

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1



BÁO CÁO BÀI TẬP LỚN

Môn: Hệ điều hành Windows và Linux/Unix

Đề tài: So sánh cài đặt và quản trị giữa Windows và Linux(Ubuntu)

Giảng viên: Đinh Trường Duy

Nhóm sinh viên: G1906807 - Lớp D19-068

1. Hoàng Ngọc Thắng-B19DCAT186
2. Nguyễn Khánh Hưng-B19DCAT095
3. Cao Xuân Phong-B19DCAT136
4. Lê Văn Đức - B19DCAT045
5. Đinh Quang Hiếu- B19DCAT065

Hà Nội – 2021

I. Dịch vụ và cài đặt DNS, DHCP trên máy Windows và Linux/Unix

1. Giới thiệu chung về DNS:

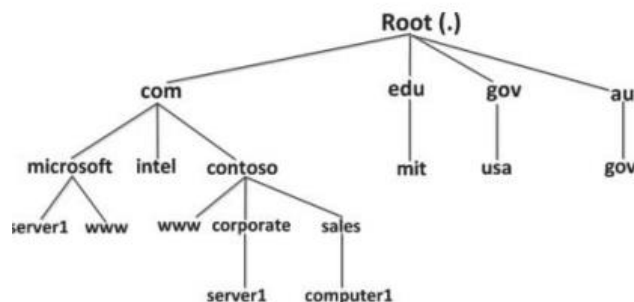
Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập địa chỉ IP của trang web. Quá trình "dịch" tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một DNS server. Các DNS trợ giúp qua lại với nhau để dịch địa chỉ "IP" thành "tên" và ngược lại. Người sử dụng chỉ cần nhớ "tên", không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ)

•DNS là hệ thống quản lý cơ sở dữ liệu phân tán dựa trên mô hình phân cấp chủ/khách để chuyển đổi tên máy chủ hay tên miền thành địa chỉ mạng Internet.

•Khi người dùng truy cập tài nguyên mạng, dịch vụ DNS trên máy tính sẽ xác định vị trí vật lý của máy tính chứa nội dung muốn truy cập

°Ưu điểm

- Dễ sử dụng: người dùng chỉ cần nhớ tên của máy tính hay tài nguyên mạng thay vì các con số của địa chỉ mạng
- Khả năng mở rộng phân rã tên/ địa chỉ mạng tên nhiều máy chủ và CSDL
- Tính nhất quán: địa chỉ mạng có thể thay đổi trong khi tên các máy vẫn giữ nguyên, dễ dàng xác định tài khoản hơn



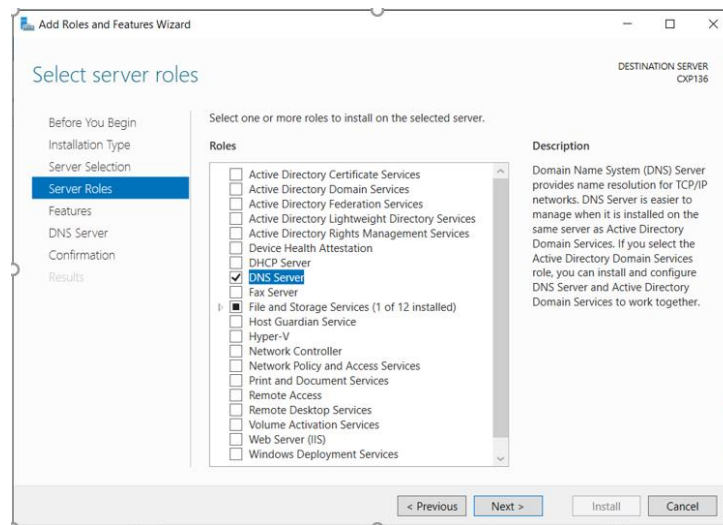
DNS chính là hệ thống phân cấp của cây tên các miền như trong hình trên. Ở gốc của cây chính là vùng gốc. Sau đó, được chia thành các vùng con, mỗi vùng có một máy chủ DNS tương ứng. Trách nhiệm quản trị tại bất kỳ vùng nào được ủy nhiệm hay phân chia qua việc tạo các miền con mà tên miền này được gán cho một máy chủ khác và một đối tượng quản trị khác.

Mỗi một nút hay là trong cây chính là bản ghi tài nguyên (resource record) lưu thông tin thuộc về tên miền. Bản ghi tài nguyên phổ biến nhất là địa chỉ máy trạm cho biết tên của máy và địa chỉ mạng tương ứng.

2.Cài đặt

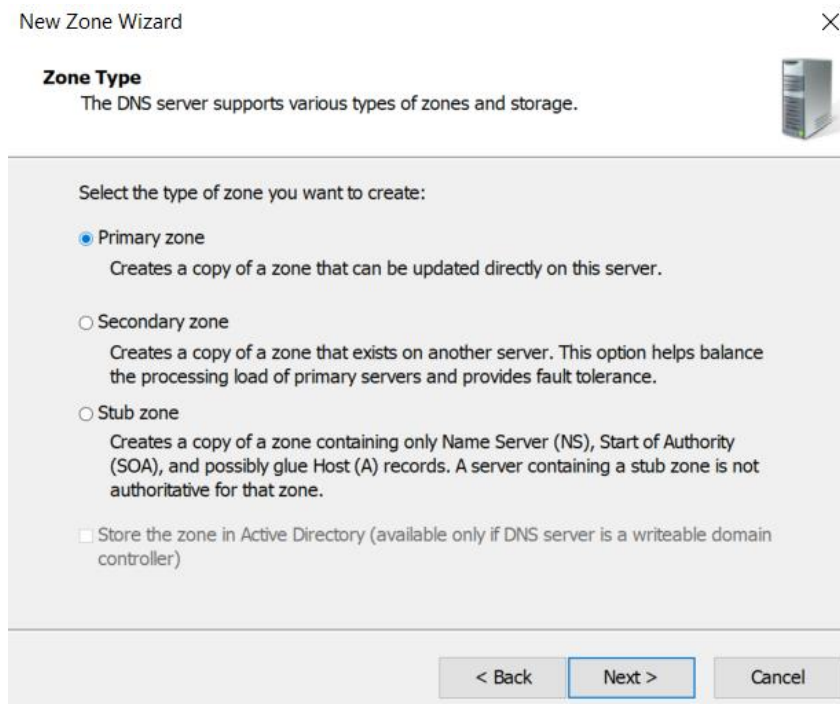
A.Ở trên hệ điều hành Windows Server

Dễ dàng cài đặt tiện ích qua Server Manager



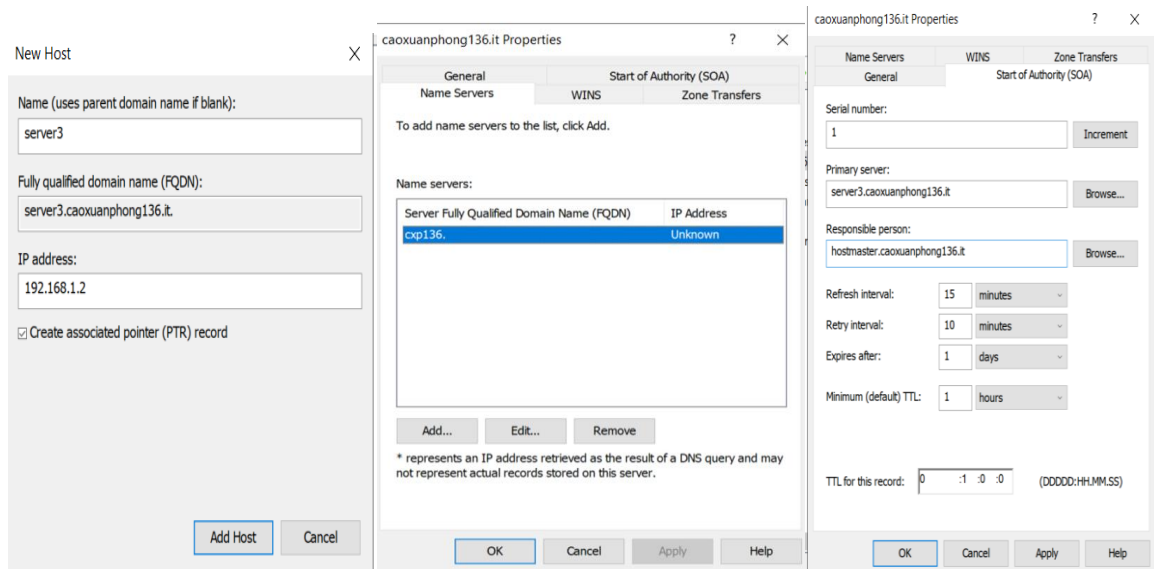
Máy chủ DNS quản lý miền chính và miền thứ cấp

Miền chính cho phép sửa đổi cập nhật các bản ghi về tên miền còn miền thứ cấp thì không



Một số điểm lưu ý

- Số các mạng vật lý cần dịch vụ DNS
- Số lượng máy chủ DNS
- Bảng thông WAN
- Số miền hay vùng
- Các dạng và số lượng bản ghi



- Cách kiểm tra cài đặt bằng công cụ nslookup

```

C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\phong>nslookup
Default Server: server3.caoxuanphong136.it
Address: 192.168.1.2

> set type=any
type=any
> caoxuanphong136.it
Server: server3.caoxuanphong136.it
Address: 192.168.1.2

caoxuanphong136.it    nameserver = server3.caoxuanphong136.it
caoxuanphong136.it    primary name server = server3.caoxuanphong136.it
caoxuanphong136.it    responsible mail addr = hostmaster.caoxuanphong136.it
caoxuanphong136.it    serial = 5
caoxuanphong136.it    refresh = 900 (15 mins)
caoxuanphong136.it    retry = 600 (10 mins)
caoxuanphong136.it    expire = 86400 (1 day)
caoxuanphong136.it    default TTL = 3600 (1 hour)
> server3.caoxuanphong136.it
Server: server3.caoxuanphong136.it
Address: 192.168.1.2
Internet address = 192.168.1.2
>

```

B. Cài đặt DNS trên LINUX/UNIX

- +, Cài đặt phần mềm: `sudo apt-get install bind9`
- +, File cấu hình `/etc/bind/etc/bind/named.conf.local` để cài đặt máy chủ tên miền chính cho miền "ptit.com"
- +, Tạo dữ liệu cho file `hn.ptit.com`:
- +, Bản ghi SOA
- +, Bản ghi NS: `ns IN A 192.168.200.3`

```

ptit.com.fw
/etc/bind
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      hn.ptit.com. root.ptit.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       hn.ptit.com.
hn.ptit.com. IN      A      192.168.200.3

```

*,Kiểm tra lại cài đặt dịch vụ DNS

+,ping: Kiểm tra máy trạm gắn với tên miền có hoạt động hay không ping my_server

+,named-checkzone: kiểm tra dữ liệu tên named-checkzone my_domain /etc/bind/db.my_domain

