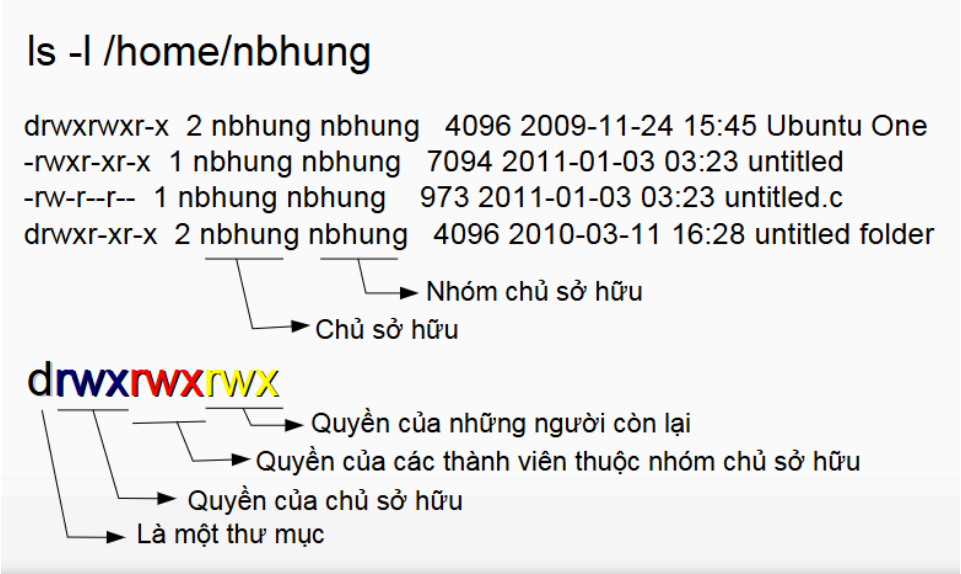
Quản trị người dùng trên Linux Quản trị người dùng

Lệnh cho biết tên tài khoản hiện hành
$whoami
nbhung
• Lệnh xem user id và các groups của một user
$id user-name
– Nếu không có user-name thì sẽ lấy login namecủa người dùng hiện tại
• uid <1000: system users
• uid>=1000: normal users
Thêm người dùng mới
sudo adduser user-name
Xóa/Khóa/Mở tài khoản
Xóa tài khoản
sudo deluser user-name
Xóa tài khoản user2 cùng với home của user
sudo deluser --remove-home user2
Xóa người dùng user2, có backup home cho user2
sudo deluser --remove-home --backup --backup-to /backup user2
Chuyển vào /backup
sudo tar xvjf user2.tar.bz
Copy /backup/home/user2 vào /home
sudo cp -r /backup/home/user2 /home
đánh lệnh add user2 và sudo chown -R user2 /home/user2
Khóa một tài khoản
sudo passwd -l user-name
Mở khóa một tài khoản
sudo passwd -u user-name
Nhà quản trị có quyền đặt lại (reset) mật khẩu cho các tài khoản khác
$sudo passwd user-name
Mỗi người dùng có thể tự đổi mật khẩu của mình
$passwd
Nhập lại mật khẩu cũ
Nhập 2 lần mật khẩu mới
Đặt chiều dài tối thiểu mật khẩu
File cấu hình /etc/pam.d/common-password
Thay đổi dòng
Password …..... sha512sha512 minlen=8
Xem trạng thái mật khẩu: sudo chage -l user1
Đặt thời hạn cho mật khẩu
• Account quá hạn (E) ngày 12/31/2025
• Tuổi thọ ít nhất (m) 5 ngày
• Tuổi thọ lâu nhất (-M) 90 ngày
• Không hoạt động (-I) 5 ngày sau khi mật khẩu quá hạn
• Cảnh báo trước (-W) 14 ngày trước khi mật khẩu quá hạn
sudo chage -E 12/31/2025 -m 5 -M 90 -I 5 -W 14 username

