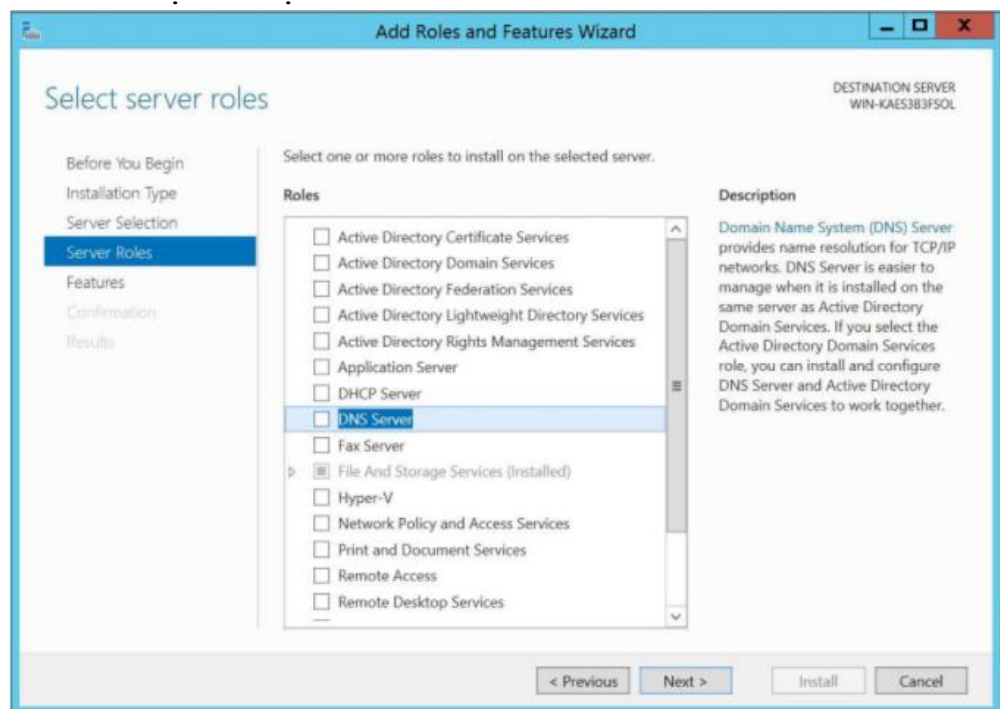


1. So sánh cài đặt và quản trị giữa Windows và Linux(Ubuntu) về dịch vụ DNS/DHCP

- Khác nhau cơ bản :
 - Cài đặt và quản trị trên Windows qua giao diện đồ họa (tiện ích “Server Manager”).)
 - Cài đặt và quản trị trên Linux qua file cấu hình
- Khác nhau chi tiết
 - ❖ Windows
 - DNS :
 - Việc cài đặt máy chủ DNS khá dễ dàng qua tiện ích “Server Manager”. Chức năng máy chủ DNS được liệt kê trong phần lựa chọn các chức năng cài đặt như trong hình dưới. Người quản trị tuân theo hướng dẫn của tiện ích để hoàn tất việc cài đặt.



- Máy chủ DNS có thể quản lý hoặc miền chính (primary zone) hay miền thứ cấp (secondary zone) hay cả hai. Miền chính cho phép cập nhật các bản ghi về tên miền, trong khi đó miền thứ cấp không cho phép sửa đổi các bản ghi tên miền mà chỉ lưu bản sao của miền chính. Khi đặt cấu hình cho máy chủ DNS có hai kiểu vùng khác nhau:

- Vùng tìm kiếm thuận (Forward Lookup Zone): cho phép máy tính truy vấn địa chỉ Internet ứng với một tên
- Vùng tìm kiếm nghịch (Reverse Lookup Zone): là việc ngược lại trả lại tên miền ứng với địa chỉ Internet
- Các dạng bản ghi DNS
 - Bản ghi khởi đầu 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 máy chủ: thông tin căn bản ánh xạ tên của một máy chủ ra địa chỉ mạng Internet
 - Bản ghi CNAME: ánh xạ máy chủ tới một tên có sẵn
 - Bản ghi NS: lưu định danh các máy chủ DNS trong miền
 - Bản ghi dịch vụ SRV: hỗ trợ việc tự động phát hiện các tài nguyên TCP/IP có trên mạng
 - Bản ghi con trỏ PTR: là các bản ghi tìm kiếm ngược
 - Bản ghi máy chủ thư: chỉ định máy chủ nhận thư của miền.
- ⇒ Việc điền các thông tin vào các bản ghi này có thể được thực hiện một cách thuận tiện thông qua việc sử dụng giao diện đồ họa như cửa sổ nhập bản ghi SOA dưới đây.

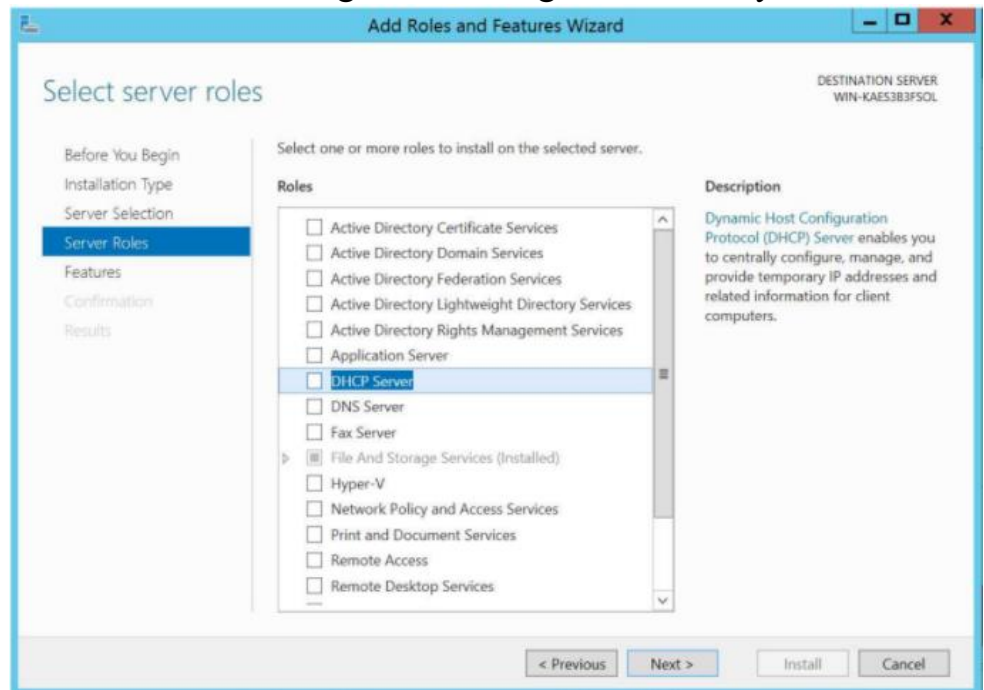


Hình III-4. Cửa sổ nhập bản ghi SOA.

- Một số điểm chú ý khi cài đặt máy chủ DNS cần xem xét :
 - 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
- ⇒ Với mức độ sử dụng tiêu biểu, mỗi máy chủ DNS cần khoảng 4MB bộ nhớ để chạy, khi số lượng các bản ghi tăng thì máy chủ DNS cần thêm bộ nhớ để hoạt động. Trung bình 1000 bản ghi cần thêm khoảng 100KB bộ nhớ.

- DHCP :

- Cài đặt dịch vụ DHCP khá dễ dàng thông qua giao diện của tiện ích “Server Manager” như trong hình dưới đây.