+,nslookup: kiểm tra tên Internet nslookup hn.ptit.com

```

root@ubuntu: /etc/bind
root@ubuntu:/etc/bind# nslookup
> hn.ptit.com
Server:          192.168.200.3
Address:         192.168.200.3#53

Name:   hn.ptit.com
Address: 192.168.200.3
> 192.168.200.3
Server:          192.168.200.3
Address:         192.168.200.3#53

3.200.168.192.in-addr.arpa    name = hn.ptit.com.
>

```

3.Nhận xét

Windows server	Linux(unbutu)
+bản ghi SOA là bản ghi đầu tiên trong cơ sở dữ liệu xác định các tham số chung cho vùng DNS bao gồm định danh máy chủ ủy quyền của vùng đó	+ ,Bản ghi SOA bắt đầu mô tả các mục nhập DNS của trang web như tên miền ,số sê-ri của dữ liệu, tên miền gốc, thời gian làm mới, thời gian đệm
+,Bản ghi NS :lưu định danh các máy chủ DNS trong miền	+,Bản ghi NS được sử dụng để chỉ định máy chủ định danh nào duy trì bản ghi trong vùng máy .Nếu tồn tại bất kì máy chủ định danh phụ nào mà bạn định chuyển vùng sang chúng cần được chuyển định tại đây
+Bản ghi A :thông tin căn bản ánh xạ tên của một máy chủ ra địa chỉ mạng Internet	+ bản ghi A được sử dụng để cung cấp ánh xạ từ tên máy chủ đến địa chỉ IP.Định dạng IP rất đơn giản Hostname IN A IP-address
+Bản ghi con trỏ PTR: là các bản ghi tìm kiếm ngược	+bản ghi PTR để thực hiện phân giải tên ngược ,do đó cho phép ai đó chỉ định đại chỉ IP và xác định tên máy chủ tương ứng +bản ghi CNAME cho phép tạo bí danh cho tên máy chủ. Điều này rất hữu ích khi ta muốn cung cấp dịch vụ có tính khả dụng

<p>+Bản ghi CNAME: ánh xạ máy chủ tới một tên có sẵn</p> <p>+Bản ghi dịch vụ SRV: hỗ trợ việc tự động phát hiện các tài nguyên TCP/IP có trên mạng</p> <p>+Bản ghi máy chủ thư: chỉ định máy chủ nhận thư của miền.</p>	<p>cao với một cái tên dễ nhớ nhưng vẫn cung cấp tên thật cho máy chủ</p> <p>+Bản ghi SRV được sử dụng để xác định vị trí các dịch vụ đặc biệt trong 1 domain, ví dụ tên máy chủ và số cổng của các máy chủ cho các dịch vụ được chỉ định.</p> <p>+Bản ghi MX có tác dụng xác định, chuyển thư đến domain hoặc subdomain đích.</p>
---	--

4. GIỚI THIỆU CHUNG VỀ DHCP

DHCP là yếu tố cần thiết quyết định số lượng thiết bị có thể kết nối vào một mạng. Nó đảm bảo tất cả các thiết bị mạng đều sở hữu một địa chỉ IP riêng biệt, không trùng nhau.

DHCP là một thuận lợi rất lớn đối với người điều hành mạng. Nó làm yên tâm về các vấn đề cố hữu phát sinh khi phải khai báo cấu hình thủ công

Về cơ bản, thông tin cấu hình gồm có:

- Địa chỉ Internet và mạng con
- Địa chỉ Internet của máy cổng
- Địa chỉ Internet của máy chủ tên miền

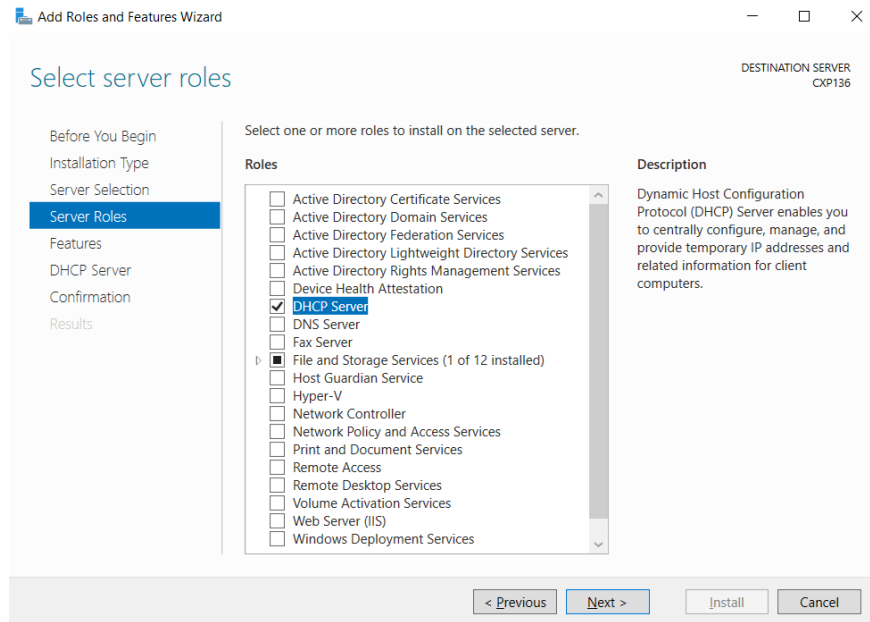
Các chế độ hoạt động DHCP:

- Cấp phát tĩnh (thủ công): Gán thông tin cấu hình mạng không đổi cho máy trạm căn cứ vào địa chỉ vật lý của kết nối mạng mỗi khi có yêu cầu từ máy trạm
- Cấp phát động: Gán thông tin cấu hình mạng từ dải địa chỉ định trước trong một khoảng thời gian nhất định còn gọi là thời gian mượn địa chỉ.
- Cấp phát tự động: Tự động gán cấu hình mạng cố định từ dải địa chỉ định trước cho thiết bị yêu cầu. So với phương pháp cấp phát động, thông tin cấu hình mạng không bị hết hạn.

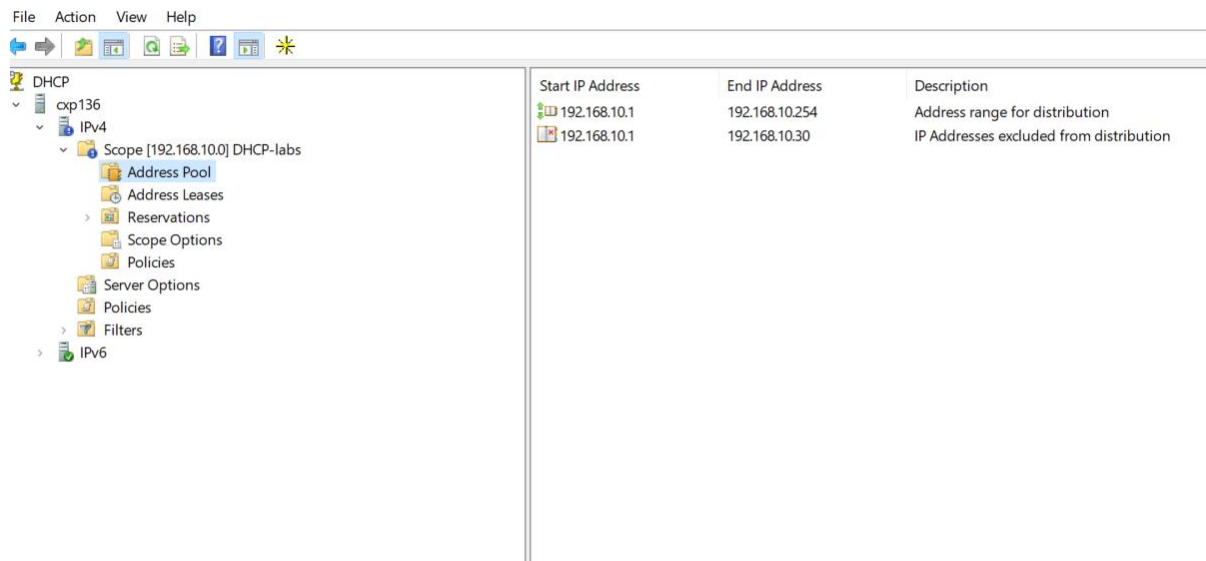
5. CÀI ĐẶT

A HỆ ĐIỀU HÀNH WINDOWS SERVER

Máy chủ cài đặt dễ dàng quan tiện ích “Server Manager”



Mục address pool là nơi chứa các range ip mà ta đã cài đặt



Lệnh kiểm tra cài đặt

+ Ping

+ Nslookup

+ Ipconfig

```
C:\Windows\system32\cmd.exe
Default Gateway . . . . . :
Tunnel adapter isatap.{2AD200E4-9409-49BE-9951-457C99E8B4E9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\phong>ipconfig /renew
Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2c04:e61f:5612:9bac%11
IPv4 Address. . . . . : 192.168.10.31
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.20
Tunnel adapter isatap.{2AD200E4-9409-49BE-9951-457C99E8B4E9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\phong>
```

B HỆ ĐIỀU HÀNH UNBUTU

CÀI ĐẶT

Gõ lệnh: `sudo apt-get install isc-dhcp-server`

```
b19at136-phong@ubuntu:~$ sudo apt-get install isc-dhcp-server
[sudo] password for b19at136-phong:
```

Máy chủ DHCP được lưu tại `/etc/default/isc-dhcp-server` file mô tả `/etc/dhcp/dhcpd.conf`

```
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-10-21 19:47:45 PDT; 8s ago
     Docs: man:dhcpd(8)
    Main PID: 2489 (dhcpd)
      Tasks: 4 (limit: 4612)
     Memory: 4.3M
    CGroup: /system.slice/isc-dhcp-server.service
            └─2489 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

Oct 21 19:47:45 ubuntu dhcpd[2489]: Database file: /var/lib/dhcp/dhcpd.leases
Oct 21 19:47:45 ubuntu dhcpd[2489]: PID file: /run/dhcp-server/dhcpd.pid
Oct 21 19:47:45 ubuntu dhcpd[2489]: Wrote 0 leases to leases file.
Oct 21 19:47:45 ubuntu dhcpd[2489]: Listening on LPF/ens33/00:0c:29:56:f4:56/192.168.17.0/24
Oct 21 19:47:45 ubuntu sh[2489]: Listening on LPF/ens33/00:0c:29:56:f4:56/192.168.17.0/24
Oct 21 19:47:45 ubuntu sh[2489]: Sending on LPF/ens33/00:0c:29:56:f4:56/192.168.17.0/24
Oct 21 19:47:45 ubuntu sh[2489]: Sending on Socket/fallback/fallback-net
Oct 21 19:47:45 ubuntu dhcpd[2489]: Sending on LPF/ens33/00:0c:29:56:f4:56/192.168.17.0/24
Oct 21 19:47:45 ubuntu dhcpd[2489]: Sending on Socket/fallback/fallback-net
Oct 21 19:47:45 ubuntu dhcpd[2489]: Server starting service.
```

Người quản trị kiểm tra các yêu cầu cấp phát được bằng cách kiểm tra nội dung file nhật ký `/var/lib/dhcpd.leases` hay trạng thái của dịch vụ `service isc-dhcp-server status`

6.NHẬN XÉT

Như vậy thì DHCP là yếu tố cần thiết quyết định số lượng thiết bị có thể kết nối vào một mạng. Nó đảm bảo tất cả các thiết bị mạng đều sở hữu một địa chỉ IP riêng biệt, không trùng nhau.