Thay đổi thư mục cá nhân
sudo usermod -d /home/new-home username

Quản trị nhóm người dùng

Thêm nhóm
sudo addgroup my-group
Thêm người dùng mới vào nhóm đã có
sudo adduser user-name my-group
Thêm người dùng đã có vào nhóm đã có
sudo usermod -G group-name user-name
Xóa nhóm
sudo delgroup my-group
Thay đổi nhóm chính của một người dùng
usermod -g new-primary-group user-name
Thay đổi nhóm chính tạm thời
newgrp new-temp-primary-group
Trở lại nhóm chính ban đầu:
exit
Xác định người quản trị nhóm
gpasswd -A user-admin group-name



Thay đổi quyền trên thư mục

chmod -R g+rwX,o+rX my-dir
● Đệ qui cho tất cả các thư mục hậu duệ
● Thêm quyền rwx cho nhóm chủ sở hữu và quyền rx cho những người khác một cách đệ qui trên các thư mục con và trên các tập tin có thể thực thi
● Đối với các tập tin không thực thi: Thêm quyền rw cho nhóm chủ sở hữu và quyền r cho những người khác

Quyền sticky trên thư mục

Một tập tin nằm trong thư mục có quyền stick chỉ được xóa bởi chủ sở hữu hoặc admin/root
chmod +t public-dir
● Gán quyền sticky trên thư mục public-dir

Quyền SETUID

Khi một **tệp thực thi** có gắn quyền `setuid`, nó sẽ **chạy với quyền của chủ sở hữu tệp đó**, **không phải người dùng thực thi**.

Bước 1: Tạo file C đơn giản

```
// hello.c
#include <stdio.h>
#include <unistd.h>

int main() {
    printf("Thực thi với UID: %d\n", geteuid());
    return 0;
}
```

Bước 2: biên dịch

```
gcc hello.c -o hello
```

Bước 3: Gán quyền sở hữu và setuid
sudo chown root:root hello
sudo chmod u+s hello
Bước 4: Kiểm tra
ls -l hello
-rwsr-xr-x 1 root root 16768 Jul 22 12:00 hello
^--- "s" nghĩa là setuid
Bước 5: Chạy chương trình với user thường
./hello
Thực thi với UID: 0
`0` là UID của **root**!

Quyền SETGID (Set Group ID on execution hoặc thư mục)

Với tệp thực thi: chương trình sẽ chạy với **quyền nhóm của tệp**, thay vì quyền nhóm của người chạy
Với thư mục: **mọi tệp/tệp con** được tạo bên trong thư mục sẽ **tự động thừa kế group của thư mục**, không phải group của người tạo ra
Bước 1:Tạo nhóm và thư mục dùng chung
sudo groupadd sharedgroup
sudo mkdir /home/shared
sudo chown root:sharedgroup /home/shared
sudo chmod 2775 /home/shared
hoặc sudo chmod g+ws /home/shared

`giải thích`

`2` đầu tiên trong `2775` là bit SETGID

`775`: owner và group có rwx

drwxrwsr-x 2 root sharedgroup 4096 Jul 22 14:00 /home/shared

Bước 2: Thêm user vào nhóm
sudo usermod -aG sharedgroup alice
sudo usermod -aG sharedgroup bob
Bước 3: Khi `alice` tạo file
cd /home/shared
touch test.txt
ls -l
→ File sẽ có group là `sharedgroup` dù group chính của alice là khác.

Thiết lập quyền mặc định umask

Sử dụng lệnh umask XYZ
Yêu cầu: Hãy thiết đặt để các tập tin/thư mục mới tạo ra có quyền sau: rwx r-x r-x
$umask 000 010 010
hoặc $umask 022
umask 0022 # Cũng OK
giải thích:mặc định là 777 trừ 022 , 777-002= 775 → rwx r-x r-x
Chữ số đầu tiên là cho special bits:

- 4 = setuid
- 2 = setgid
- 1 = sticky bit
- 0 = không có special bits

! thư mục mới tạo thì 755 được nhưng tệp thì chỉ có thể 644 thôi
đánh thêm *chmod +x myfile*
yêu cầu Nếu bạn muốn **thư mục mới có quyền mặc định là `750` (rwx r-x ---)** thì bạn nên thiết lập:
`umask 027`

