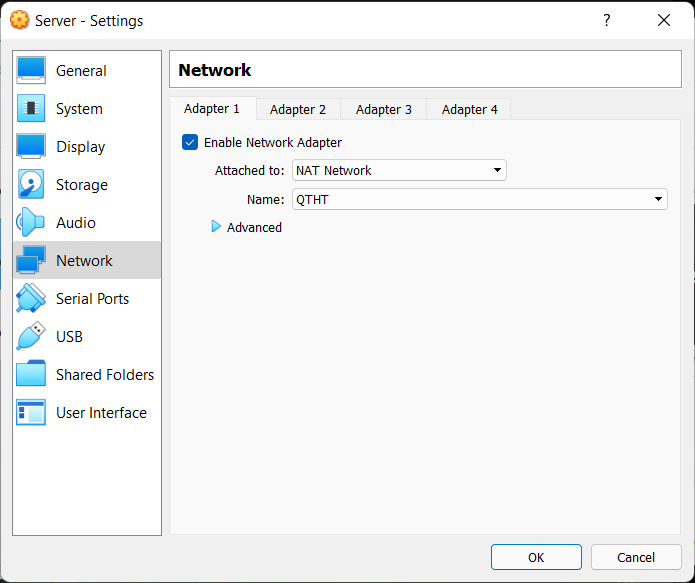


Hình 1: Tạo NAT Network tên "QTHT" có địa chỉ mạng là 10.0.2.0/24

- Tạo 2 máy ảo với thông tin như sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | |  |  | **Desktop** | |
| **Host name** | server |  |  | **Host name** | desktop |
| **Hệ điều hành** | CentOS 8 |  |  | **Hệ điều hành** | Lubuntu 20.04  hoặc 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** | 10.0.2.2 |  |  | **IP**  **Subnet mask**  **Gateway**  **DNS** | Cấu hình động sử dụng dịch vụ DHCP trên server |
| **Subnet mask** | 255.255.255.0 |  |  |
| **Gateway** | 10.0.2.1 |  |  |
| **DNS** | 10.0.2.1 |  |  |

* **Máy ảo Server (CentOS 8)**
  + Cài đặt NAT Network với Name là: “QTHT”

****

Hình 2: Cài đặt NAT Network cho máy Server

* + Cấu hình kết nối Ethernet

*nano /etc/sysconfig/network-scripts/ifcfg-enp0s3*

*DEVICE=enp0s3*

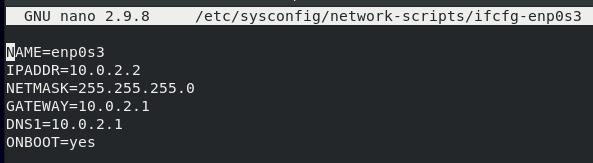
*IPADDR=10.0.2.2*

*NETMASK=255.255.255.0*

*GATEWAY=10.0.2.1*

*DNS1=10.0.2.1*

*ONBOOT=yes*



Hình : Cấu hình kết nối Ethernet cho máy ảo Server

* + Khởi động lại dịch vụ mạng

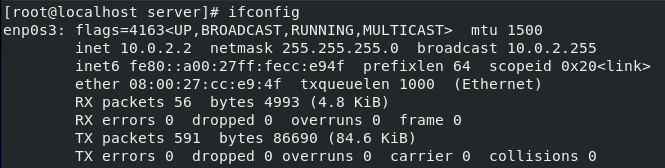
*systemctl restart NetworkManager.service*



Hình : Khởi động lại dịch vụ mạng

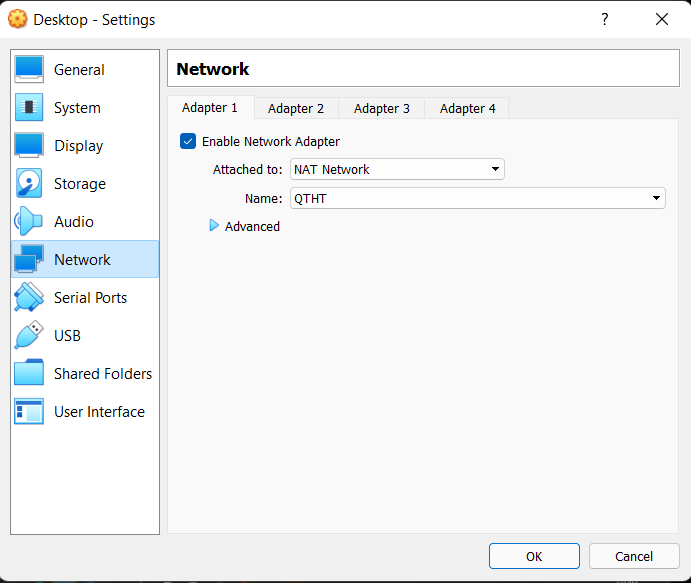
* + Cấu hình mạng hiện tại của máy

*ifconfig -a*



Hình : Cấu hình của máy ảo Server

* **Máy ảo Desktop (Lubuntu 20.04)**
  + Cài đặt NAT Network với Name là: “QTHT”

****

Hình 6: Cài đặt NAT Network cho máy Desktop

***Lưu ý:*** *Khi cài hệ điều hành Lubuntu 20.04 nên tắt (disable) card mạng trước khi cài.*

## **1.2**. (10%) Để quản lý các bộ phận và người dùng trong công ty, hãy tạo các nhóm người dùng (group) và người dùng (user) trên server như sau. Lưu ý chỉ có các thành viên trong ban giám đốc mới có quyền sudo trên server.

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

* Tạo các người dùng trên máy server, sau đó đặt mật khẩu cho người dùng bằng các lệnh

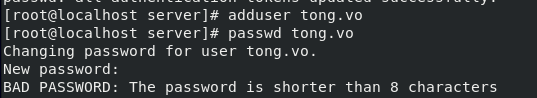
*adduser < username >*

*passwd < username >*

* + Tạo người dùng tong.vo và đặt mật khẩu cho người dùng

*adduser tong.vo*

*passwd tong.vo*



Hình : Tạo người dùng "tong.vo" và đặt mật khẩu cho người dùng đó

* Tạo các nhóm người dùng, sau đó thêm người dùng vào các nhóm người dùng đã tạo

*groupadd < tên nhóm người dùng >*

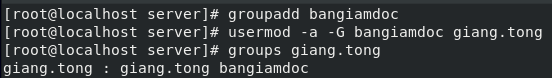
*usermod -a -G < tên nhóm người dùng > < tên người dùng >*

* + Tạo nhóm người dùng “bangiamdoc”, thêm người dùng “giang.tong” vào nhóm, và kiểm tra nhóm người dùng của “giang.tong” bằng các lệnh

*groupadd bangiamdoc*

*usermod -a -G bangiamdoc giang.tong*

*groups giang.tong*

**

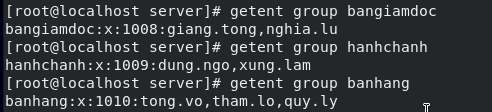
Hình : Tạo nhóm người dùng "bangiamdoc" và thêm người dùng "giang.tong" vào nhóm

* Liệt kê tất cả người dùng trong một nhóm bằng lệnh

*getent group < tên nhóm người dùng >*

* + Để liệt kê tất cả người dùng trong nhóm “hanh.chanh”, sử dụng lệnh

*getent group hanhchanh*

**

Hình : Liệt kê tất cả người dùng trong nhóm

* Cấp quyền sudo cho nhóm người dùng “*bangiamdoc”* bằng cách:
  + Truy cập vào tập tin */etc/sudoers*