Cấu hình cho dịch vụ DHCP(windows server) khá thuận tiện nhờ giao diện đồ họa của phần quản trị DHCP. Với việc cấp phát động, người quản trị cần xác định dải địa chỉ cần cấp phát, dải địa chỉ dành riêng/dự phòng, và khoảng thời gian “sống” của địa chỉ được cấp phát.

Kiểm tra thì nhìn vào unbutu chúng ta sẽ dễ dàng kiểm tra hơn so với bên windows

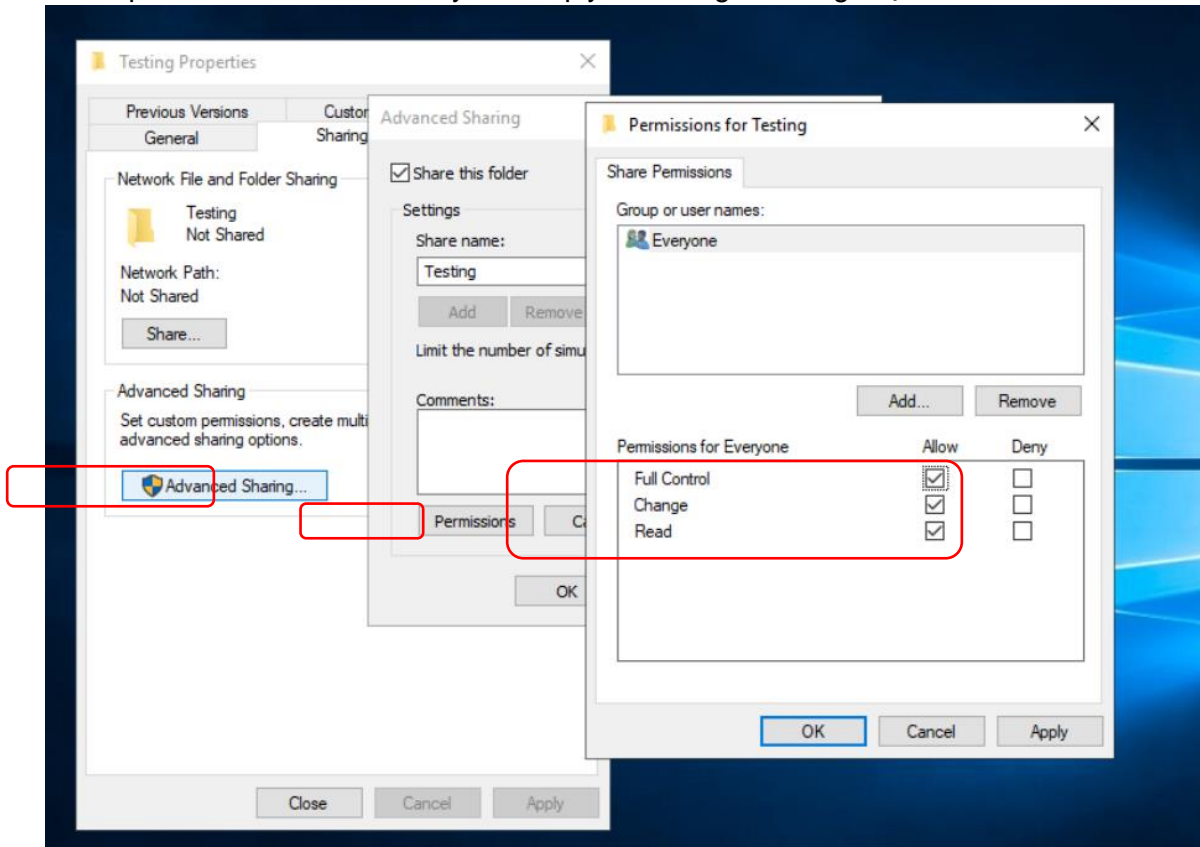
II. Chia sẻ file và máy in

1. Giới thiệu chung

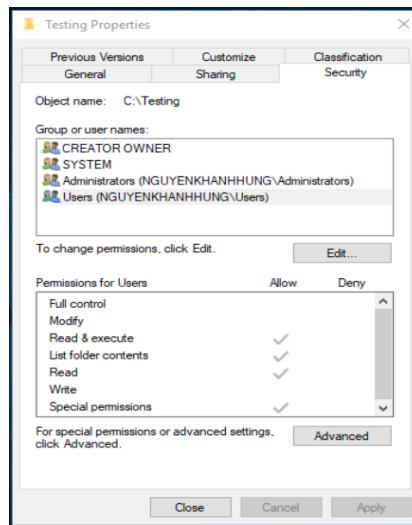
- Dịch vụ file cho phép người dùng lưu trữ và chia sẻ các dữ liệu, chương trình với người dùng khác trong mạng. Việc truy nhập thành công các file chia sẻ phải căn cứ vào quyền truy nhập mà người dùng có được.
- Dịch vụ in là Một trong những dịch vụ quan trọng trong mạng là in ấn. Các máy in mạng được kết nối trực tiếp với mạng hay thông qua máy tính cho phép người dùng trong mạng có thể sử dụng các dịch vụ của máy in. Các máy chủ in ấn là máy tính kết nối với máy in và làm nhiệm vụ xử lý các yêu cầu in ấn từ các người dùng trong mạng.

2. Windows

- Dịch vụ file:
Trong windows có thể áp dụng 2 hình thức để đảm bảo an ninh:
 - Share permission: hình thức này chỉ ra quyền của người dùng: Đọc/Ghi/Sở hữu với thư mục.



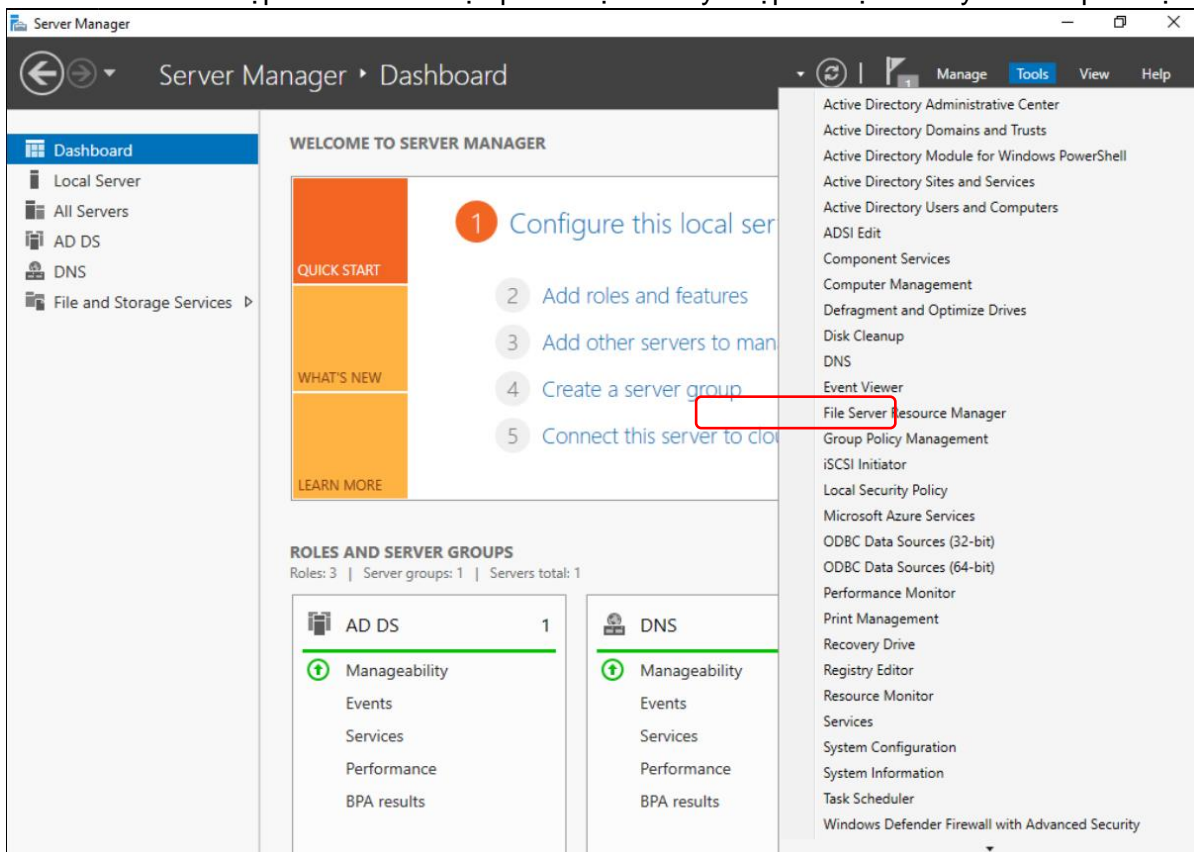
- Sử dụng cách thức phân quyền NTFS để kiểm soát việc truy nhập.



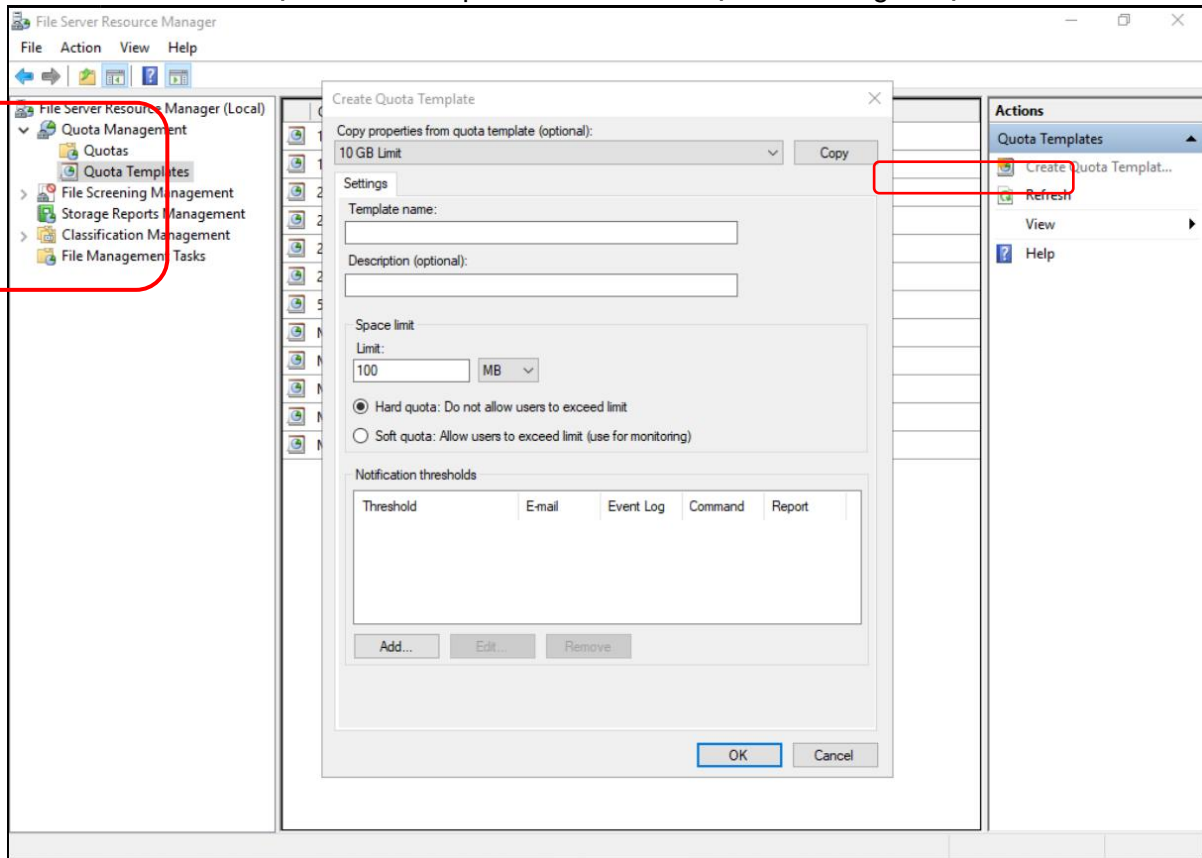
Chia sẻ file có thể được thực hiện trực tiếp từ trình duyệt file của windows. Hình thức chia sẻ lúc này là chia sẻ thư mục đòi hỏi người dùng phải có tài khoản và quyền phù hợp.