An toàn cho hồ sơ người dùng

Kiểm tra quyền trên thư mục cá nhân
 ls -ld /home/user-name
Không cho người khác đọc thư mục cá nhân
 sudo chmod 0750 /home/username
Sửa đổi/etc/adduser.conf
 DIR_MODE=0750

Thay đổi chủ sở hữu và nhóm

Thay đổi chủ sở hữu
 chown new-owner file-name
chown new-owner [-R] dir-name

– Tùy chọn -R để thay đổi một cách đệ qui trên thư mục
Thay đổi nhóm chủ sở hữu
chgrp new-group file-name
chgrp new-group [-R] dir-name
– Tùy chọn -R để thay đổi một cách đệ qui trên thư mục

APACHE

- install apache :
  sudo apt update
  sudo apt install apache2 php

Lưu ý: Thư mục cấu hình /etc/apache2:
❑ apache2.conf: tập tin cấu hình chính, tập tin chịu trách nhiệm tải các tập tin khác.
❑ ports.conf: chỉ định các cổng TCP mà Apache2 lắng nghe
❑ conf.d: Thư mục chứa các files cấu hình tổng thể
❑ envvars: Chứa các biến môi trường cho Apache2
❑ httpd.conf: Tập tin cấu hình cũ, dùng thiết đặc các cấu hình đặc biệt cho một số người dùng

cách 1:
bước 1: sudo nano /etc/apache2/sites-available/000-default.conf
chỉnh thư mục lại:
DocumentRoot /var/www/myweb
bước 2: cập nhật thư mục chứa web site website
sudo mkdir /var/www/**myweb**
Bước 3: cập nhật quyền sở hữu thư mục
sudo chown -R $USER:$USER /var/www/**myweb**
Bước 4: cập nhật quyền truy cập thư mục
sudo chmod -R 755 /var/www/**myweb**
bước 5: truy cập bằng quyền **người sở hữu tạo trang web**
sudo nano /var/www/**myweb**/index.html

```
<html>
<head>
<title>Welcome to QTM</title>
</head>
<body>
<h1>My name is: …….</h1>
</body>
</html>
```

hoặc tạo file list.php

```
<?php
echo “B2204973”;
?>
```

restart lại:

sudo systemctl reload apache2

cách 2: **Virtual Host cho Website**
sudo mkdir /var/www/your_domain
sudo chown -R $USER:$USER /var/www/your_domain
sudo nano /etc/apache2/sites-available/your_domain.conf
tại: /etc/apache2/sites-available/your_domain.conf

```
<VirtualHost *:80>
    ServerName your_domain
    ServerAlias www.your_domain
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/your_domain
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Thực hiện từng bước sau:
sudo a2ensite your_domain
sudo a2dissite 000-default
sudo apache2ctl configtest
sudo systemctl reload apache2
sudo nano /etc/apache2/mods-enabled/dir.conf
tại /etc/apache2/mods-enabled/dir.conf thê,

```
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm
</IfModule>
```

sudo systemctl reload apache2
Truy cập thử
http://server_domain_or_IP

Lưu ý Quản trị dịch vụ apache2
sudo systemctl status apache2
sudo systemctl stop apache2
sudo systemctl start apache2
sudo systemctl restart apache2

SQL

Bước 1: Install SQL
sudo apt update
sudo apt install mysql-server
Bước 2: cài đặt cấu hình bảo mật
sudo mysql_secure_installation
sudo mysql

```
CREATE DATABASE lbt_database;
CREATE USER 'lbt_b2204973'@'%' IDENTIFIED BY 'password';
GRANT ALL ON lbt_database.* TO 'lbt_b2204973'@'%';
```

mysql -u lbt_b2204973 -p

```
CREATE TABLE lbt_database.todo_list (

 item_id INT AUTO_INCREMENT,
 content VARCHAR(255),
 PRIMARY KEY(item_id)
);
INSERT INTO lbt_database.todo_list (content) VALUES ("My first important item");
SELECT * FROM lbt_database.todo_list;
```

bước 3: tạo file todo_list.php