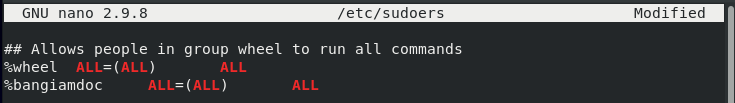
*nano /etc/sudoers*



Hình : Truy cập vào tập tin /etc/sudoers

* + Thêm dòng lệnh sau vào tập tin để cấp quyền **sudo** cho nhóm người dùng

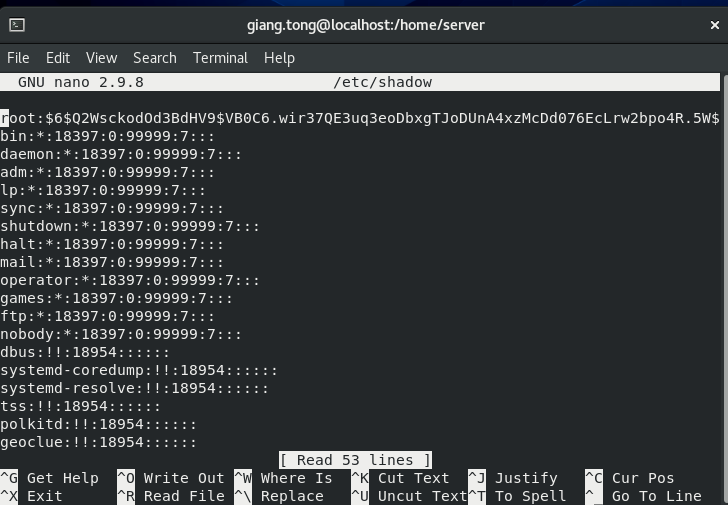
*%bangiamdoc ALL=(ALL) ALL*



Hình : Thêm nhóm người dùng "bangiamdoc" vào nhóm người dùng có quyền sudo

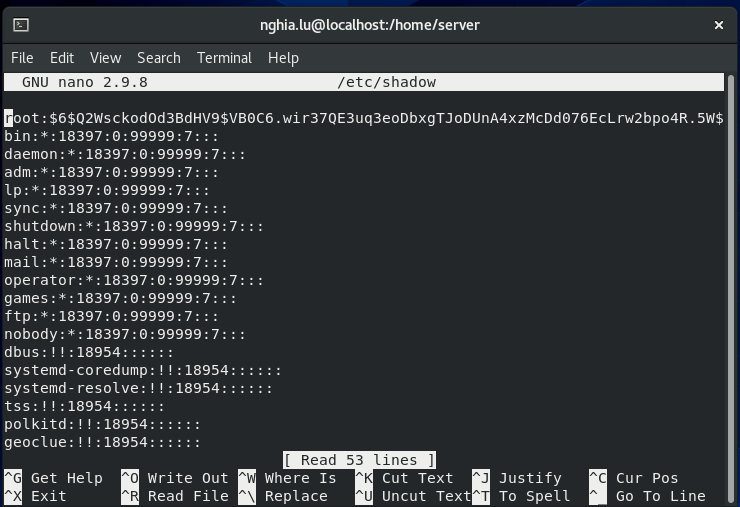
* Các người dùng nằm trong nhóm người dùng “bangiamdoc” đã có thể truy cập vào tập tin */etc/shadow* bằng câu lệnh **sudo**





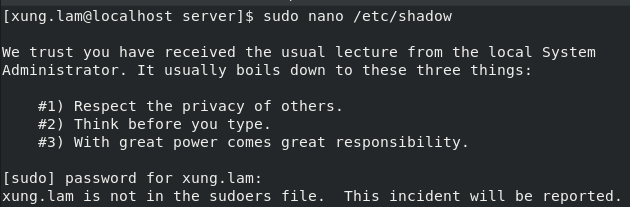
Hình : Người dùng "giang.tong" có thể truy cập vào tập tin /etc/shadow thông qua lệnh **sudo**





Hình : Người dùng "nghia.lu" có thể truy cập vào tập tin /etc/shadow thông qua lệnh **sudo**

* Người dùng “lam.xung” không nằm trong nhóm người dùng “bangiamdoc” nên bị từ chối quyền truy cập qua **sudo**

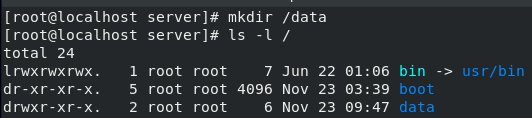


Hình : Người dùng "lam.xung" không thể truy cập vào tập tin /etc/shadow thông qua lệnh sudo

## **1.3.** (10%) Tạo thư mục /data trên server và phân quyền sao cho thành viên ban giám đốc có toàn quyền (read, write và execute), các trưởng phòng có quyền read và execute, các nhân viên khác không có quyền gì. Ngoài ra chỉ chủ sở hữu tập tin có quyền xóa hoặc đổi tên tập tin trong thư mục.

* Tạo thư mục /data

*mkdir /data*

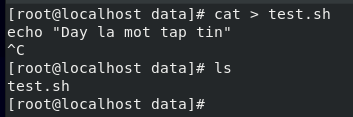


Hình : Tạo thư mục /data và kiểm tra phân quyền

* Tạo tập tin test.sh bên trong thư mục /data và thêm 1 dòng lệnh

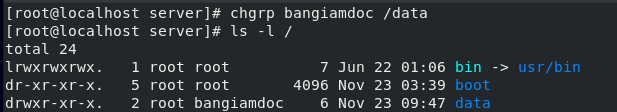
*cat > test.sh*

*echo “Day la mot tap tin”*



* Chuyển nhóm chủ sở hữu của thư mục /data sang nhóm “bangiamdoc” để thành viên trong nhóm có toàn quyền (read, write và execute)

*chgrp -R bangiamdoc /data*



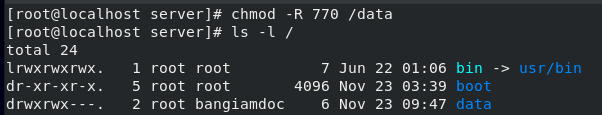
Hình : Chuyển nhóm chủ sở hữu của thư mục /data sang nhóm "bangiamdoc"

Tham số *-R* trong câu lệnh để áp dụng phân quyền cho tất cả các file và folder bên trong thư mục /data.

* Phân quyền truy cập cho chủ sở hữu và nhóm chủ sở hữu có toàn quyền (read, write và execute), các người dùng còn lại không có quyền gì

*chmod -R 770 /data*

Tham số *-R* trong câu lệnh để áp dụng phân quyền cho tất cả các file và folder bên trong thư mục /data.

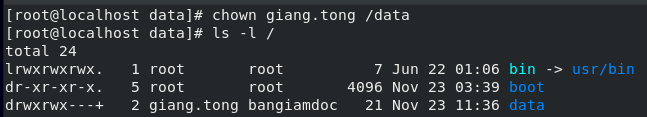


Hình : Phân quyền truy cập cho chủ sở hữu, nhóm chủ sở hữu và các người dùng khác

* Chuyển chủ sở hữu của thư mục /data từ “*root”* sang người dùng “*giang.tong”*

*chown -R giang.tong /data*

Tham số *-R* trong câu lệnh để áp dụng phân quyền cho tất cả các file và folder bên trong thư mục /data.



Hình : Chuyển chủ sở hữu của thư mục /data từ "root" sang "giang.tong"

* Thêm quyền đọc và thực thi cho các trưởng phòng gồm “*dung.ngo*” và “*tong.vo*” bằng lệnh

*setfacl -R -m u:dung.ngo:rx /data*

*setfacl -R -m u:tong.vo:rx /data*



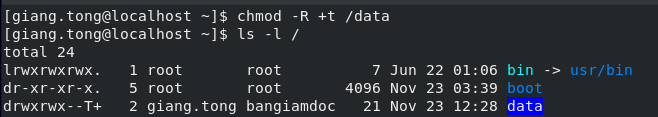
Hình : Thêm quyền đọc và thực thi cho các người dùng là trưởng phòng

Tham số *-R* trong câu lệnh để áp dụng phân quyền cho tất cả các file và folder bên trong thư mục /data.

Tham số *-m (--modify)* trong câu lệnh dùng để xác định câu lệnh này là để sửa đổi danh sách kiểm soát truy cập tệp.

* Thay đổi quyền của thư mục để chỉ có chủ sở hữu mới có thể xóa hoặc đổi tên tập tin trong thư mục, sử dụng lệnh

*chmod -R +t /data*

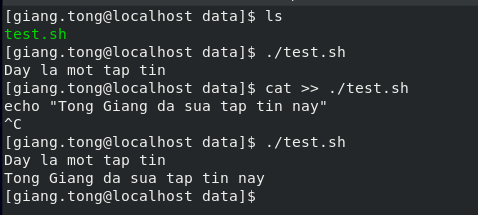


Hình : Thay đổi quyền của thư mục để chỉ chủ sở hữu mới có thể xóa hoặc đổi tên tập tin trong thư mục

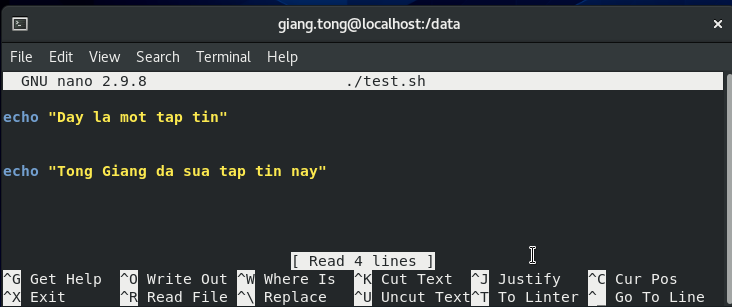
Tham số *-R* trong câu lệnh để áp dụng phân quyền cho tất cả các file và folder bên trong thư mục /data.