- ⇒ Để bắt đầu quá trình cài đặt và cấu hình DHCP server , bạn có thể kích vào Add Roles từ cửa sổ Initial Configuration Tasks hoặc từ Server Manager à Roles à Add Roles.
- ⇒ Khi Add Roles Wizard xuất hiện, bạn hãy kích Next trên màn hình đó. Tiếp đến, chọn thành phần muốn bổ sung, DHCP Server Role, sau đó kích Next.
- ⇒ Nếu không có địa chỉ IP tĩnh được gán trên máy chủ thì bạn sẽ gặp một cảnh báo, cảnh báo này thông báo cho bạn biết rằng bạn không nên cài đặt DHCP với một địa chỉ IP động. Ở đây, bạn sẽ được nhắc nhở về các thông tin IP mạng, thông tin về phạm vi và các thông tin DNS. Nếu chỉ cài đặt DHCP server bạn chỉ cần kích **Next** xuyên suốt quá trình cài đặt. Mặt khác, bạn cũng có thể cấu hình tùy chọn DHCP Server trong suốt giai đoạn này của quá trình cài đặt. Trong trường hợp cấu hình một số thiết lập IP cơ bản và cấu hình DHCP Scope đầu tiên.

- ⇒ Tiếp đến, nhập vào **Parent Domain, Primary DNS Server**, và **Alternate DNS** và kích **Next**.
- ⇒ Lựa chọn NOT để sử dụng WINS trên mạng của mình và kích **Next**. Sau đó chúng ta sẽ được tăng cấp để cấu hình DHCP scope cho DHCP Server mới. Chọn địa chỉ IP là 172.30.2.1.10. Để thực hiện điều đó, bạn cần kích **Add** để bổ sung thêm một phạm vi mới. Chọn **Disable DHCPv6 stateless mode** cho máy chủ này và kích **Next**. Sau đó xác nhận DHCP Installation Selections và kích **Install**.
- ⇒ Sau đó một vài giây, DHCP Server sẽ được cài đặt và ta sẽ thấy một cửa sổ xuất hiện (Hình ảnh). Cửa sổ này giúp bạn hoàn thành xong quá trình cài đặt và cấu hình DHCP server rồi đó

Kiểm tra cài đặt : Sau khi cài đặt dịch vụ DNS và DHCP, người quản trị có thể sử dụng các câu lệnh sau từ cửa sổ dòng lệnh để kiểm tra tình trạng hoạt động của các máy tính trong mạng

- *ping* kiểm tra kết nối mạng tới một máy tính trong mạng Internet.
- *nslookup* kiểm tra việc cài đặt cấu hình DNS
- *ipconfig* xem các tham số mạng được đặt cho máy tính như địa mạng, địa chỉ máy chủ DNS. Ngoài ra, lệnh này có thể dùng để yêu cầu cập lại địa chỉ mạng

Linux :

❖ DNS:

- Ubuntu cung cấp dịch vụ DNS qua gói phần mềm BIND (Berkley Internet Naming Daemon). Phần mềm này có thể tải về và cài đặt qua câu lệnh sau
sudo apt-get install bind9
- Các file cấu hình dịch vụ DNS được đặt trong thư mục */etc/bind*. Trong thư mục này, file cấu hình chính là *named.conf* và *db.root* cung cấp thông tin về máy chủ DNS gốc, và các file dữ liệu cụ thể về địa chỉ Internet/tên miền và ngược lại.
- Để cài đặt máy chủ tên miền chính cho miền “*example.com*”, người quản trị cần sửa đổi file cấu hình */etc/bind/etc/bind/named.conf.local* bằng bất kỳ tiện ích soạn thảo nào như *vi*, *nano*, hay *gedit* với nội dung như sau:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