Sử dụng tiện ích File Server Resource Manager để kiểm soát và quản lý tài nguyên máy chủ file với các chức năng tiêu biểu:

- Các chức năng quản lý file: cho phép người quản trị đặt các chính sách lên file.
- Quản lý giới hạn lưu trữ: đặt các hạn chế về không gian lưu trữ của người dùng.
- Hạ tầng phân loại file: áp dụng các chính sách lên các loại file để quản lý hiệu quả hơn.
- Quản lý việc soi nội dung: cho phép soi nội dung file và hạn chế các dạng file được lưu trữ trên máy chủ.
- Báo cáo lưu trữ: lập báo cáo về việc phân loại và truy nhập dữ liệu theo yêu cầu quản trị



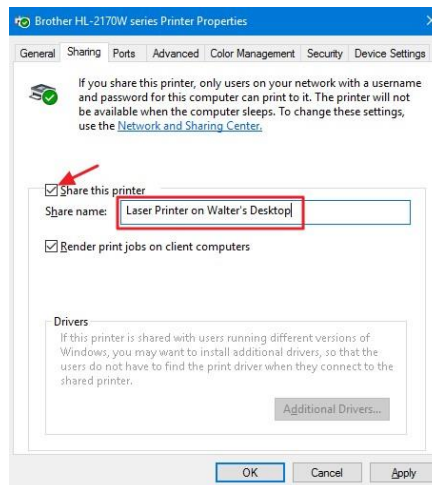
Chọn Quota Templates -> Creat để tạo các mẫu giới hạn



Để đặt các hạn chế khác cho thư mục cũng tương tự như trên tùy theo nhu cầu sử dụng.

o Dịch vụ in

Để máy tính kết nối được với máy in cần có trình điều khiển thích hợp và để chia sẻ máy in vật lý cần cài đặt máy in phù hợp. Việc chia sẻ máy in có thể được thực hiện dễ dàng thông qua giao diện của Windows sau khi cài đặt thành công trình điều khiển.



Các truy nhập của người dùng tới máy in chia sẻ chịu kiểm soát với các quyền sau:

- **Quyền in (Print):** được phép gửi tài liệu tới máy in để in ra.
- **Quyền quản lý máy in (Manage this printer):** Cho phép người dùng thay đổi cài đặt và cấu hình cho máy in.
- **Quyền quản lý tài liệu in (Manage document):** Hủy, dừng in và khởi động lại máy in.

3.Linux(Ubuntu)

o Dịch vụ file:

Linux sử dụng vsftpd một loại máy chủ FTP với các tính năng chính là bảo mật, hiệu suất và ổn định. FTP server hỗ trợ hai chế độ hoạt động:

- Anonymous: người dùng không cần mật khẩu
- Authenticated: phải có tài khoản và mật khẩu để truy nhập

Cách cài đặt trên ubuntu:

```
ubuntu@ubuntu:~$ sudo apt-get install vsftpd
```

Với các cấu hình cơ bản bao gồm:

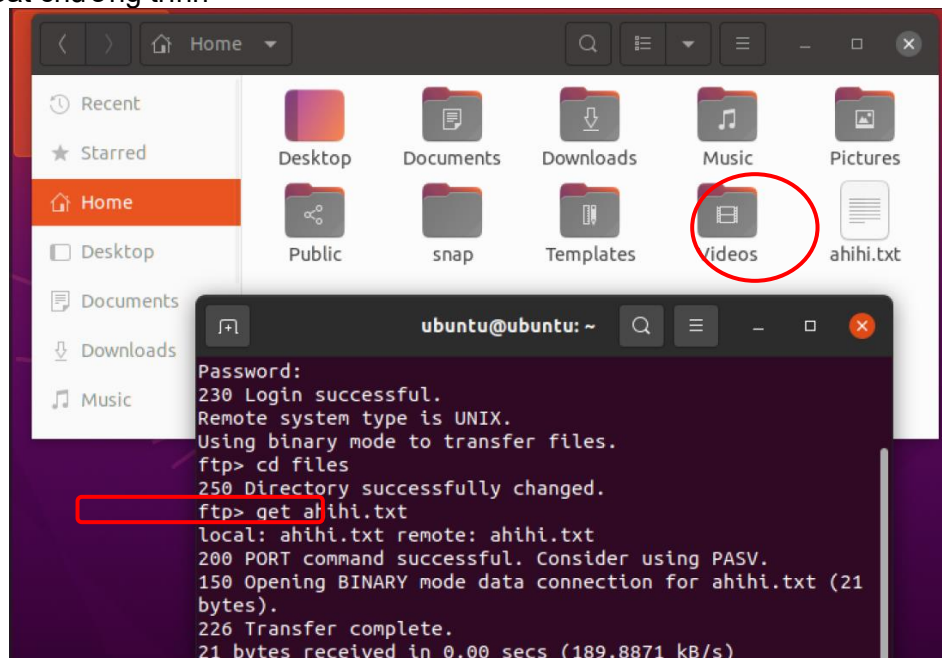
- Cho phép người dùng truy nhập ẩn danh: *anonymous_enable=YES*
- Cho phép người dùng tải file lên máy chủ: *write_enable=YES*
- Cho phép người dùng ẩn danh tải file lên: *anon_upload_enable=YES*

Kết nối đến máy chủ dịch vụ 192.168.78.137

```
ubuntu@ubuntu:~$ ftp 192.168.78.137
Connected to 192.168.78.137.
220 (vsFTPd 3.0.3)
Name (192.168.78.137:ubuntu): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Ở chế độ người dùng sử dụng các câu lệnh:

- **get, mget:** tải file về
- **put, mput:** để upload file
- **open, close:** mở đóng kết nối
- **bye:** thoát chương trình



Ngoài ra linux còn sử dụng dịch vụ NFS, một dịch vụ chia sẻ file trong môi trường Linux/Unix. Dịch vụ cho phép người dùng sử dụng file/thư mục trên máy tính mạng như ổ đĩa cục bộ. Hoạt động theo mô hình chủ khách:

- Máy chủ chia sẻ thư mục /shared
- Máy khác truy nhập vào thư mục chia sẻ qua lệnh mount

Sử dụng câu lệnh sau để cài đặt:

```
ubuntu@ubuntu:~$ sudo apt-get install nfs-kernel-server
```

Cấu hình thư mục/file chia sẻ được thực hiện thông qua việc thay đổi các dòng trong file /etc/export.

Các quyền truy nhập gồm có:

- ro: chỉ đọc
- rw: đọc và ghi
- noaccess: không cho truy nhập
- root_squash: từ chối đặc quyền root của người dùng từ xa
- no_root_squash: cho phép đặc quyền

o Dịch vụ in

Sử dụng CUPS(Common UNIX Printing System) để cung cấp và quản lý dịch vụ in.

Dịch vụ CUPS hỗ trợ việc tự động phát hiện các máy in mạng và cung cấp các công cụ quản trị và đặt cấu hình đơn giản qua Web.

Cài đặt qua câu lệnh:

```
ubuntu@ubuntu:~$ sudo apt-get install cups
```

Với các cấu hình cơ bản gồm:

- Địa chỉ quản trị
- Cổng hoạt động
- Cho phép sử dụng dịch vụ
- Từ chối dịch vụ

Phía máy khách sử dụng câu lệnh lpr để in các file tài liệu cần thiết theo dạng : lpr file_cần_in.

Trong quá trình hoạt động, CUPS ghi nhật ký hoạt động vào thư mục /var/log/cups.

III. Quản lý người dùng và máy tính

1.Hệ điều hành ubuntu(linux):

Ubuntu là hệ điều hành đa người dùng, nghĩa là nhiều người có thể truy cập và sử dụng một máy tính cài Ubuntu. Có 3 đối tượng người đó là: user, group và other. Mỗi người muốn sử dụng được máy tính cài Ubuntu thì phải có một tài khoản (account) đã được đăng ký. Một tài khoản gồm có một tài khoản người dùng (username) và một mật khẩu (password). Để có thể bắt đầu thao tác và sử dụng, người dùng phải thực hiện thao tác đăng nhập (login và hệ thống). Mỗi người trên Ubuntu được cấp một thư mục riêng (gọi là homedirectory), thực chất là một thư mục con của /home. Có dạng home/username nghĩa là nếu username bạn là mrbinh thì home directory của bạn là /home/mrbinh. Riêng đối với account root thì home directory là /root.

Quản trị users :

Trên Linux có 2 loại user :

- User hệ thống
- User người dùng

User hệ thống : dùng để thực thi các module , script cần thiết phục vụ cho hệ điều hành .

User người dùng : là những tài khoản để login sử dụng hệ điều hành .

Trong các tài khoản người dùng thì tài khoản user root (super user) là tài khoản quan trọng nhất :

Tài khoản này được tự động tạo ra khi cài đặt Linux .

Tài khoản này không thể đổi tên hoặc xóa bỏ.

User root còn gọi là super user vì nó có toàn quyền trên hệ thống .

Mỗi user thường có đặc điểm như sau :

- Tên tài khoản user là duy nhất , có thể đặt tên *chữ thường* , *chữ hoa* .
- Mỗi user có 1 mã định danh duy nhất (uid) .
- Mỗi user có thể thuộc về nhiều group .
- Tài khoản super user có uid=gid=0 .

Quản trị group:

Group là tập hợp của nhiều user .

Mỗi group có 1 tên duy nhất và 1 mã định danh duy nhất (gid) .

Khi tạo ra 1 user (không dùng option -g) thì mặc định 1 group mang tên user được tạo ra.

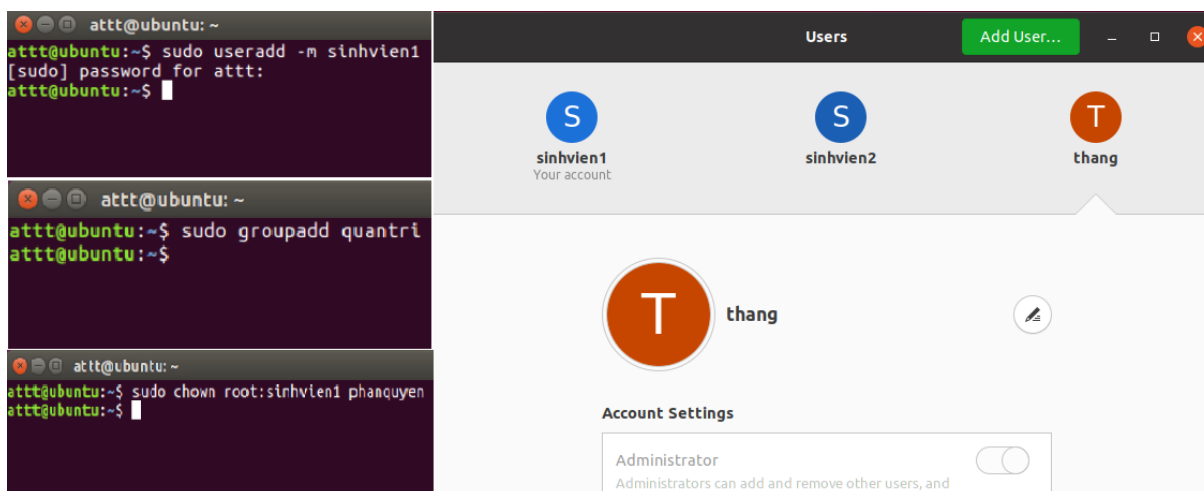
Một số thao tác với user:

- Thêm 1 tài khoản người dùng
- Đổi mật khẩu người dùng
- Sửa thông tin tài khoản
- Xóa tài khoản người dùng
- Thiết lập chính sách cho user

Thao tác quản trị group:

- Tạo thông tin cho group
- Sửa thông tin, đặt mật khẩu cho group
- Xóa group

Trong hệ điều hành ubuntu, ta có thể thêm, sửa, xóa các user, phân quyền truy cập, chia sẻ thư mục bằng câu lệnh trong terminal hoặc bằng giao diện đồ họa. Ta cũng có thể thêm các user vào 1 nhóm để phân quyền và quản trị.



2.Hệ điều hành Window

Máy tính sử dụng hệ điều hành Windows có thể được **một hay nhiều người sử dụng**, và Windows đã được thiết kế để vận hành như một hệ điều hành đơn và đa người dùng. **Mọi người dùng phải đăng nhập với một tài khoản, mỗi tài khoản này có desktop, menu Start, thư mục Documents, History, Favorites và những tùy biến riêng.** Tất cả những dữ liệu người dùng nằm trong thư mục Users của ổ đĩa hệ thống, trong đó mỗi tài khoản sẽ có một thư mục con được đặt tên theo tên của tài khoản này.

Quản lý user: Windows có 4 loại user là: Administrator, Standard, Child và Guest :

- **Administrators** (quản trị). Kiểu tài khoản sẽ có toàn quyền kiểm soát hệ thống. Chúng có thể cài đặt phần mềm ứng dụng, driver cho phần cứng, và có thể tạo, hiệu chỉnh người dùng hay nhóm người dùng mới. Ngoài ra, chúng có thể thiết lập lại mật khẩu, cài đặt chính sách và hiệu chỉnh Registry. Windows sẽ xác định những tác vụ yêu cầu quyền quản trị với một biểu tượng bảo mật của Windows.
- **Standard users** (người dùng chuẩn): Kiểu tài khoản này được cho phép đăng nhập vào máy tính, chạy ứng dụng, hiệu chỉnh thông tin tài khoản riêng, lưu file trong thư mục người dùng của chúng. Người dùng sẽ bị hạn chế thực hiện thay đổi trên hệ thống.
- **Child**: bạn cũng có thể tạo ra một tài khoản đặc biệt dành cho con của bạn, nơi bạn có thể hạn chế thời gian sử dụng, giới hạn các chức năng, ứng dụng, trò chơi theo ý của bạn. Các tài khoản này sẽ giúp con bạn sử dụng máy tính an toàn hơn khi truy cập Internet.
- **Guest**: Tài khoản khách là tài khoản mà chúng ta tạo ra để cho một người nào đó truy cập tạm thời vào máy tính của bạn. Tài khoản này chỉ là một tài khoản tạm thời và người sử dụng nó bị cấm không được phép thực hiện bất kỳ thay đổi thiết lập máy tính của bạn hoặc truy cập bất kỳ tập tin cá nhân nào của bạn được lưu trữ trong máy.

Your info



THANG
Local Account
Administrator

Family & other users

Your family

Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.

[Sign in with a Microsoft account](#)

Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

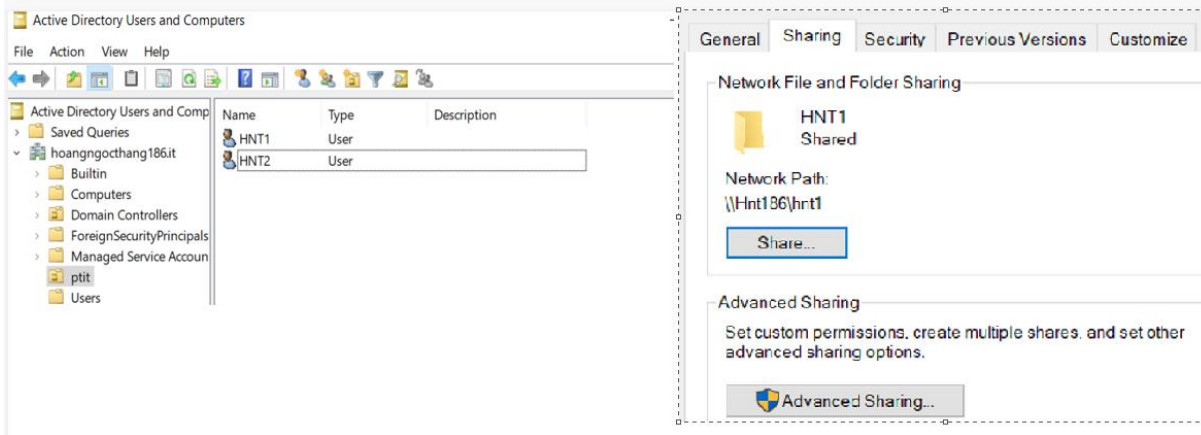
 Add someone else to this PC

Quản lý nhóm: Mọi tài khoản Windows đều là thành viên của ít nhất một nhóm. Thành viên nhóm được xác định qua giấy phép mà chúng có. Đa số người dùng sử dụng những nhóm được tạo sẵn trong Windows (được gọi là Account Types trong wizard Create User), tuy nhiên chúng ta có thể tạo nhóm khác và tùy chỉnh cho nó. Nhóm được sử dụng để giúp đơn giản hóa tác vụ quản trị máy tính bằng cách cho phép quản trị viên áp dụng đồng thời các cài đặt và giấy phép cho nhiều tài khoản.

Ngoài **Users** và **Administrators**, chúng ta sẽ thấy rất nhiều nhóm khác trong Windows. Một số được sử dụng để tương thích với các hệ điều hành trước đó, trong khi số khác được thiết kế cho những mục đích riêng, như cho phép truy cập để backup và khôi phục file, để đọc các file Log, hay để kết nối qua Remote Desktop.

Trong **Computer Management** ta có thể kiểm tra sự kiện hệ thống với Event Viewer, kiểm tra các tài nguyên chia sẻ mạng với Shared Folders, quản lý tài khoản người dùng với Local Users and Groups, xem và quản lý các trình điều khiển bằng Device Manager, quản lý ổ đĩa với Disk Management, quản lý các dịch vụ Windows với Services and Applications.

Windows có thể quản trị người dùng cục bộ trong 1 máy đồng thời có thể quản trị người dùng cùng join vào 1 domain riêng. Windows có quản trị chính sách nhóm kiểm soát môi trường làm việc với tài khoản người dùng và máy tính cấp đặc quyền cho người dùng và nhóm, cho phép quản lý và cấu hình tập trung các cài đặt người dùng giúp việc quản trị đơn giản hơn.



	Window	Linux(ubuntu)
Quản lý user	<ul style="list-style-type: none"> -Có 4 loại user => đa dạng hơn trong việc quản lý người dùng, có thể sử dụng máy tính mà không cần đăng nhập bất kì tk nào(Guest) - Thêm user qua giao diện đồ họa 	<ul style="list-style-type: none"> -Có 2 loại user --> bắt buộc phải có tk user để sử dụng máy tính. -Có thể thêm user bằng giao diện đồ họa hoặc dòng lệnh. => linh hoạt, nhanh hơn window