Tham số *+t* trong câu lệnh để chỉ ra đây là chế độ “Sticky bit”, được sử dụng cho các thư mục chia sẻ. Chỉ duy nhất owner file (và root) mới có quyền rename hay xóa các file, thư mục khi nó được set sticky bit.

* Người dùng “*giang.tong”* là thành viên ban giám đốc nên có thể read, write và execute tập tin trong thư mục /data

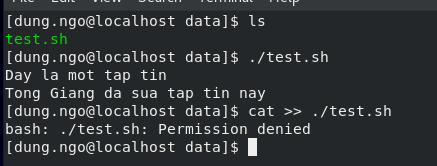


Hình : Người dùng "giang.tong" có thể ghi và thực thi trên tập tin test.sh nằm trong thư mục /data

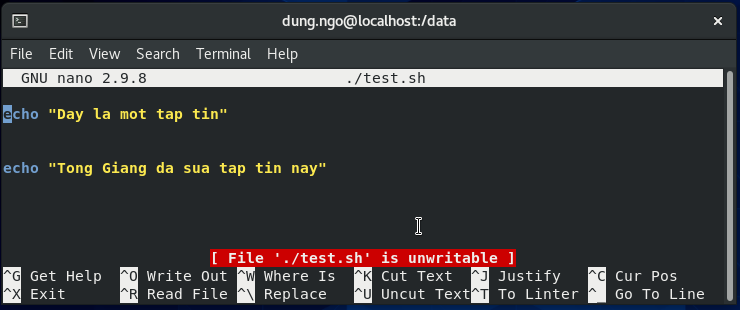


Hình : Người dùng "giang.tong" có thể đọc tập tin test.sh nằm trong thư mục /data

* Người dùng “*dung.ngo”* là trưởng phòng nên có thể read và execute tập tin trong thư mục /data

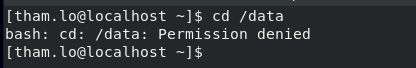


Hình : Người dùng "dung.ngo" có thể thực thi thư mục test.sh nằm trong thư mục /data



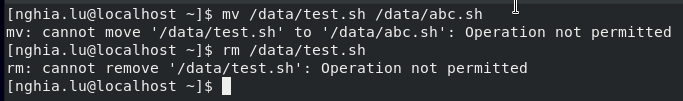
Hình : Người dùng "dung.ngo" không thể ghi trên thư mục test.sh nằm trong thư mục /data

* Người dùng “*tham.lo”* là nhân viên nên không có quyền gì trên thư mục /data, vì thế không thể truy cập được vào thư mục /data



Hình : Người dùng "tham.lo" không thể truy cập được vào thư mục /data

* Người dùng “nghia.lu” là thành viên ban giám đốc nhưng không thể thay đổi tên tập tin hoặc xóa tập tin trong thư mục /data do chỉ có chủ sở hữu mới có quyền trên nó.



Hình : Người dùng "nghia.lu" không thể thay đổi tên tập tin hoặc xóa tập tin trong thư mục /data

## **1.4.** (10%) Cài đặt và cấu hình dịch vụ DHCP trên server để cấu hình mạng tự động cho các máy desktop.

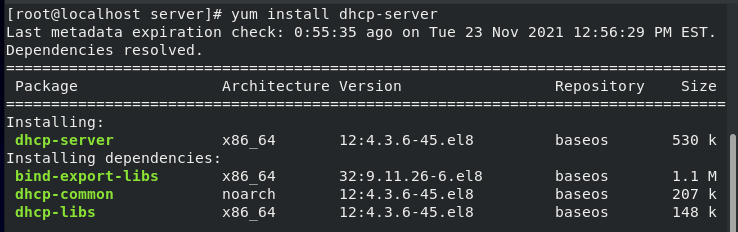
+ Địa chỉ IP của desktop: trong dãy 10.0.2.50/24 đến 10.0.2.100/24

+ Địa chỉ gateway: 10.0.2.1

+ DNS server: 10.0.2.2 và 8.8.8.8

* Cài đặt dịch vụ DHCP trên máy server

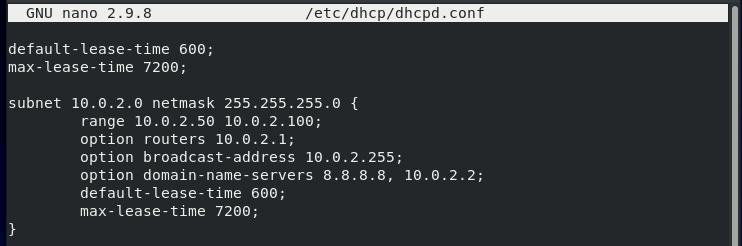
*yum install dhcp-server*



Hình : Cài đặt dịch vụ DHCP trên server

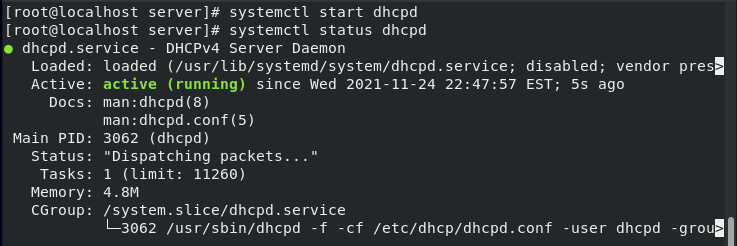
* Cấu hình dịch vụ DHCP qua tập tin dhcpd.conf

*nano /etc/dhcp/dhcpd.conf*



Hình : Cấu hình dịch vụ DHCP qua tập tin /etc/dhcp/dhcpd.conf

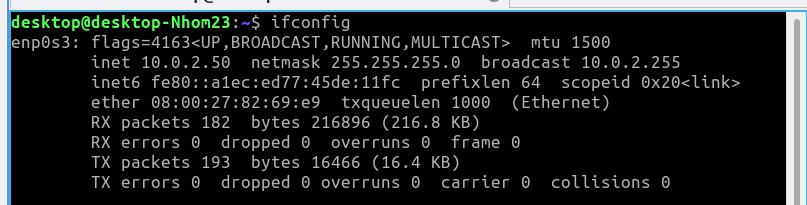
* + Dịch vụ DHCP sẽ cung cấp địa chỉ IP cho nhánh mạng 10.0.2.0, có mặt nạ mạng là 255.255.255.0
  + Phạm vi (range) từ 10.0.2.50 đến 10.0.2.100
  + Địa chỉ Gateway (routers) là 10.0.2.1
  + Địa chỉ quảng bá (broadcast) là 10.0.2.255
  + DNS server là 8.8.8.8 và 10.0.2.2
  + Thời gian thuê mặc định là 600 giây (10 phút) và thời gian thuê tối đa là 7200 giây (2 giờ). Máy chủ DHCP sẽ dự trữ địa chỉ IP trong ít nhất 10 phút và tối đa 2 giờ cho một thiết bị cụ thể.
* Khởi động dịch vụ DHCP



Hình : Khởi động dịch vụ DHCP

* Khởi động máy ảo Desktop (Lubuntu) và kiểm tra địa chỉ IP

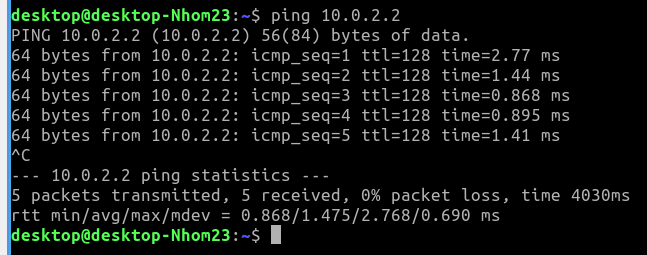
*ifconfig*



Hình : Kiểm tra địa chỉ IP trên máy Lubuntu

* Từ máy Lubuntu ping tới CentOS

*ping 10.0.2.2*



Hình : Từ máy Lubuntu ping tới CentOS

Kết quả cho thấy dịch vụ DHCP đã chạy thành công.