- Với thẻ file mô tả vị trí của file db.example.com chứa các dữ liệu về tên miền và địa chỉ Internet. Bước tiếp theo là tạo dữ liệu cho file db.example.com bằng cách xây dựng các bản ghi theo các cấu trúc như sau:
 - ⇒ Bản ghi SOA: bản ghi khởi đầu cho các mục khác trong file và mô tả các tham số cấu hình cơ bản như số sê-ri của dữ liệu, tên miền gốc, thời gian làm mới, thời gian đệm ...
 - ⇒ Bản ghi NS: thông báo máy chủ lưu các bản ghi cho vùng tên miền theo cấu trúc “*ns IN A địa_chỉ_IP*”. Ví dụ: *ns IN A 192.168.1.10*
 - ⇒ Bản ghi A: cho biết tên và địa chỉ Internet theo cấu trúc “*Tên IN A địa_chỉ_IP*”. Ví dụ: *www IN A 192.168.1.12*
 - ⇒ Bản ghi CNAME: tạo ánh xạ tới bản ghi A, ví dụ: *Web IN CNAME www*
 - ⇒ Bản ghi PTR: tạo ánh xạ từ địa chỉ sang tên theo cấu trúc “*Địa_chỉ_IP IN PTR tên_đầy_đủ*”. Ví dụ: *192.168.1.2 IN PTR mail.mydomain.*
- Dưới đây là file “db.example.com” chứa dữ liệu về địa chỉ sử dụng cho máy chủ tên miền:

```

$TTL      604800
@         IN      SOA      example.com. root.example.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
;
@         IN      NS       ns.example.com.
@         IN      A        192.168.1.10
@         IN      AAAA     ::1
ns        IN      A        192.168.1.10

```

- Điều cần chú ý là số sê-ri trong bản ghi SOA được tăng lên sau mỗi lần thay đổi dữ liệu. Để việc thay đổi có hiệu lực, người quản trị cần khởi động lại dịch vụ DNS thông qua câu lệnh *"sudo service bind9 restart"*.
- Để tạo cơ sở dữ liệu cho dịch vụ tra cứu địa chỉ/tên miền hay còn gọi là dịch vụ tra cứu tên miền ngược, như cho dải địa chỉ 192.168.1.*, người quản trị cần sửa đổi file cấu hình *"/etc/bind/named.conf.local"* nội dung sau:

```

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};

```

- Sau đó, dùng trình soạn thảo văn bản tạo nội dung dữ liệu cho file */etc/bind/db.192* như dưới đây:

```

$TTL      604800
@         IN      SOA      ns.example.com. root.example.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
;
@         IN      NS       ns.
10        IN      PTR      ns.example.com.

```

- Dịch vụ DNS cần khởi động lại để các thay đổi có hiệu lực.

- Để kiểm tra các cài đặt dịch vụ DNS có hoạt động như mong muốn, người quản trị có thể sử dụng các câu lệnh kiểm tra sau:
 - ⇒ *ping*: Kiểm tra máy trạm gắn với tên miền có hoạt động hay không
 - ⇒ *named-checkzone*: kiểm tra dữ liệu tên
 - ⇒ *nslookup*: kiểm tra tên Internet

❖ DHCP

- Dịch vụ DHCP được cung cấp thông qua nhiều gói phần mềm khác nhau như trên RedHat, Debian, Ubuntu. Phần dưới đây trình bày phần cài đặt sử dụng gói phần mềm của Ubuntu sử dụng công cụ quản lý phần mềm apt-get. Trước khi cài đặt phần mềm người dung quản trị cần xác định giao tiếp mạng nào sẽ chịu trách nhiệm quảng bá hay cung cấp dịch vụ DHCP. Thông thường giao tiếp mạng eth0 được chọn trong trường hợp máy chủ chỉ có một giao tiếp mạng. Câu lệnh sử dụng đặc quyền để cài đặt phần mềm dịch vụ như sau:

sudo apt-get install isc-dhcp-server

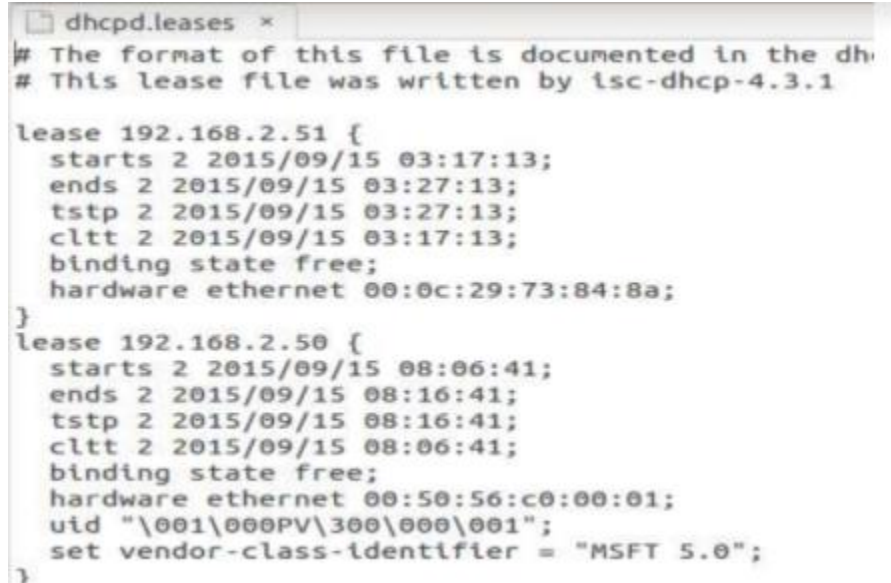
- Các thông tin cài đặt cho máy chủ DHCP được lưu tại */etc/default/isc-dhcp-server*. Các thông tin cần bản cần cung cấp là giao tiếp mạng chạy dịch vụ DHCP, chi tiết về cấu hình mạng. Thông tin về địa chỉ cấp cho các máy tính trong mạng được mô tả trong file */etc/dhcp/dhcpd.conf* có cấu trúc như dưới đây.

```
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.150 192.168.1.200;
    option routers 192.168.1.254;
    option domain-name-servers 192.168.1.1, 192.168.1.2;
    option domain-name "mydomain.example";
}
```

Các thông tin cần mô tả trong file cấu hình gồm có dải địa chỉ mạng, máy chủ cổng, các máy chủ DNS và tên miền. Người quản trị có thể sửa đổi nội dung file cho phù hợp với yêu cầu quản trị.

- 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*



```

dhcpd.leases x
# The format of this file is documented in the dh
# This lease file was written by isc-dhcp-4.3.1

lease 192.168.2.51 {
  starts 2 2015/09/15 03:17:13;
  ends 2 2015/09/15 03:27:13;
  tstp 2 2015/09/15 03:27:13;
  cltt 2 2015/09/15 03:17:13;
  binding state free;
  hardware ethernet 00:0c:29:73:84:8a;
}
lease 192.168.2.50 {
  starts 2 2015/09/15 08:06:41;
  ends 2 2015/09/15 08:16:41;
  tstp 2 2015/09/15 08:16:41;
  cltt 2 2015/09/15 08:06:41;
  binding state free;
  hardware ethernet 00:50:56:c0:00:01;
  uid "\001\000PV\300\000\001";
  set vendor-class-identifier = "MSFT 5.0";
}

```

- Ngoài ra, người quản trị có thể sử dụng các câu lệnh có đặc quyền để kiểm tra và khởi động lại dịch vụ DHCP “*sudo service isc-dhcp-server status/restart*”