	Cả 2 đều là hệ điều hành đa người dùng nhưng chỉ có 1 người dùng có quyền cao nhất trong hệ thống.	Mỗi user đều được cấp cho thư mục riêng. Mỗi tài khoản phải có mật khẩu để đăng nhập.
Quản lý group	-những user muốn chia sẻ file thì phải join vào cùng 1 domain.	<ul style="list-style-type: none"> -Có thể tạo group và thêm ngay các user vào. -Có thể tạo group hoặc thêm user vào group bằng giao diện hay câu lệnh. => linh hoạt, thuận tiện hơn window
	Cả 2 hệ điều hành cho phép chia sẻ đọc ghi file trong cùng 1 group.	Có thể cấp quyền cho từng tài khoản người dùng truy cập hoặc thực thi file

IV. Truy nhập từ xa

1.Giới thiệu chung về dịch vụ truy nhập từ xa

Truy cập từ xa cho phép người dùng từ xa truy cập các tệp và tài nguyên hệ thống khác trên bất kỳ thiết bị hoặc máy chủ nào được kết nối với mạng bất cứ lúc nào, giúp tăng năng suất của nhân viên và cho phép họ cộng tác tốt hơn với các đồng nghiệp trên khắp thế giới. Các chuyên gia hỗ trợ kỹ thuật cũng sử dụng quyền truy cập từ xa để kết nối với máy tính của người dùng từ các địa điểm từ xa để giúp họ giải quyết các sự cố với hệ thống hoặc phần mềm của họ.

2.Dịch vụ truy nhập từ xa trên windows

Mạng riêng ảo VPN

VPN là viết tắt từ **Virtual Private Network**, có nghĩa là mạng riêng ảo.

Mạng riêng ảo VPN giúp người dùng tạo ra một mạng riêng từ một kết nối Internet công cộng qua đó thiết lập các kết nối được mã hóa.

Thông thường, VPN được dùng để kết nối các máy tính của các công ty hay tổ chức với nhau thông qua mạng Internet công cộng, trong trường hợp một số trang web bị hạn chế truy cập về mặt vị trí địa lý để bảo vệ hoạt động duyệt web.

➤ Nguyên lý hoạt động

Khi sử dụng mạng VPN để kết nối các thiết bị cá nhân (điện thoại, laptop, máy tính để bàn,...) với Internet, kết nối an toàn được thiết lập và cho phép bạn truy cập đến nguồn dữ liệu ở bất cứ nơi nào trên thế giới.

Cụ thể hơn, thiết bị của bạn sẽ liên kết với Internet (trang web) thông qua kết nối VPN đã được mã hóa. Qua đó, kết nối an toàn này sẽ là trung gian để trao đổi mọi thông tin, yêu cầu, dữ liệu giữa bạn và trang web truy cập.

Để sử dụng hệ thống VPN, mỗi tài khoản (đã xác thực) được cấp quyền truy cập thông qua 1 mã PIN (Personal Identification Number).

Mỗi mã PIN chỉ có hiệu lực trong một khoảng thời gian nhất định, thông thường từ **30 giây đến 1 phút** mà thôi.

❖ Các giao thức thường dùng trong VPN

➤ Point-To-Point Tunneling Protocol (PPTP)

- **Point-To-Point Tunneling Protocol (PPTP)** được sử dụng lần đầu tiên vào năm 1995. Đây được xem là giao thức lâu đời nhất hiện vẫn đang được sử dụng của VPN.
- PPTP không được dùng để chỉ định giao thức mã hóa mà được dùng để sử dụng một số giao thức như MPPE-128. Ngoài ra, PPTP chỉ có thể phát huy tối ưu công dụng của nó khi sử dụng tiêu chuẩn mã hóa mạnh nhất mà cả 2 phía cùng hỗ trợ. Nếu không, kết nối phải sử dụng mã hóa yếu hơn mong đợi của người dùng.
- Bên cạnh đó, điểm trừ của PPTP còn nằm ở vấn đề xác thực, hiện nay, kẻ tấn công có thể dễ dàng bẻ crack giao thức MS-CHAP mà PPTP sử dụng và mạo danh người dùng.

➤ Giao thức L2TP

- **Giao thức L2TP** mạnh hơn đáng kể so với PPTP và thường hoạt động với thuật toán mã hóa IPSec. Tuy nhiên, giao thức này cũng có những lỗ hổng không tránh khỏi.
- Lỗ hổng chính của giao thức L2TP là **phương thức trao đổi khóa công khai (public key)**. Dù bề khóa công khai phải có sức mạnh điện toán khá lớn nhưng sau khi đã thành công bề khóa này, người tấn công sẽ có thể truy cập vào tất cả các giao tiếp và dữ liệu trên một VPN nhất định.

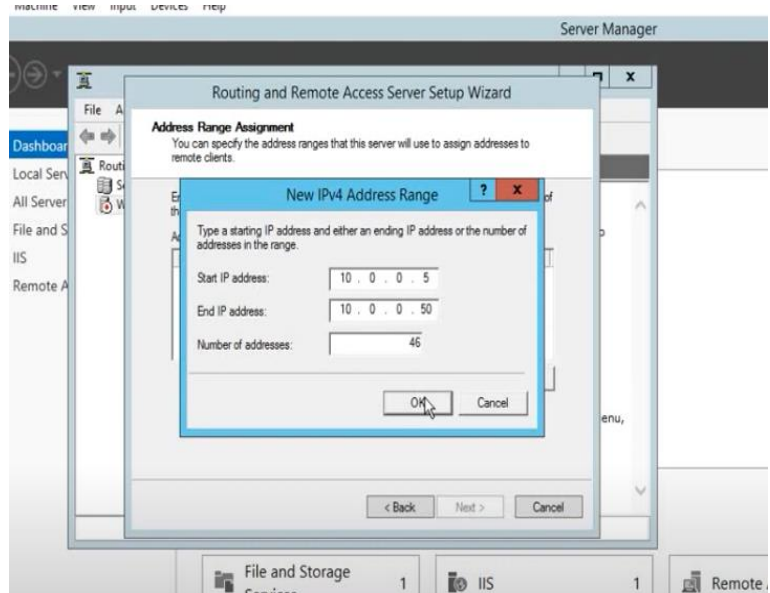
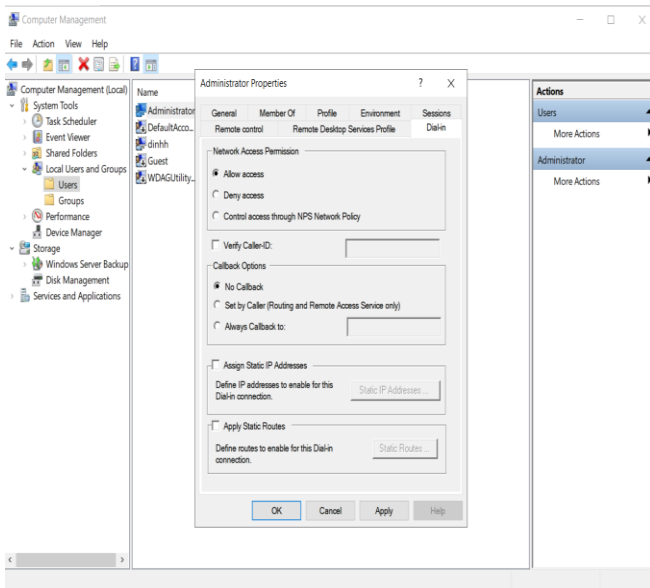
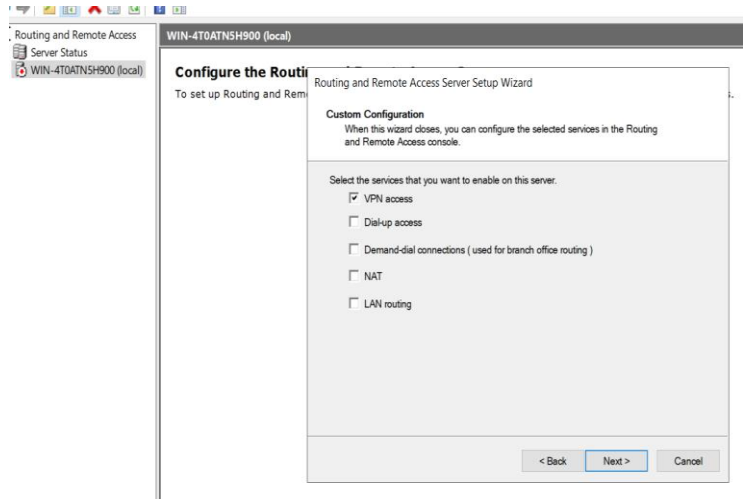
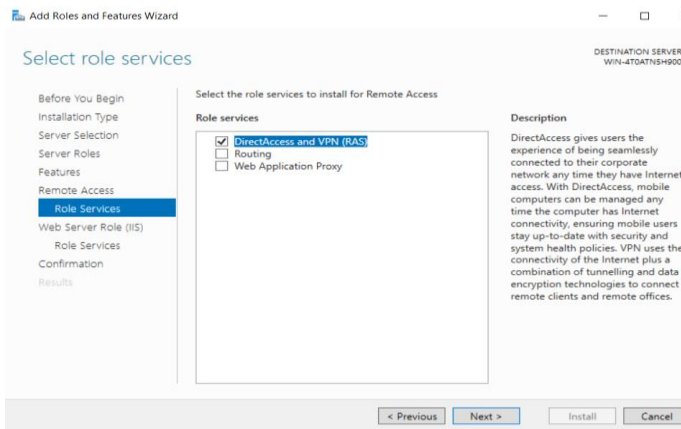
➤ SSTP (Secure Socket Tunneling Protocol)

- **SSTP (Secure Socket Tunneling Protocol)** là một giao thức tốt do Microsoft phát hành và hiện tại gần như vẫn chưa tìm được bất kỳ lỗ hổng nào.
- Đặc biệt, SSTP khi sử dụng với AES và SSL càng cung cấp tính năng bảo mật tốt hơn cả. Tuy nhiên, SSTP có một điểm yếu đó chính là hỗ trợ chủ yếu trên nền tảng Windows, còn những hệ điều hành khác thì khá hạn chế.

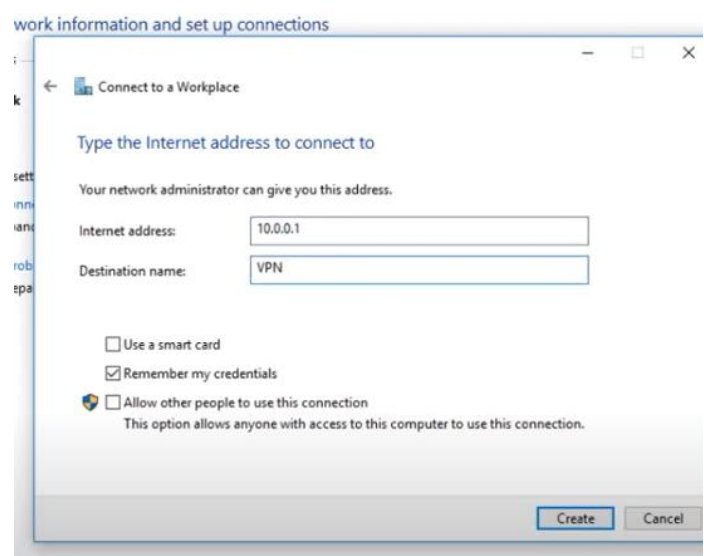
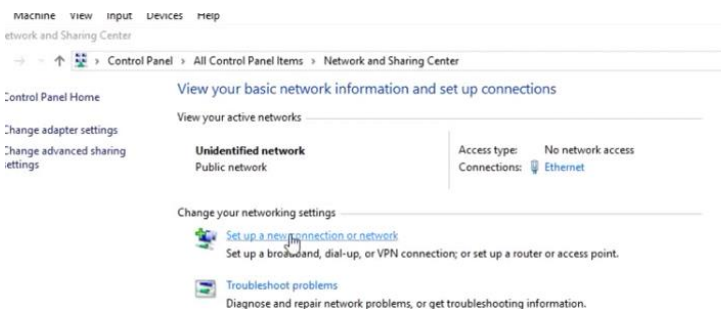
❖ Cài đặt

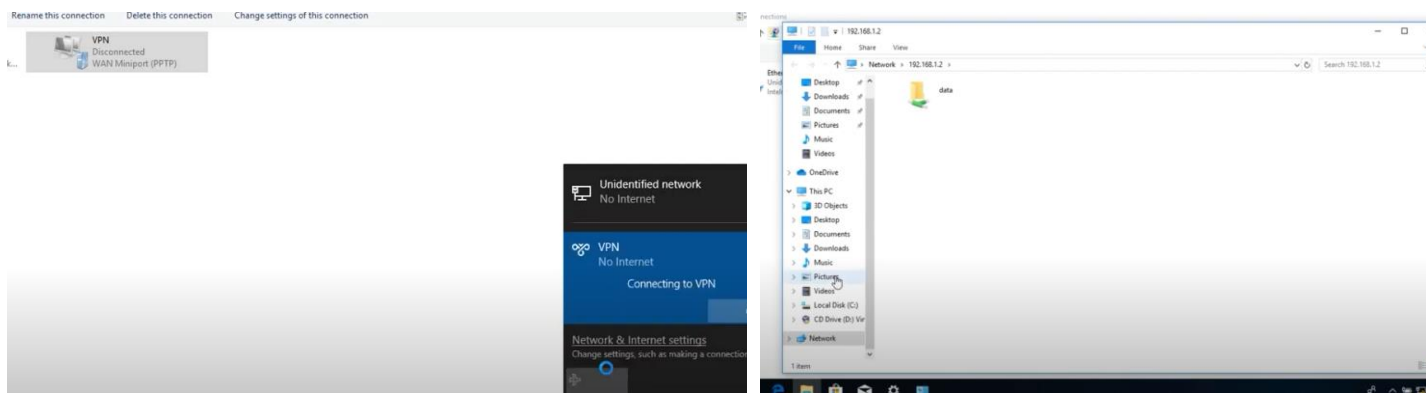
Dịch vụ VPN được cung cấp thông qua dịch vụ truy nhập từ xa và định tuyến RRAS (Routing and Remote Access Services). Cũng giống như các dịch vụ máy chủ khác, dịch vụ RRAS được cài đặt thông qua “Server Manager”. Người quản trị có thể chọn chức năng VPN từ giao diện cài đặt RRAS như trong hình dưới.

Bước tiếp theo, người quản trị cần đặt cấu hình cho máy chủ RRAS phù hợp. Các tham số cấu hình cho mạng Internet được truy nhập thông qua tiện ích quản trị RRAS.



Người dùng thiết lập và đăng nhập kết nối VPN





3. Dịch vụ truy nhập từ xa trên Linux

➤ Telnet

Telnet là một giao thức mạng (network protocol), nó cũng là công cụ quản trị server từ xa thông qua command line. **TELNET** (viết tắt của **TERminal NETwork**) được dùng phổ biến trong mạng máy tính cục bộ (LAN), Telnet sử dụng port 23.

➤ SSH

SSH, hoặc được gọi là Secure Shell, là một giao thức điều khiển từ xa cho phép người dùng kiểm soát và chỉnh sửa server từ xa qua Internet. Dịch vụ được tạo ra nhằm thay thế cho trình Telnet vốn không có mã hóa và sử dụng kỹ thuật cryptographic để đảm bảo tất cả giao tiếp gửi tới và gửi từ server từ xa diễn ra trong tình trạng mã hóa. Nó cung cấp thuật toán để chứng thực người dùng từ xa, chuyển input từ client tới host, và relay kết quả trả về tới khách hàng.

Secure Shell là một giao thức được tối ưu hóa để truy cập máy chủ Linux, nhưng có thể sử dụng được trên bất kỳ máy chủ của hệ điều hành nào. SSH chỉ có giao diện dòng lệnh, thường được điều khiển thông qua bash. Do đó, SSH đòi hỏi kỹ thuật cao hơn đối với người dùng cuối và thậm chí còn đòi hỏi kỹ thuật cao hơn khi thiết lập.

Cài đặt trong Ubuntu

- Cài đặt trên máy chủ: `sudo apt-get install openssh-server`.
- Cài đặt trên máy khách: `sudo apt-get install openssh-client`.
- Khởi động lại SSH sever khi thay đổi cấu hình:
`Sudo restart ssh / sudo service ssh restart`
- Thông tin cấu hình đặt trong file: `/etc/ssh/sshd_config`
 - + Áp dụng xác thực mã khóa công khai: `PubkeyAuthentication yes`
 - + Hiện thông báo trong file `issue.net` khi đăng nhập: `Banner /etc/issue.net`
 - + Cho phép người dùng sử dụng SSH: `AllowUser tên_người_dùng`
 - + Cấm người dùng sử dụng SSH: `DenyUser tên_người_dùng`
- Tạo khóa công khai và bí mật để sử dụng trong dịch vụ SSH: `ssh-keygen -t rsa`
- Khóa SSH gồm khóa công khai và khóa bí mật:
 - + Khóa công khai: `~/.ssh/id_rsa.pub`
 - + Khóa bí mật: `~/.ssh/id_rsa`.
- Chép khóa công khai vào máy chủ: `ssh-copy-id user@remotehost`
 - + Nếu quyền truy nhập vào file chứa khóa xác thực chưa phù hợp thì phải cập nhật lại theo câu lệnh: `chmod 600 .ssh/authorize_d_keys`