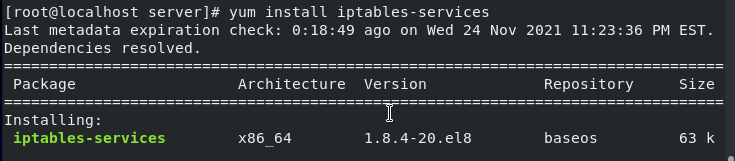
## **1.5.** (10%) Cài đặt và cấu hình tường lửa trên server để cho phép desktop:

+ Có thể truy cập các dịch vụ DNS, DHCP, SSH, Web, FTP trên server. Các dịch vụ khác KHÔNG truy cập được.

+ Chỉ desktop có thể ping tới server, các máy khác KHÔNG ping được.

* Cài đặt tường lửa *iptables*
  + Cài đặt dịch vụ *iptables*

*yum install iptables-service*

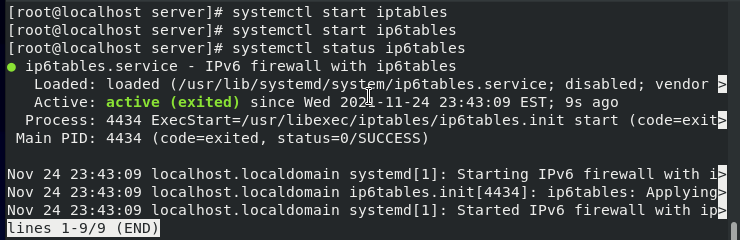
**

Hình : Cài đặt dịch vụ iptables

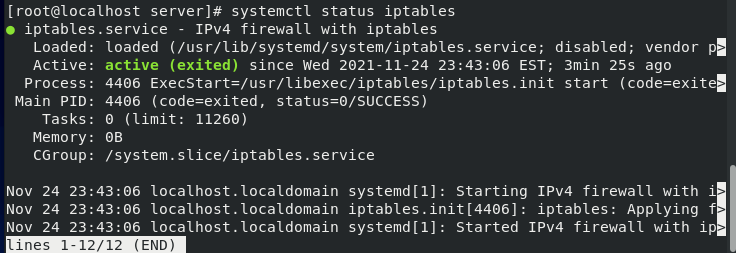
* + Khởi động dịch vụ *iptables*

*systemctl start iptables*

*systemctl start ip6tables*

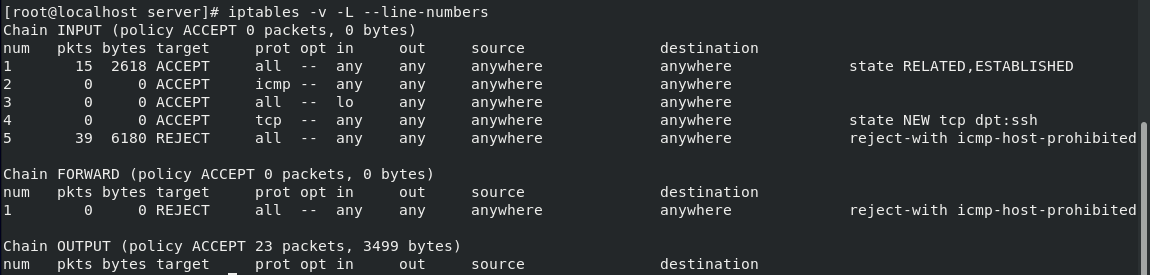


Hình : Khởi động dịch vụ iptables



Hình : Trạng thái của dịch vụ iptables

* Kiểm tra các rules hiện có trong *iptables*

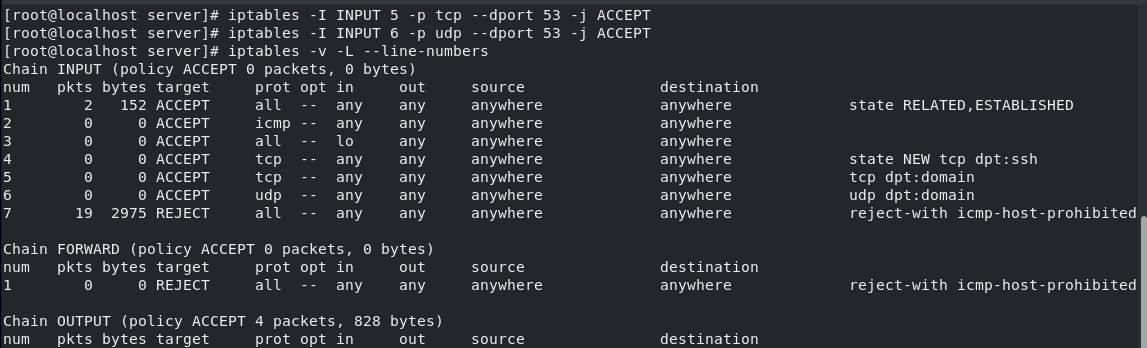


Hình : Các rules hiện có trong iptables

* Ta có thể thấy rule số 4 trong iptables cho phép dịch vụ SSH truy cập được vào máy Server, nên không cần cài đặt gì thêm
* Thêm rule cho phép dịch vụ DNS truy cập được vào máy Server

*iptables -I INPUT 5 -p tcp --dport 53 -j ACCEPT*

*iptables -I INPUT 6 -p tcp --dport 53 -j ACCEPT*

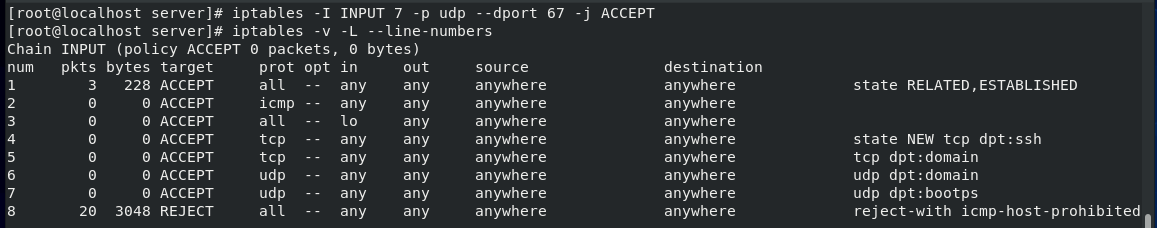


Hình : Thêm rule cho phép dịch vụ DNS truy cập được vào máy Server

Dịch vụ DNS hoạt động ở 2 giao thức là TCP và UDP ở cổng 53.

* Thêm rule cho phép dịch vụ DHCP truy cập được vào máy Server

*iptables -I INPUT 7 -p udp --dport 67 -j ACCEPT*



Hình : Thêm rule cho phép dịch vụ DHCP truy cập được vào máy Server

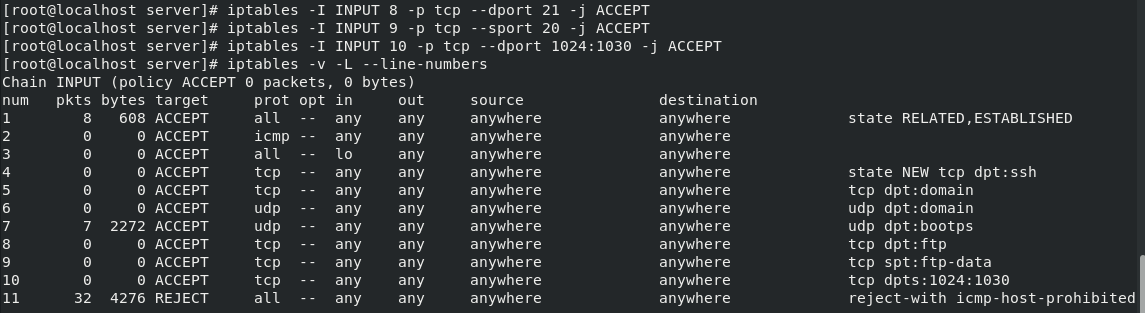
Dịch vụ DHCP giao tiếp bằng UDP và sử dụng cổng 67 để nghe thông tin từ các client.