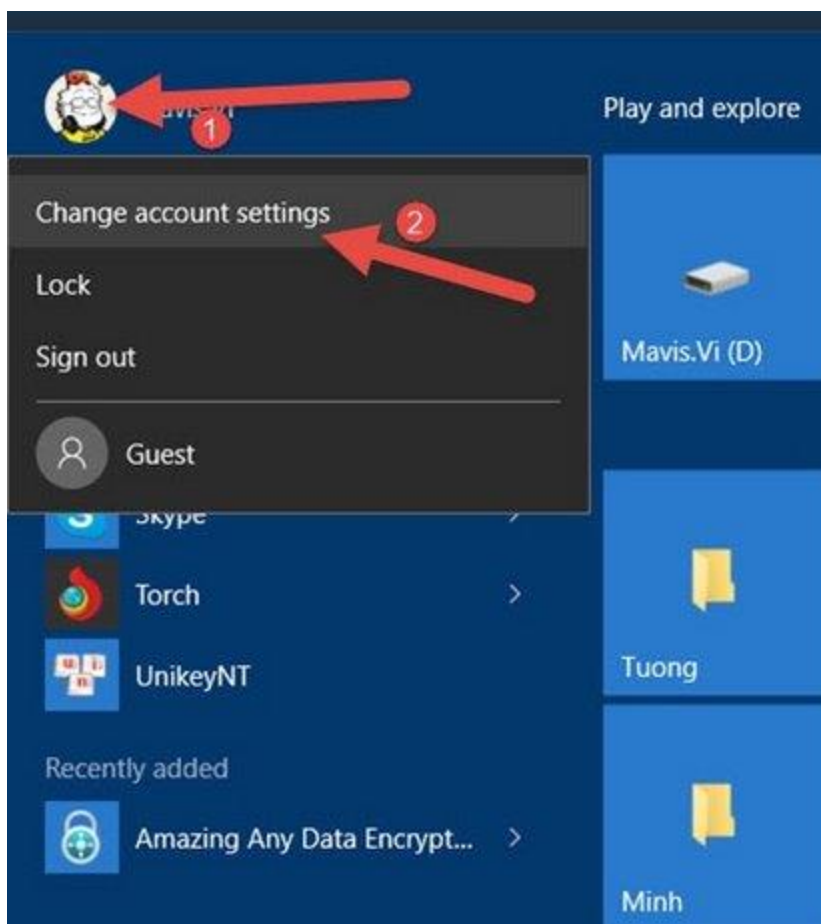
2. Quản lý người dùng và máy tính

CÁC MỤC

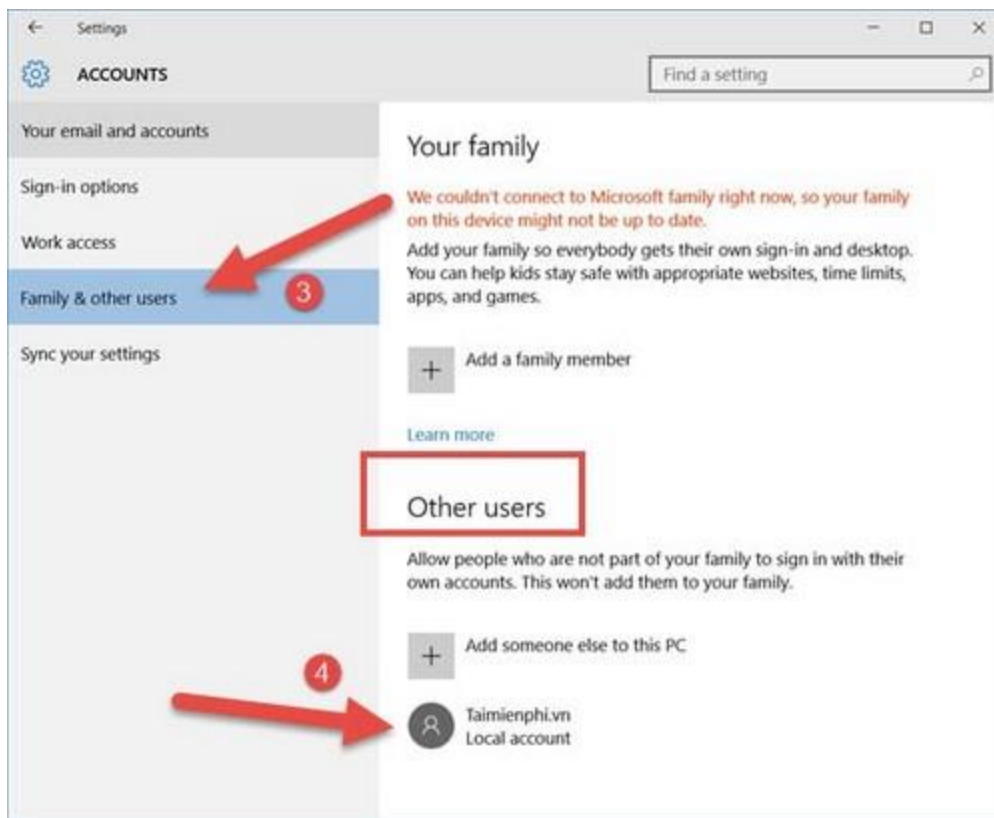
- Phân quyền Admin cho User trong Win 10
- Tạo và xóa user, tài khoản người dùng mới trên Windows 10
- Tạo và quản lý user_linux