```
dinhquanghieu@dinhquanghieu:~$ sudo apt-get install openssh-server
Reading package lists... Done

dinhquanghieu065@ubuntu:~$ sudo apt-get install openssh-client
[sudo] password for dinhquanghieu065:
Reading package lists... Done
```

```
dinhquanghieu@dinhquanghieu:~$
ECDSA key fingerprint is SHA256:eyeDwKR2dk0QnT00SkxGR6khpeoAKPC0kPASaxbovdg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.152.166' (ECDSA) to the list of known hosts.
dinhquanghieu@192.168.152.166's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 24 Oct 2021 08:42:23 AM UTC

System load:  0.0          Processes:      226
Usage of /:   22.5% of 18.57GB Users logged in: 1
Memory usage: 21%         IPv4 address for ens33: 192.168.152.166
Swap usage:   0%

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Sun Oct 24 08:10:47 2021
dinhquanghieu@dinhquanghieu:~$
```

```
dinhquanghieu@dinhquanghieu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dinhquanghieu/.ssh/
```

```
dinhquanghieu@dinhquanghieu:~$ sudo ssh-copy-id dinhquanghieu@192.168.152.166
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.152.166 (192.168.152.166)' can't be established.
```

```
dinhquanghieu@192.168.152.166's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 24 Oct 2021 09:15:35 AM UTC

System load:  0.0          Processes:      229
Usage of /:   22.5% of 18.57GB Users logged in: 1
Memory usage: 21%         IPv4 address for ens33: 192.168.152.166
Swap usage:   0%