* Thêm rule cho phép dịch vụ FTP truy cập được vào máy Server

*iptables -I INPUT 8 -p tcp --dport 21 -j ACCEPT*

*iptables -I INPUT 9 -p tcp --sport 20 -j ACCEPT*

*iptables -I INPUT 10 -p tcp --dport 1024:1030 -j ACCEPT*



Hình : Thêm rule cho phép dịch vụ FTP truy cập được vào máy Server

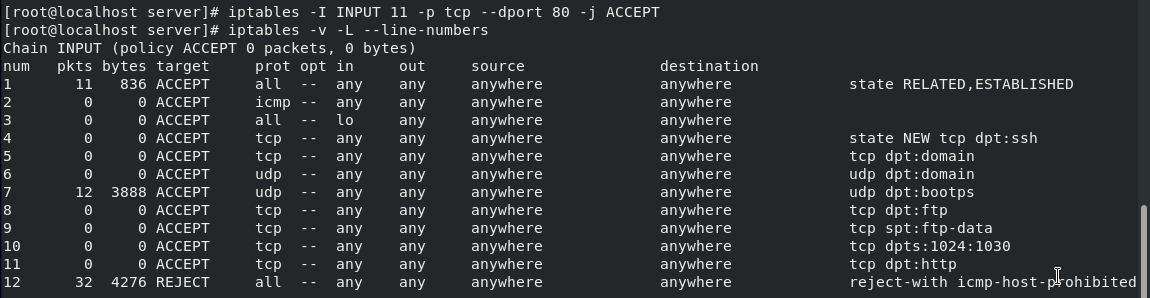
Dịch vụ FTP giap tiếp bằng TCP sử dụng cổng 21 để thiết lập nối kết giữa 2 máy tính (hoặc máy chủ) và cổng 20 để truyền dữ liệu.

Tham số --dport là cổng đích, --sport là cổng nguồn.

Cổng 1024-1030: các cổng ví dụ cho chế độ thụ động được chỉ định trong cấu hình máy chủ FTP.

* Thêm rule cho phép dịch vụ Web truy cập được vào máy Server

*iptables -I INPUT 11 -p tcp --dport 80 -j ACCEPT*



Hình : Thêm rule cho phép dịch vụ Web truy cập được vào máy Server

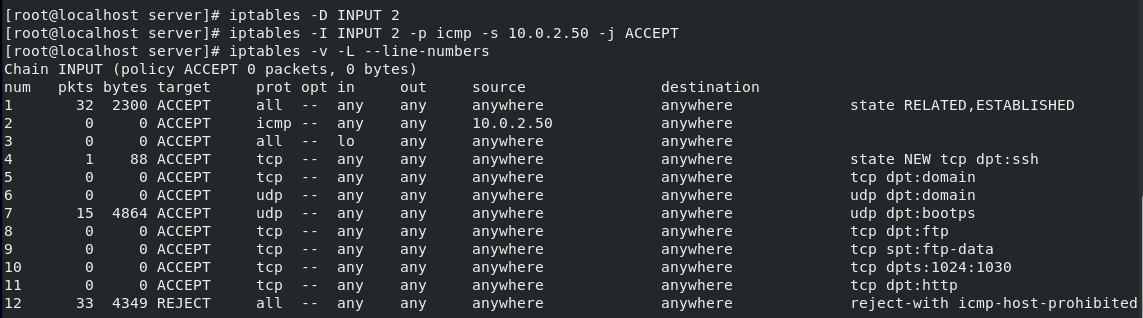
Dịch vụ Web giao tiếp bằng TCP trên cổng 80.

* Thay đổi rule để chỉ Desktop có thể ping tới Server, các máy khác không ping được
  + Xóa rule số 2 là rule cho phép tất cả các thiết bị có thể gửi ICMP tới Server

*iptables -D INPUT 2*

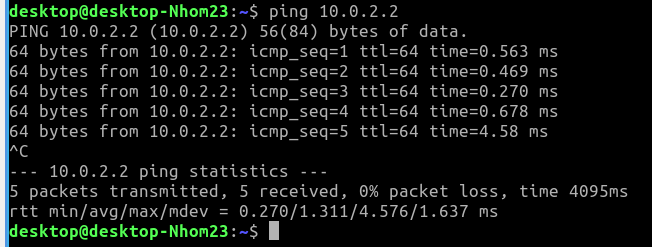
* + Thêm rule để chấp nhận địa chỉ IP của Desktop có thể gửi ICMP tới Server

*iptables -I INPUT 2 -p icmp -s 10.0.2.50 -j ACCEPT*

**

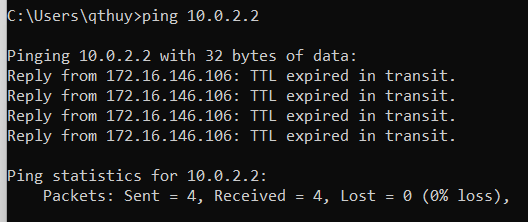
Hình : Thay đổi rule để chỉ Desktop có thể ping tới Server

* Từ máy Desktop ping tới Server



Hình : Từ máy Desktop ping tới Server

* Từ máy thực Windows ping tới máy ảo CentOS (Server)



Hình : Từ máy thực Windows ping tới máy ảo CentOS (Server)

Không thể thực hiện được lệnh ping do Server đã chặn ICMP từ các máy khác trừ máy

Desktop

* Sao lưu các luật trong iptables

*cp /etc/sysconfig/iptables /etc/sysconfig/iptables.orig*

*iptables-save > /etc/sysconfig/iptables*

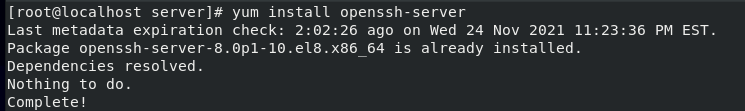


Hình : Sao lưu rules trong iptables

## **1.6.** (10%) Cài đặt và cấu hình dịch vụ SSH để cho phép điều khiển từ xa server. Lưu ý: chỉ có thành viên ban giám đốc và các trưởng phòng mới có quyền điều khiển từ xa server. Tài khoản root không được nối kết tới server từ xa.

* Cài đặt dịch vụ SSH cho Server

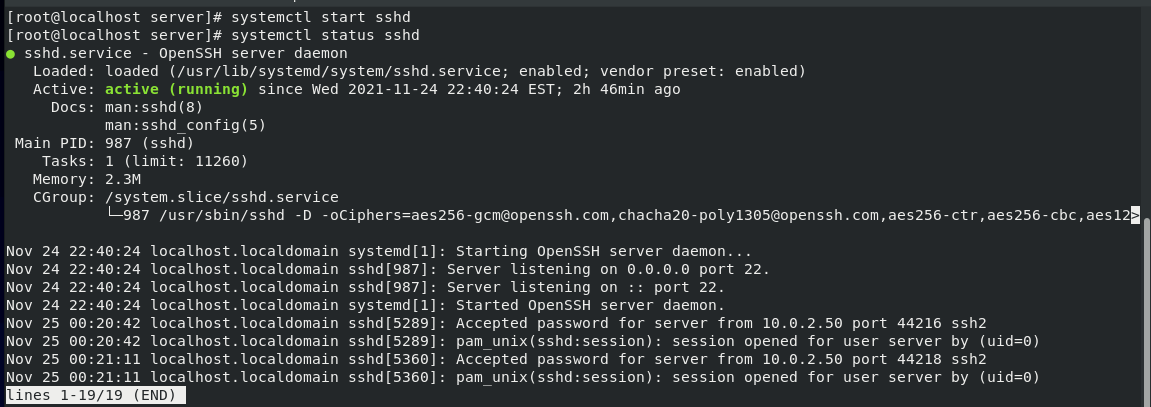
*yum install openssh-server*



Hình : Cài đặt dịch vụ SSH cho Server

* Khởi động dịch vụ SSH

*systemctl start sshd*

**

Hình : Khởi động dịch vụ SSH

* Cấu hình dịch vụ SSH cho Server

*nano /etc/ssh/sshd\_config*

* + Trong tập tin *sshd\_config,* thêm các dòng lệnh sau
    - Không cho phép tài khoản *root* đăng nhập

*PermitRootLogin no*

**

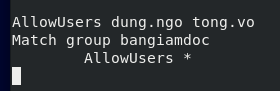
Hình : Không cho phép tài khoản root đăng nhập

* + - Cho phép group “*bangiamdoc*” và các trưởng phòng đăng nhập, nếu đăng nhập bằng user ngoài các user chỉ định trong *AllowUsers* và không nằm trong các group chỉ định trong *Match group* thì sẽ nhận được thông báo:.