```
$nano /var/www/myweb/todo_list.php
<?php
$user = "lbt_b2204973";
$password = "password";
$database = "lbt_database";
$table = "todo_list";

try {
  $db = new PDO("mysql:host=localhost;dbname=$database", $user, $password);
  echo "<h2>TODO</h2><ol>";
  foreach($db->query("SELECT content FROM $table") as $row) {
    echo "<li>" . $row['content'] . "</li>";
  }
  echo "</ol>";
} catch (PDOException $e) {
    print "Error!: " . $e->getMessage() . "<br/>";
    die();
}
```

SSH

Cấu hình OpenSSH Server (tuc la lam tu server)

Tập tin cấu hình /etc/ssh/sshd_config

nano /etc/ssh/sshd_config

Port new-port-number

kiem tra tuong lua

sudo ufw status

sudo ufw allow ssh

- Có người dùng muốn đến ssh đến trên máy Ubuntu Server rồi thì mới ssh từ máy client vô được nha
- kiểm tra đã tạo những key nào
  ls ~/.ssh
- Kết quả thường sẽ liệt kê các file như:
  id_rsa # private key (RSA)
  id_rsa.pub # public key

id_ed25519
id_ed25519.pub
known_hosts
config

xem dấu vân tay

$ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub

kết nối

ssh **b2204973**@172.30.118.151

có cổng ssh -p 2222 b2204973@172.30.118.151

Đổi cổng SSH từ mặc định 22 sang một cổng khác (ví dụ: 2222)

Bước 1: Mở file cấu hình SSH

sudo nano /etc/ssh/sshd_config

Bước 2: Tìm dòng cấu hình cổng

#Port 22

→ Bỏ dấu # và thay 22 bằng số cổng bạn muốn, ví dụ:

Port 2222

Bước 3: Mở firewall (nếu đang bật)

sudo ufw allow 2222/tcp

Bước 4: Khởi động lại SSH

sudo systemctl restart sshd

Bước 5: SSH vào server bằng cổng mới

`ssh user1@your_server_ip -p 2222`

hoặc ssh -p 2222 b2204973@172.30.118.151

hoặc ssh -i ~/.ssh/id_ed25519_b2204973 -p 2222 b2204973@172.30.118.151

1. **Tạo cặp public key – private key**

ssh-keygen -t dsa -C user1@172.16.18.(100+X)

hoặc **ssh-keygen -t dsa -C user1@172.16.18.151 -f ~/.ssh/id_dsa_user1**

hoặc **ssh-keygen -t ed25519 -C "user1@172.16.18.151"**

hoặc **ssh-keygen -t rsa -b 4096 -C "user1@172.16.18.151"**

Hoặc **ssh-keygen -t dsa -C rusername@remoteIP**

Đăng nhập mà không cần mật khẩu

2. **Copy public key lên remote server dùng kết nối vào tập tin /home/user1/.ssh/authorized_keys Hoặc dùng ssh-copy-id**

cách 1: đánh lệnh Từ máy trạm (client), dùng:

ssh-add

ssh-copy-id user1@172.16.18.(100+X)

vd: ssh-copy-id user1@172.30.118.151

Copy **public key SSH** của máy bạn vào **server có IP** `172.30.118.151`, để user `user1` trên server đó có thể **cho phép bạn đăng nhập mà không cần mật khẩu**. nó sẽ tự động copy vào /home/user1/.ssh/authorized_keys

nó sẽ Tự động:

- Tạo thư mục `~/.ssh` trên server nếu chưa có.
- Tạo (hoặc thêm vào) file `~/.ssh/authorized_keys`.

- Đảm bảo phân quyền đúng (`chmod 700 ~/.ssh`, `chmod 600 ~/.ssh/authorized_keys`).
  Nếu bạn có nhiều key, bạn có thể chỉ định key nào để copy:
  ssh-copy-id -i ~/.ssh/id_ed25519.pub user1@172.30.118.151

Nếu muốn xóa hết làm lại