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Sun Oct 24 08:42:23 2021 from 192.168.152.151
dinhquanghieu@dinhquanghieu:~$
```

So sánh :

WINDOWS	LINUX
Cài Đặt đơn giản xong tính an toàn không cao để nâng cao tính an toàn lên phải thiết lập các khóa an toàn hơn rất phức tạp	Cài đặt dễ dàng việc sử dụng dịch vụ openssh rất an toàn và dễ sử dụng
Song việc lạc gói tin mất gói tin vẫn có thể xảy ra do việc trễ gói tin là có thể vì không sử dụng dịch vụ QoS. Các gói tin trước khi đi ra ngoài mạng internet sẽ được mã hóa và bảo mật cao tránh việc ăn cắp.	Sử dụng 2 khóa công khai và khóa bảo mật để xác thực tránh việc mật khẩu người dùng bị chiếm đoạt và sử dụng..Dữ liệu,gói tin được mã hóa giúp tăng tính bảo mật an toàn cho gói tin nhiều hơn
Sử dụng kết nối để trao đổi sử dụng dữ liệu	Sử dụng kết nối có thể sử dụng các câu lệnh điều khiển,trao đổi dữ liệu từ máy chủ đến máy trạm và ngược lại
Tiêu tốn nhiều tài nguyên	Tiêu tốn ít tài nguyên
Các Dịch vụ chất lượng sẽ tốn tiền.	Giá thành rẻ hơn , phiên bản openssh miễn phí
Cần đăng nhập user và pass mỗi khi kết nối.	Có thể sử dụng tạo key để xác thực không cần pass giúp bảo mật password của user

Sử dụng VPN để truy nhập file,dữ liệu trong mạng của công ty	Sử dụng telnet và openssh để truy nhập từ xa vào giao diện dòng lệnh để điều khiển máy chủ.
Có thể sử dụng để truy nhập mạng nội bộ giữa 2 công ty doanh nghiệp(site to site) giữa người dùng đến công ty(client to site)	Sử dụng để kết nối giữa máy trạm và máy chủ
Tạo cấp người dùng có thể truy cập vào tài nguyên thông qua quản lý người dùng trong máy chủ miền	Cho phép,cấm người dùng thông qua file /etc/ssh/sshd_config

V. Sao lưu và khôi phục

1. Giới thiệu chung

- Sao lưu (back-up) về cơ bản là tạo các bản sao của dữ liệu để có thể khôi phục (restore) dữ liệu gốc trong tình huống lỗi.

- Các dữ liệu sao lưu có thể được lưu trữ trên nhiều phương tiện khác nhau như ổ đĩa cứng, ổ đĩa quang, hay băng từ. Qua thời gian, ổ đĩa cứng đã chứng minh được sự vượt trội nhờ chi phí không lớn, tốc độ cao.

- Việc sao lưu có thể thực hiện qua các phương pháp:

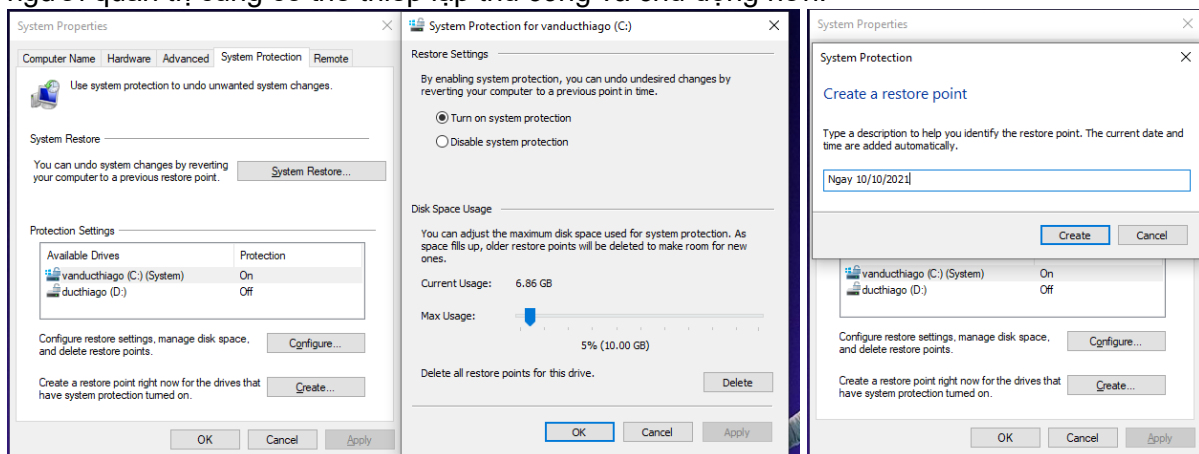
- *Trực tuyến*: Dùng đĩa cứng hoặc chuỗi đĩa cứng có thể khôi phục ngay lập tức, đòi hỏi chi phí cao
- *Cận trực tuyến*: thường dùng băng từ, thời gian khôi phục lâu hơn
- *Không trực tuyến*: cần thao tác của người quản trị để thực hiện sao lưu nên không tối ưu về thời gian
- *Sao lưu toàn bộ*: sao lưu toàn bộ hệ thống phòng sự cố có thể chuyển sang vị trí khác để hoạt động, đòi hỏi sao lưu cả thiết bị

- Người quản trị có thể cân nhắc các phương pháp sao lưu sau:

- *Sao lưu toàn bộ*: Tạo bản sao toàn bộ file và dữ liệu
- *Sao lưu tăng dần*: Sao lưu toàn bộ tiếp theo là sao lưu tăng dần
- *Sao lưu khác biệt*: Sao lưu toàn bộ tiếp theo là sao lưu các file và dữ liệu khác biệt.

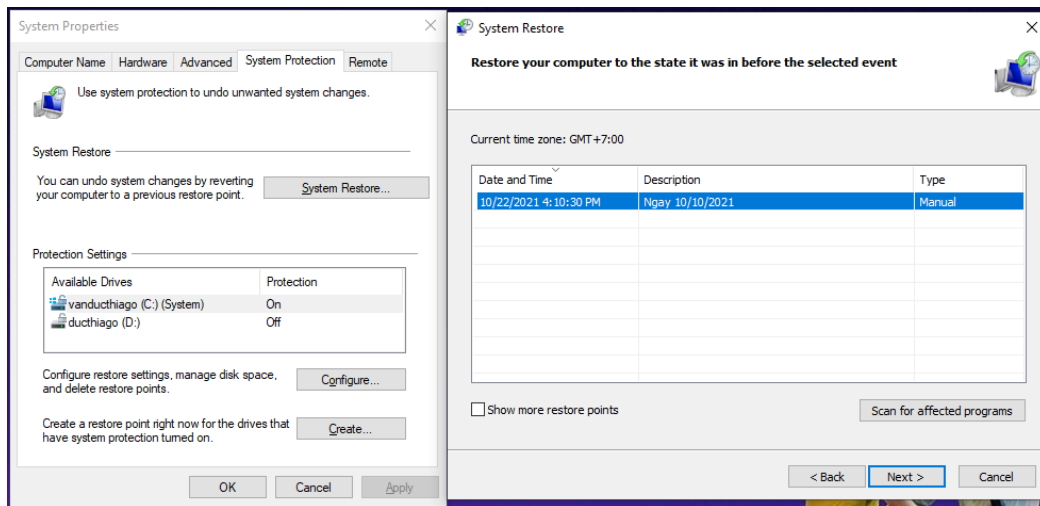
2. Trên hệ điều hành Windows

- Có thể chọn sao lưu dữ liệu trên Windows 10 với System Restore. Từ Windows 8 thì Microsoft đã bật tính năng System Protection tự động trên ổ đĩa logic chứa hệ điều hành(thường là ổ đĩa C) với dung lượng bản sao lưu có dung lượng tùy chọn để đưa máy về 1 thời điểm cố định. Chúng được thiết lập tự động nhưng người quản trị cũng có thể thiết lập thủ công và chủ động hơn:



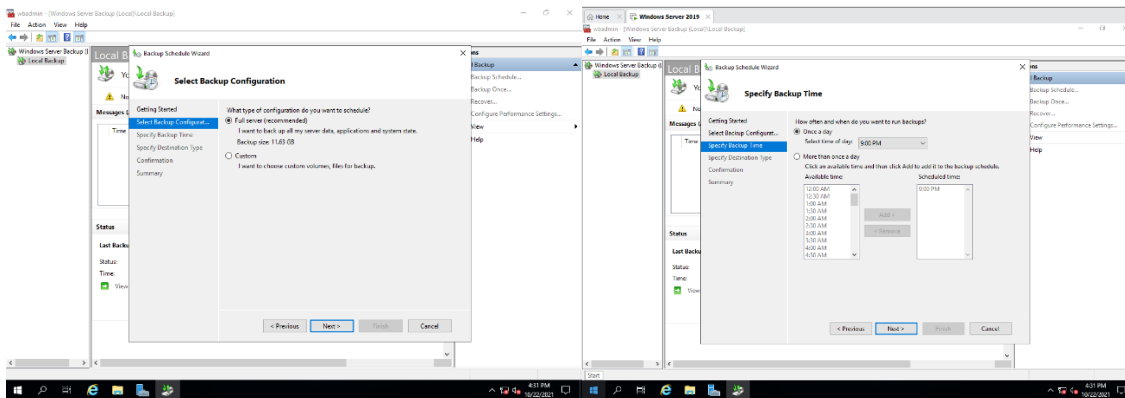
Ổ C có sao lưu tự động

Tự tạo bản sao lưu



Phục hồi

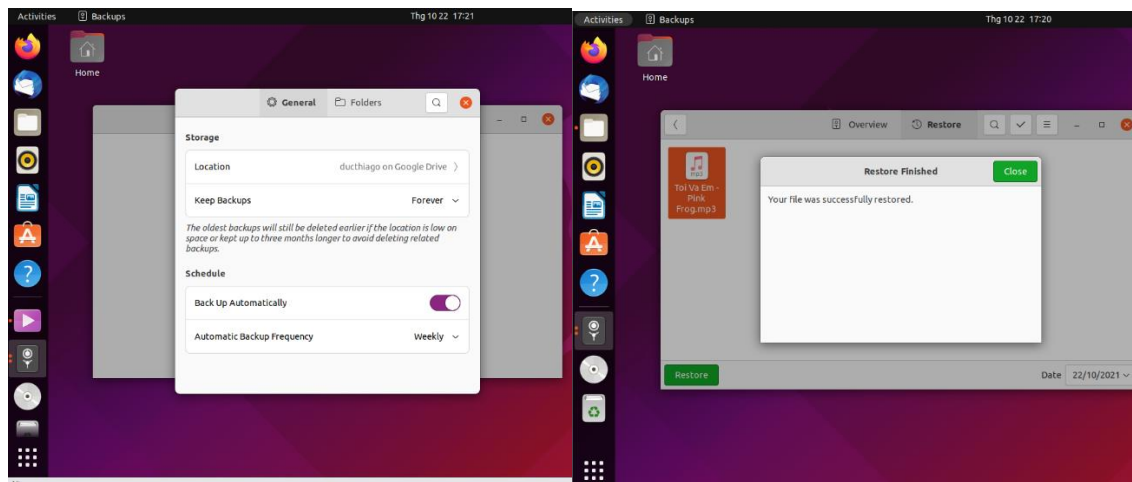
Hoặc tại Windows Server có thể dùng chương trình “Windows Server backup”:



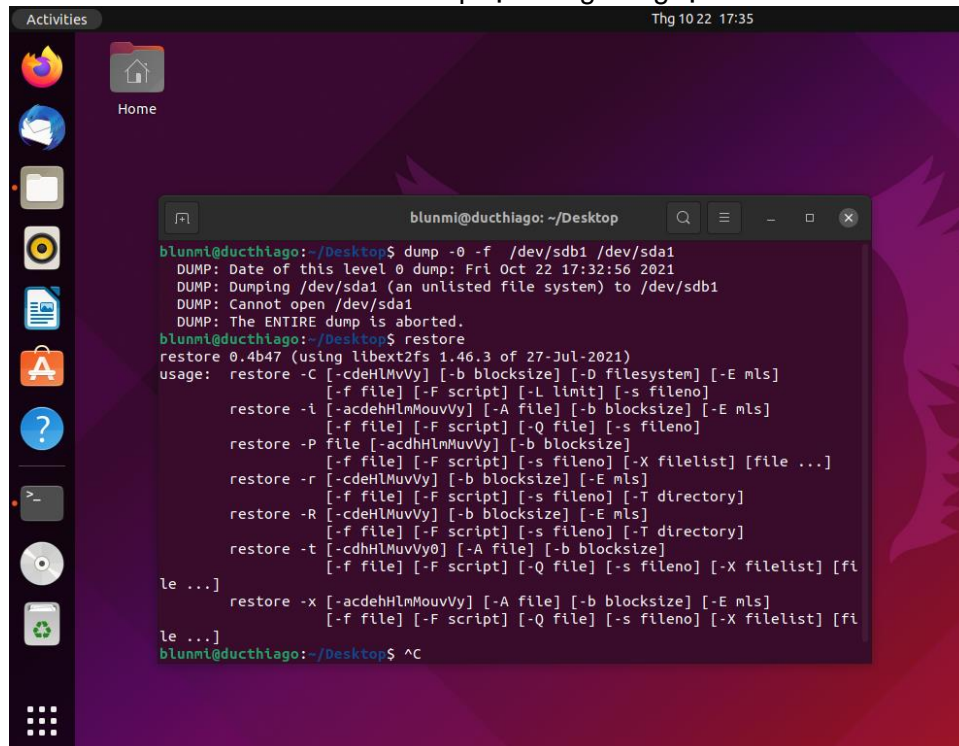
3. Hệ điều hành Linux (Ubuntu)

Việc sao lưu trong Ubuntu được thực hiện qua cả 3 phương thức là: dòng lệnh, giao diện đồ họa hoặc qua các bộ phần mềm theo các cấp độ sao lưu từ 0 đến 9.

- Sao lưu và khôi phục bằng giao diện đồ họa:



-Sao lưu và khôi phục bằng dòng lệnh:



The screenshot shows a terminal window titled 'blunmi@ducthiago: ~/Desktop'. The user has executed the following commands and received the following output:

```
blunmi@ducthiago:~/Desktop$ dump -0 -f /dev/sdb1 /dev/sda1
DUMP: Date of this level 0 dump: Fri Oct 22 17:32:56 2021
DUMP: Dumping /dev/sda1 (an unlisted file system) to /dev/sdb1
DUMP: Cannot open /dev/sda1
DUMP: The ENTIRE dump is aborted.
blunmi@ducthiago:~/Desktop$ restore
restore 0.4b47 (using libext2fs 1.46.3 of 27-Jul-2021)
usage: restore -C [-cdeHLMuvVy] [-b blocksizes] [-D filesystem] [-E mls]
       [-f file] [-F script] [-L limit] [-s fileno]
       [-i [-acdeHLMuvVy] [-A file] [-b blocksizes] [-E mls]
       [-f file] [-F script] [-Q file] [-s fileno]
       [-P file [-acdHLMuvVy] [-b blocksizes]
       [-f file] [-F script] [-s fileno] [-X filelist] [file ...]
       [-r [-cdeHLMuvVy] [-b blocksizes] [-E mls]
       [-f file] [-F script] [-s fileno] [-T directory]
       [-R [-cdeHLMuvVy] [-b blocksizes] [-E mls]
       [-f file] [-F script] [-s fileno] [-T directory]
       [-t [-cdHLMuvVy0] [-A file] [-b blocksizes]
       [-f file] [-F script] [-Q file] [-s fileno] [-X filelist] [fi
le ...]
       [-x [-acdeHLMuvVy] [-A file] [-b blocksizes] [-E mls]
       [-f file] [-F script] [-Q file] [-s fileno] [-X filelist] [fi
le ...]
blunmi@ducthiago:~/Desktop$ ^C
```

4. Nhận xét

- Cả Windows và Ubuntu đều có thể cài đặt ở chế độ người dùng, hỗ trợ việc sao lưu file có lịch trình, sao lưu trên ổ cứng, sao lưu trên cloud(google drive, one drive, ...) hoặc từ một mạng khác.
- Ubuntu dễ dàng sao lưu hơn Windows ở chế độ dòng lệnh, đa dạng hóa trong các cấp độ sao lưu, đồng thời có khả năng bảo mật dữ liệu mạnh hơn.
- Windows có khả năng hỗ trợ người dùng phổ thông cài đặt và quản trị dễ dàng hơn nhờ giao diện đồ họa mạnh và tự động, có lợi thế hơn trong sao lưu từ network server vì hệ điều hành này rất phổ biến.
- Ubuntu dễ dàng sao lưu hơn Windows ở chế độ dòng lệnh đồng thời có khả năng quản trị mạnh hơn.