*AllowUsers dung.ngo tong.vo*

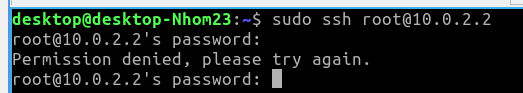
*Match group bangiamdoc*

*AllowUsers \**



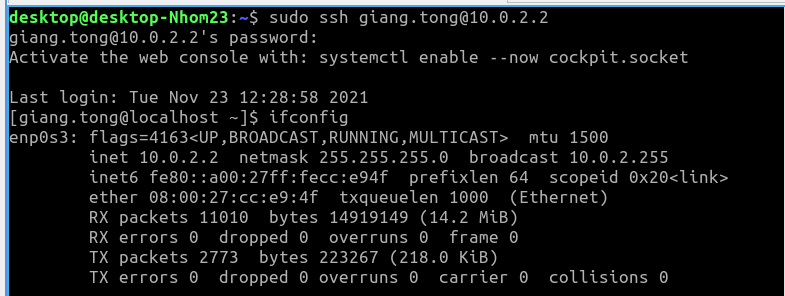
Hình : Cho phép group "bangiamdoc" và các trưởng phòng đăng nhập

* Điều khiển Server từ xa trên máy Desktop sử dụng dịch vụ SSH
  + Khi đăng nhập bằng tài khoản *root* để điều khiển từ xa bị từ chối



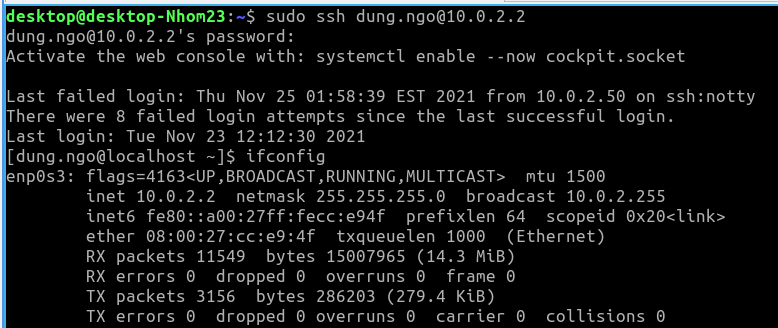
Hình : Tài khoản root bị từ chối đăng nhập

* + Tài khoản trong nhóm “*bangiamdoc*” đăng nhập thành công



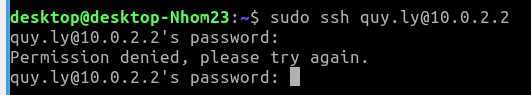
Hình : Tài khoản giang.tong đăng nhập thành công

* + Tài khoản là trưởng phòng đăng nhập thành công



Hình : Tài khoản dung.ngo đăng nhập thành công

* + Tài khoản nhân viên không thể đăng nhập



Hình : Tài khoản nhân viên bị từ chối đăng nhập

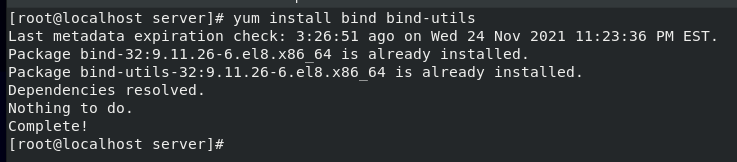
## **1.7.** (5%)Cài đặt và cấu hình dịch vụ DNS trên server để phân giải tên miền *trasualsb.com*

Tên miền: *www.trasualsb.com <----> IP:* 10.0.2.2 (server IP)

Tên miền: *ftp.trasualsb.com <----> IP:* 10.0.2.2 (server IP)

* Cài đặt BIND và các công cụ cần thiết:

*yum install bind bind-utils*

**

Hình : Cài đặt BIND và các công cụ cần thiết

* Cấu hình DNS server

*nano /etc/named.conf*

Thêm vào file các câu lệnh sau

*options {*

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

*…*

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

*}*

*zone “10.0.2.2” IN {*

*type master;*

*file “forward.trasualsb”;*

*allow-update { none;} ;*

*};*

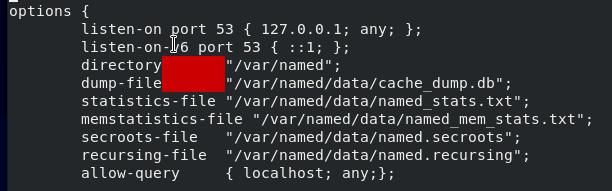
*zone “2.0.10.in-addr.arpa” IN {*

*type master;*

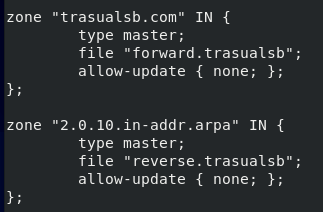
*file “reverse.trasualsb”;*

*allow-update { none;} ;*

*};*

**

Hình : Thêm vào file /etc/named.conf các câu lệnh



Hình : Thêm vào file /etc/named.conf các câu lệnh

* Tạo tập tin cấu hình phân giải xuôi
  + Sao chép tập tin /var/named/named.localhost

*cp /var/named/named.localhost /var/named/forward.trasualsb*

*chgrp named /var/named/forward.trasualsb*

*nano /var/named/forward.trasualsb*

* + Cấu hình file /var/named/forward.trasualsb

*$TTL 1D*

*@ IN SOA @ trasualsb.com. (*

*0 ;Serial*

*1D ;Refresh*

*1H ;Retry*

*1W ;Expire*

*3H ;Minimum TTL*

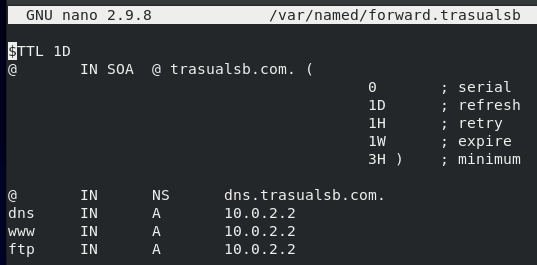
*)*

*@ IN NS dns.trasualsb.com.*

*dns IN A 10.0.2.2*

*www IN A 10.0.2.2*

*ftp IN A 10.0.2.2*



Hình : Tạo tập tin cấu hình phân giải xuôi

* Tạo tập tin cấu hình phân giải ngược:
  + Sao chép tập tin /var/named/named.localhost