PHÂN QUYỀN ADMIN CHO USER TRONG WIN 10

Bước 1: Mở MenuStart click vào tài khoản đang sử dụng và chọn **Change Account settings**.

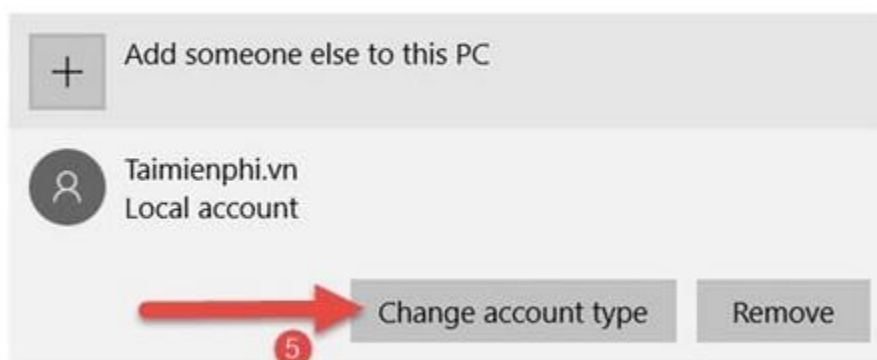


Bước 2: Vào mục **Family & other users** chọn **Other Users** khác.

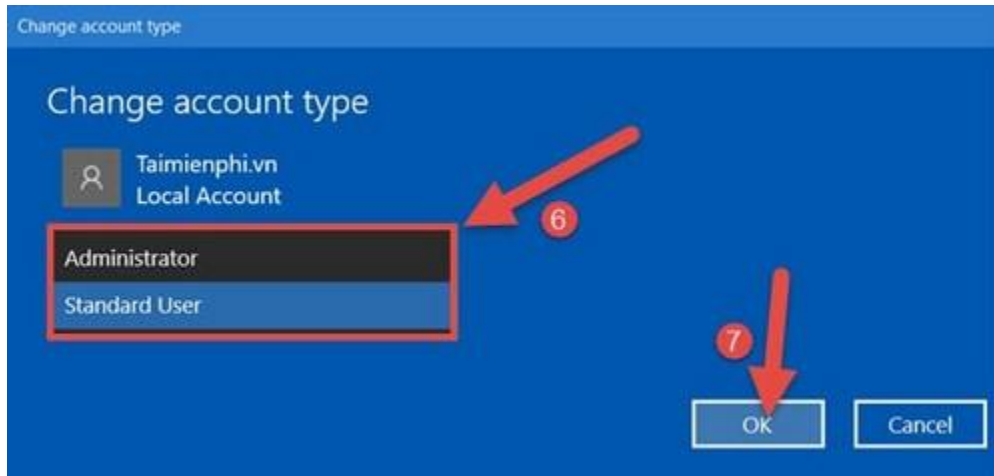


Bước 3: Click vào chọn **Change account type**.