1. Trên máy client:
rm -rf ~/.ssh
Xóa toàn bộ key cũ, file cấu hình, known_hosts,..
Sau đó tạo lại bằng:
ssh-keygen -t ed25519 -C "user@client"

🔹 2. Trên server (đăng nhập qua mật khẩu):
rm -rf ~/.ssh
Xóa file authorized_keys → nghĩa là **không ai đăng nhập được bằng key** nữa.
Nếu bạn đang đăng nhập bằng key, hãy mở 1 cửa sổ SSH khác (đang kết nối) để không bị "mất cửa sổ".

Nếu bạn muốn mình kiểm tra xem key đã bị xóa đúng chưa, bạn có thể chạy:
Trên client:
ls ~/.ssh
Trên server:
ls ~/.ssh
cat ~/.ssh/authorized_keys

🛑 Lưu ý quan trọng:

- Sau khi xóa .ssh ở **server**, nếu **không bật lại đăng nhập bằng mật khẩu**, bạn sẽ **bị khóa ngoài**.
  → Đảm bảo dòng PasswordAuthentication yes trong /etc/ssh/sshd_config và đã restart SSH: sudo systemctl restart ssh

hoặc cách 2
• Từ máy Ubuntu Desktop
cd ~/.ssh
scp id_dsa.pub user1@ssh-server:~/.ssh/user1_pub_key
• Trên Ubuntu server
Login vào user1
cd .ssh
touch authorized_keys
cat user1_pub_key >> authorized_keys

3. **khởi động lại nếu cần**

sudo systemctl restart ssh
Lưu ý bổ sung nếu có lỗi:

chắc chắn rằng **ssh-agent** đã bật và chứa private key
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_dsa
Copy từ xa
1. Copy file từ local → server
scp myfile.txt user@172.30.118.151:/home/user/
2. Copy **file từ server → local**:
scp user@172.30.118.151:/home/user/report.pdf ./

(Tham khảo thêm về lệnh ssh và scp như ssh –help; man ssh; scp –help; man scp)
Xoa tren server - user1 de bat buoc user 1 dang nhap phai chung thuc bang mat khau
user1@server:~$ rm -r ~/.ssh/authorized_keys
Chạy lệnh sau để xóa khóa cũ:

ssh-keygen -f "/home/student/.ssh/known_hosts" -R "172.30.118.151"

Kết nối lại SSH

ssh b2204973@172.30.118.151

Bonus: **Tắt chức năng đăng nhập bằng mật khẩu, chỉ cho phép đăng nhập bằng key.**

Bước 1: Mở file cấu hình SSH
sudo nano /etc/ssh/sshd_config
Bước 2: Tìm và chỉnh sửa các dòng sau:
a. Tắt đăng nhập bằng mật khẩu:
Tìm dòng:
#PasswordAuthentication yes
→ Bỏ dấu # và sửa thành:
PasswordAuthentication no

---

b. Bật xác thực bằng public key:
Tìm dòng:
#PubkeyAuthentication yes
→ Bỏ dấu # nếu có, đảm bảo là:
PubkeyAuthentication yes

---

c. (Khuyến nghị) Đảm bảo các dòng sau có giá trị đúng:
PermitRootLogin no
ChallengeResponseAuthentication no
UsePAM no
Giúp tăng bảo mật và tránh những cơ chế đăng nhập không mong muốn.

Bước 3: Khởi động lại dịch vụ SSH
sudo systemctl restart ssh
Bước 4: Thử kết nối bằng key
ssh -i ~/.ssh/id_ed25519 user1@server_ip -p 22

CẢNH BÁO:
Trước khi tắt PasswordAuthentication, hãy chắc chắn rằng:
Bạn đã copy key public vào server: ~/.ssh/authorized_keys
Bạn đã kiểm tra SSH key hoạt động tốt
Bạn có cửa sổ SSH thứ hai đang mở sẵn để tránh bị mất quyền truy cập nếu cấu hình sai.

Bonus: **chỉ cho phép đăng nhập bằng mật khẩu, không cho phép đăng nhập bằng SSH key**

bạn cần chỉnh file cấu hình `sshd_config` trên **server**, cụ thể như sau:

Bước 1: Mở file cấu hình SSH

sudo nano /etc/ssh/sshd_config

Bước 2: Sửa các dòng sau

a. Tắt xác thực bằng public key
#PubkeyAuthentication yes
→ Bỏ dấu # nếu có, và đổi thành: PubkeyAuthentication no
b. Bật xác thực bằng mật khẩu
#PasswordAuthentication yes
→ Bỏ dấu # nếu có, đảm bảo dòng này như sau: PasswordAuthentication yes
c. (Tuỳ chọn) Đảm bảo các dòng sau đúng:
ChallengeResponseAuthentication no
UsePAM yes
UsePAM nên là yes nếu bạn dùng mật khẩu hệ thống bình thường.
Bước 3: Khởi động lại dịch vụ SSH
sudo systemctl restart ssh
Bước 4: Kiểm tra
Từ máy client, thử SSH vào server:
ssh b2204973@172.30.118.151

FTP

Không cho người dùng vô danh vào ftp

Bước 1: vào fileconfig
sudo nano /etc/vsftpd.conf
Bước 2: Sữa
anonymous_enable=NO
anon_upload_enable=NO #khong cho phep nguoi dung vo danh co the upload file

Cài đặt FTP cho user - Đăng nhập có chứng thực

Bước 1: Cài đặt vsftpd
sudo apt update
sudo apt install vsftpd -y
Bước 2: Tạo user FTP
sudo adduser ftpuser

/ *Bước 3: Tạo thư mục FTP riêng cho user*

sudo mkdir -p /home/ftpuser/ftp

sudo chown nobody:nogroup /home/ftpuser/ftp

sudo chmod a-w /home/ftpuser/ftp

 # Thư mục để upload

sudo mkdir -p /home/ftpuser/ftp/files

sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files

không cần bước này nếu không có yêu cầu đặt biệt

**/*

Bước 4: Cấu hình vsftpd
sudo nano /etc/vsftpd.conf
Tìm và chỉnh các dòng sau (nếu chưa có thì thêm):
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
allow_writeable_chroot=YES

✅ Giải thích:

- anonymous_enable=NO: không cho user ẩn danh truy cập.
- local_enable=YES: cho phép user hệ thống đăng nhập.
- **write_enable=YES: cho phép ghi file. Cấu hình cho người dùng được phép thao tác trên ftp #Cho phép thao tác ghi (upload, xóa, đổi tên...)**
- chroot_local_user=YES: khóa user vào thư mục home.
- allow_writeable_chroot=YES: cho phép upload trong chroot.

Bước 5: Khởi động lại FTP service
sudo systemctl restart vsftpd

Bước 6: Kiểm tra tường lửa (nếu có)
Cho phép FTP:

sudo ufw allow 20/tcp

sudo ufw allow 21/tcp

Bước 7: Kết nối FTP từ client
Từ máy Ubuntu Desktop, đăng nhập vào ftp
server với tài khoản user1
ftp 172.30.118.151 # ftp-server là IP hoặc Hostname
User: user1
Password: user1
Từ Ubuntu Desktop
Tạo tập tin my-doc.txt trong thư mục hiện hành
Đăng nhập vào ftp server bằng tài khoản user1
• Thực hiện các lệnh sau:
Xem thư mục hiện hành
Chuyển lên thư mục gốc
Thử download một tập tin nào đó
Chuyển về thư mục /home/user1

Thử upload tập tin my-doc.tx

Cấu hình để người dùng vô danh có thể thực hiện thao tác

anonymous user không có quyền ghi vào thư mục hiện tại (mặc định thường là /srv/ftp/ hoặc /var/ftp/), hoặc chưa có thư mục cho phép ghi.
Bước 1: vào /etc/vsftpd.conf

sudo nano /etc/vsftpd.conf

Bước 2: sửa file config
Thêm hoặc đảm bảo các dòng sau có giá trị:

```
anonymous_enable=YES          # Cho phép người dùng anonymous truy cập FTP
write_enable=YES              # Cho phép ghi (upload)
anon_upload_enable=YES        # Cho phép anonymous upload file
anon_root=/srv/ftp            # Thư mục gốc dành cho anonymous
anon_mkdir_write_enable=YES   # Cho phép anonymous tạo thư mục
```

Bạn cần đảm bảo thư mục /srv/ftp đã tồn tại và có quyền ghi phù hợp:

```
sudo mkdir -p /srv/ftp
sudo chown ftp:ftp /srv/ftp
sudo chmod 777 /srv/ftp
```

Bước 3: vào dịch vụ ftp thử
ftp 172.30.118.151
user: ftp
password: tuy y: a@gmail.com
Bước 4: Thực hiện một số tác vụ
Upload file
– put local-file-path remote-file-path
ví dụ put mytest.txt
Download file
get remote-file-path local-filename-path
● Ví dụ: get readme.txt
hoặc **ftp>** get readme.txt /home/student/dataftp/readme.txt

SAMBA

sudo apt install samba
Chỉnh sửa file cấu hình Samba tại:
sudo nano /etc/samba/smb.conf
Cấu hình tổng quát

•Sửa đổi tập tin smb.conf
•Phần mô tả tổng quát
[global]
workgroup = TenNhom
netbios name = TenServer
server string = Mô Tả về Server
security = user
map to guest = bad user
guest account = smbguest

Linux Server như một file server công cộng không chứng thực người sử dụng

mục tiêu là tạo 2 thư mục soft, data, cho bất cứ ai điều vào đọc được, riêng thư mục data thì được tạo thư mục mới, tập tin mới

vào:

sudo nano /etc/samba/smb.conf

cấu hình

[softs]
path = /srv/softs
guest ok = yes
read only = yes #chỉ đọc
[data]
path = /srv/data
guest ok = yes
read only = no #cho phép đọc và ghi

test

testparm

Tạo người dùng smbguest trên Linux server: Không có home directory, không shell;
sudo adduser --home /dev/null --shell /bin/false --disabled-password smbguest

•Tạo các thư mục chia sẻ công cộng

sudo mkdir -p /srv/softs
sudo mkdir -p /srv/data

Đổi chủ sở hữu và nhóm chủ sở hữu cho các thư mục công cộng

sudo chown -R smbguest:smbguest /srv/softs
sudo chown -R smbguest:smbguest /srv/data

Khởi động lại dịch vụ samba

sudo service smbd restart
sudo service nmbd restart

Chạy lệnh sau để cho phép mọi người ghi vào `/srv/data`:

sudo chmod -R 0777 /srv/data

Giải thích

`0` → không đặt bit đặc biệt (SGID/SUID/sticky)

`7` → user (chủ sở hữu) có quyền `rwx`

7 → group có quyền `rwx`

7 → others (người khác, bao gồm cả **guest Samba**) có quyền `rwx`

Kết nối

smb://172.30.118.151/srv/softs

smb://172.30.118.151/srv/data

Linux Server như một file server có chứng thực người sử dụng theo mô hình workgroup

Mục tiêu user1, user3 write ; user2 read

vào:

sudo nano /etc/samba/smb.conf

thêm vào

```
[homes]
   comment = Home directory
   Browsable = no
   read only = yes
   create mask = 0700
   directory mask = 0700
[project]
   path = /srv/project
   guest ok = no
   valid users = user1 user2 user3
   read list = user2
   write list = user1 user3
```

Mục tiêu user1, user3 write ; user2 read

Tạo user

sudo adduser user1

sudo adduser user2

sudo adduser user3

Thêm người dùng vào samba: sudo smbpasswd -a username

sudo smbpasswd -a user1

sudo smbpasswd -a user2

sudo smbpasswd -a user3

Nếu muốn xóa kết nối thì

NET user1 * / DELETE

Tạo group mới

sudo groupadd group13

Thêm từng user vào group bằng lệnh:

sudo usermod -aG group13 user1

sudo usermod -aG group13 user3

Tạo thư mục /srv/project

sudo mkdir /srv/project

Thay doi chu so huu cua thu muc /srv/project
sudo chmod -R root:group13 /srv/project
sudo chmod 755 /srv/project

Kết nối
smb://172.30.118.151/project/
bằng user1 user2 user3 để kiểm tra