*cp /var/named/forward.trasualsb /var/named/reverse.trasualsb*

*chgrp named /var/named/reverse.trasualsb*

*nano /var/named/reverse.trasualsb*

* + Cấu hình file /var/named/reverse.trasualsb

*$TTL 1D*

*@ IN SOA @ trasualsb.com. (*

*0 ;Serial*

*1D ;Refresh*

*1H ;Retry*

*1W ;Expire*

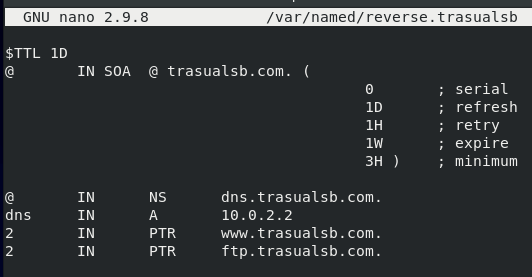
*3H ;Minimum TTL*

*)*

*@ IN NS dns.trasualsb.com.*

*dns IN A 10.0.2.2*

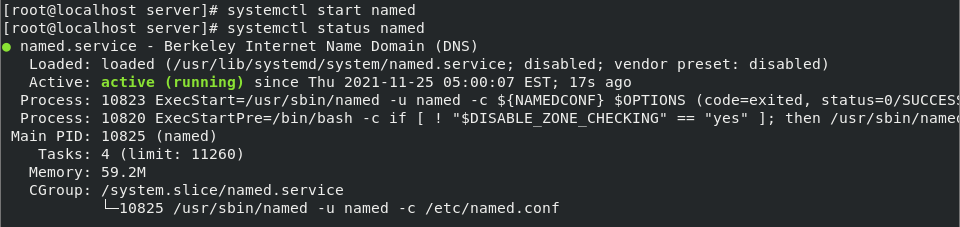
*2 IN PTR www.trasualsb.com.*



Hình : Tạo tập tin cấu hình phân giải ngược

* Khởi động dịch vụ DNS

*systemctl start named*

**

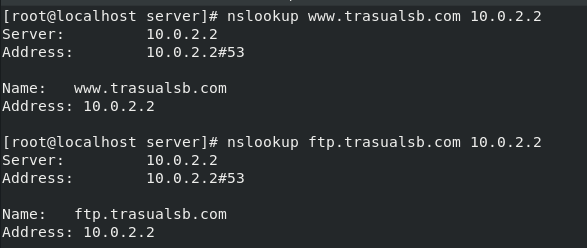
Hình : Khởi động dịch vụ DNS

* Kiểm tra phân giải tên miền bằng lệnh

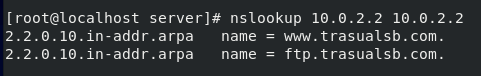
*nslookup www.trasualsb.com 10.0.2.2*

*nslookup ftp.trasualsb.com 10.0.2.2*

*nslookup 10.0.2.2 10.0.2.2*

**

Hình : Kiểm tra phân giải tên miền xuôi



Hình : Kiểm tra phân giải tên miền ngược

## **1.8.** (5%) Cài đặt và cấu hình dịch vụ máy chủ Web trên server sử dụng docker. Tạo một trang web cho công ty có tên miền *www.trasualsb.com* với nội dung trang chủ giới thiệu về các thành viên trong công ty.

* Tìm kiếm và thực thi dịch vụ máy chủ Web

*sudo docker search httpd*

*sudo docker run -d -it -p 80:80 httpd*

Các tham số:

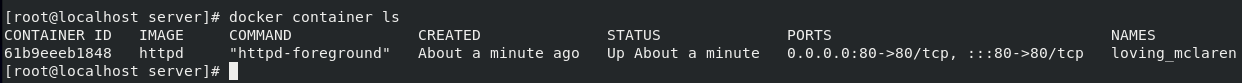
-d: chạy dịch vụ ở chế độ nền

-it: tạo kênh giao tiếp với container

-p 80:80 : lấy cổng 80 trên container đưa ra cổng 80 của máy CentOS

* Lấy shell của container chạy dịch vụ httpd
  + Liệt kê danh sách các container

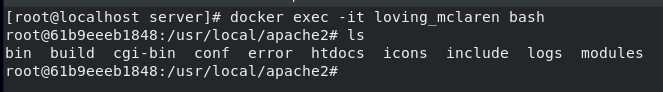
*docker container ls*

**

Hình : Liệt kê danh sách các container

* + Lấy shell container loving\_mclaren đang chạy dịch vụ httpd

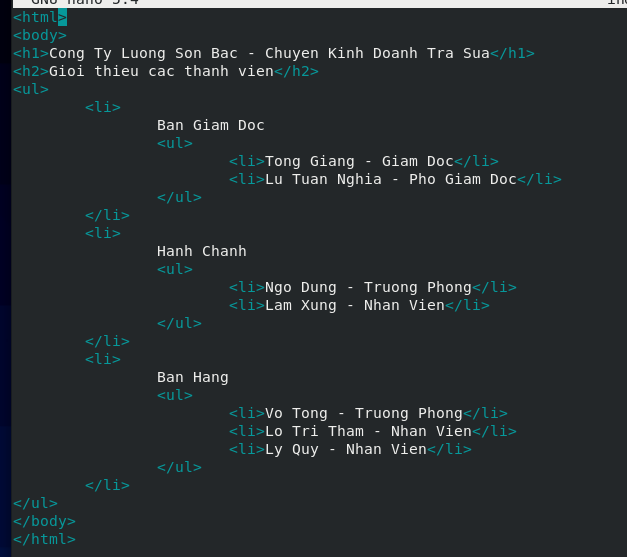
*docker exec -it loving\_mclaren bash*

**

Hình : Lấy shell container loving\_mclaren đang chạy dịch vụ httpd

* Chỉnh sửa file *index.html* trong thư mục */usr/local/apache2/htdocs* để chỉnh sửa nội dung trang chủ giới thiệu về các thành viên trong công ty

*nano htdocs/index.html*

**

Hình : Chỉnh sửa nội dung trang chủ

* Truy cập trang web thông qua địa chỉ IP (10.0.2.2)

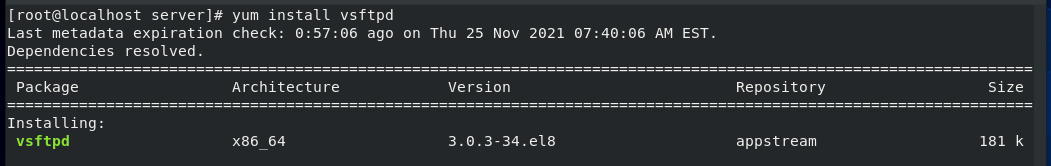


Hình : Nội dung website trang chủ của công ty

## **1.9.** (5%) Cài đặt và cấu hình dịch vụ máy chủ FTP trên server. Cấu hình chỉ cho phép người dùng download (không được upload) dữ liệu từ thư mục **/data** trên server. Không cho phép người dùng chuyển sang thư mục khác, chỉ được làm việc trong thư mục **/data**

* Cài đặt dịch vụ FTP cho máy Server

*yum install vsftpd*



Hình : Cài đặt dịch vụ FTP cho máy Server

* Cấu hình dịch vụ FTP

*nano /etc/vsftpd/vsftpd.conf*

* + Thêm các dòng lệnh sau vào file
    - Người dùng ẩn danh không được phép đăng nhập vào FTP server

*anonymous\_enable=NO*

* + - Cho phép người dùng cục bộ đăng nhập vào FTP server

*local\_enable=YES*

* + - Người dùng di chuyển đến home directory của mình sau khi đăng nhập

*chroot\_local\_user=YES*

* + - Xác định các quyền cho các tệp hoặc thư mục mới được tạo

*local\_umask=022*

* + - Cho phép sử dụng chroot setting

*allow\_writeable\_chroot=YES*

* + - Thư mục mặc định khi đăng nhập vào

*local\_root=/data*

* + - Cho phép người dùng chỉ download (không upload) dữ liệu

*write\_enable=NO*

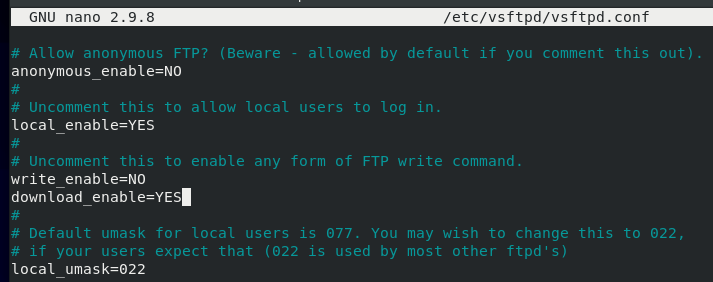
*download\_enable=YES*



Hình : Cấu hình dịch vụ FTP

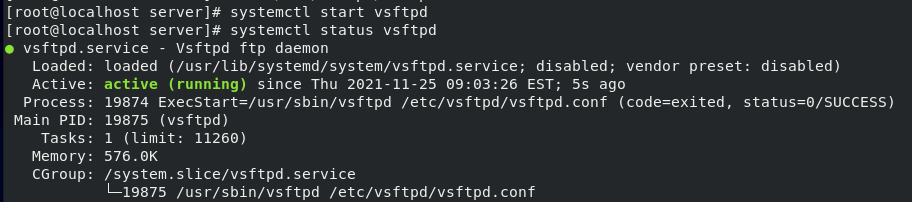


Hình : Cấu hình dịch vụ FTP



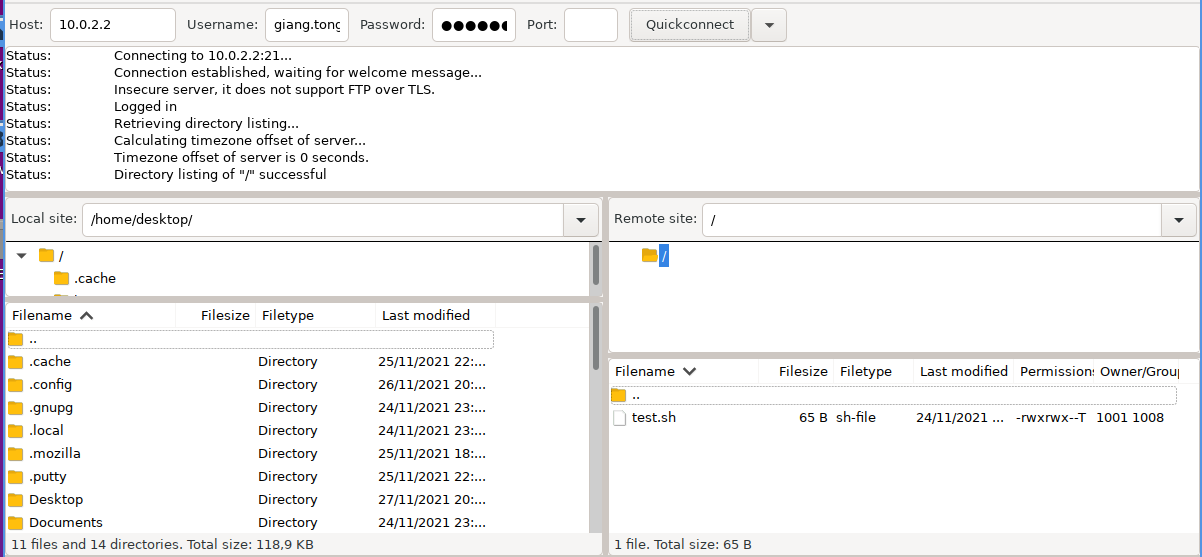
Hình : Cấu hình dịch vụ FTP

* Khởi động dịch vụ FTP



Hình : Khởi động dịch vụ FTP

* Từ máy Desktop kết nối đến Server bằng dịch vụ FTP sử dụng FileZilla



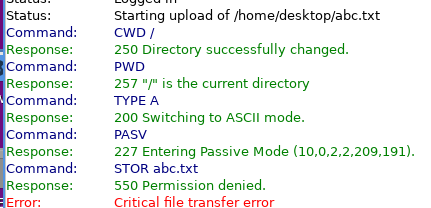
Hình : Kết nối đến Server bằng tài khoản “giang.tong”

* Khi kết nối đến Server, dịch vụ tự động chuyển đến thư mục /data và không hiển thị các thư mục khác, vì thế người dùng chỉ có thể làm việc trong thư mục /data



Hình : Các tập tin có trong thư mục /data

* Người dùng không thể upload dữ liệu lên Server



Hình : Upload tập tin “abc.txt” lên Server và nhận được phản hồi “Permission denined”

* Người dùng có thể download dữ liệu từ Server



Hình : Tải tập tin “test.sh” từ Server về Desktop

## **1.10.** (5%) Sử dụng dịch vụ cron và shell script thực hiện công việc sao lưu dữ liệu mỗi ngày, mỗi tuần, mỗi tháng như sau:

+ Dữ liệu cần sao lưu: /home, /data, /etc

+ Nơi lưu dữ liệu cần 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 lưu với tên như sau: backup\_<thứ> (ví dụ: backup\_monday).

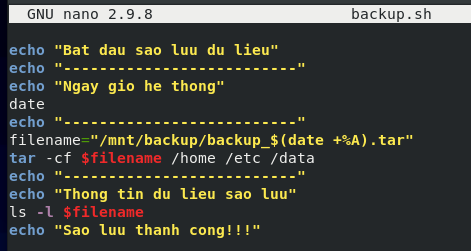
+ Sao lưu mỗi tuần: thực hiện vào lúc 23:59 ngày chủ nhật hàng tuần, dữ liệu sẽ được nén lưu với tên như sau: backup\_week<thứ tự tuần> (ví dụ: backup\_week1).

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

* Tạo thư mục nơi dữ liệu cần sao lưu

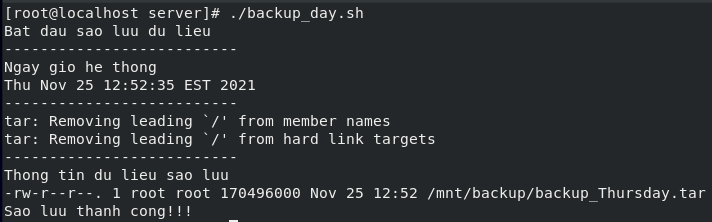
*mkdir /mnt/backup*

* Viết shell script sao lưu mỗi ngày và nén lưu với tên: backup\_<thứ>



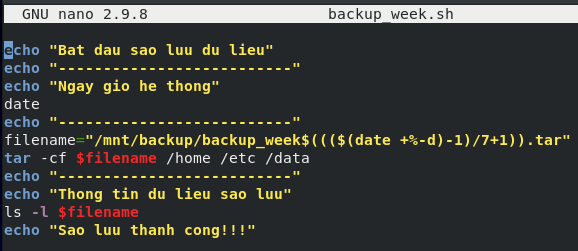
Hình : Script sao lưu mỗi ngày

* Shell script sao lưu mỗi ngày khi được thực thi



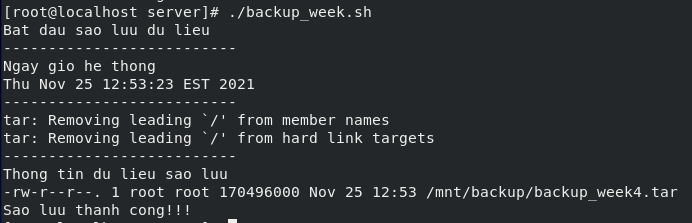
Hình : Shell script sao lưu mỗi ngày khi được thực thi

* Viết shell script sao lưu mỗi tuần và nén lưu với tên: backup\_week<thứ tự tuần>



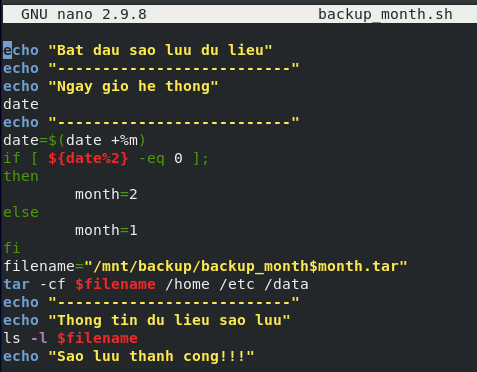
Hình : Script sao lưu mỗi tuần

* Shell script sao lưu mỗi tuần khi được thực thi



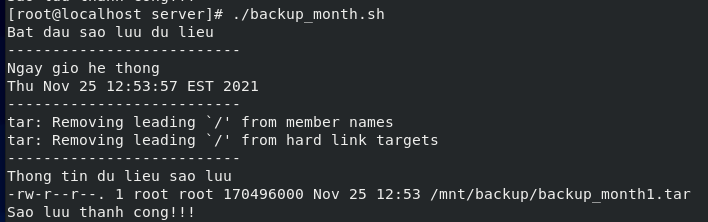
Hình : Shell script sao lưu mỗi tuần khi được thực thi

* Viết shell script sao lưu mỗi tháng và nén lưu với tên: backup\_month<tháng chẵn hoặc lẻ>



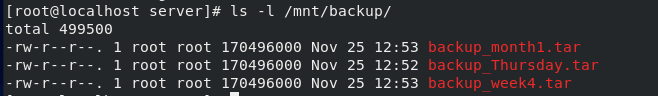
Hình : Script sao lưu mỗi tháng

* Shell script sao lưu mỗi tháng khi được thực thi



Hình : Shell script sao lưu mỗi tháng khi được thực thi

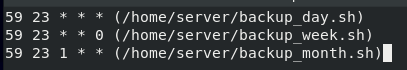
* Các file nén sau khi sao lưu được thực thi sẽ được lưu trong thư mục */mnt/backup*



Hình : Các file nén sau khi sao lưu được thực thi

* Lên lịch sao lưu định kì với *Cron*, để hiệu chỉnh file crontab ta thực hiện lệnh

*crontab -e*

**

Hình : Lên lịch sao lưu định kỳ với Cron

# 2. Hình thức bài báo cáo bài tập nhóm (20%)

Viết báo cáo trình bày các bước thực hiện công việc 1.1 đến 1.10:

- Trình bày rõ ràng đầy đủ từng bước thực hiện và có hình ảnh minh hoạ. Báo cáo ít lỗi chính tả, trình bày đẹp; có hình ảnh minh họa rõ, chi tiết, có mục lục, …

- Có sự phối hợp, thảo luận, hợp tác giữa các thành viên trong nhóm để thực hiện bài tập nhóm. Có phân chia công việc cụ thể giữa các thành viên trong nhóm.

--- Hết ---