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



Bước 4: Tương tự như Win 8, bạn được quyền chọn quyền cao cấp nhất là **Administrator** hoặc quyền giới hạn với **Standard User**, chọn lựa Administrator xong OK là hoàn tất nhé.



Như vậy là bạn đã hoàn tất việc set quyền admin cho win 8.

Tạo và xóa user, tài khoản người dùng mới trên Windows 10

Sử dụng và quản lý các User trong hệ thống Windows 10 giúp bạn dễ dàng chia sẻ máy tính cho nhiều đồng nghiệp và bạn học khi phải sử dụng chung một chiếc máy tính duy nhất.



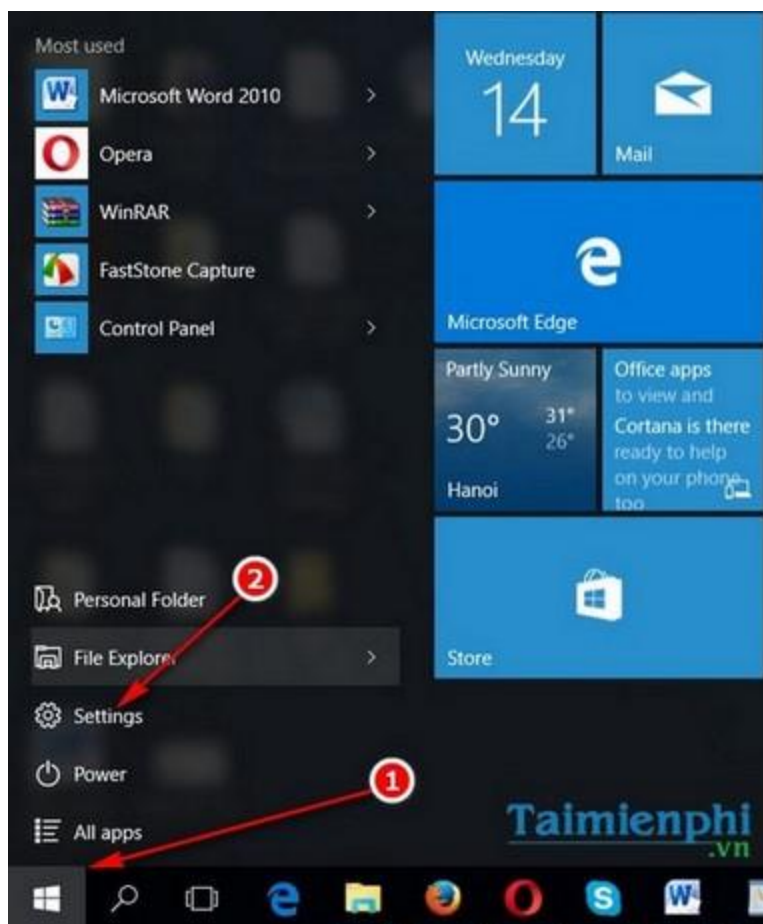
TẠO VÀ XÓA TÀI KHOẢN USER TRONG WINDOWS 10

*Đối Với Phiên Bản Windows 10 Mới (Bản Build Mới)

Hướng dẫn tạo tài khoản Windows 10 này có thể áp dụng cho người dùng đã lập hoặc chưa lập tài khoản người dùng Windows 10.

Cách 1: Tạo tài khoản Windows 10, thiết lập user Win 10 thông qua Settings.

Bước 1: Truy cập vào **Settings** trên Windows 10, đối với người dùng mới, bạn có thể sử dụng tổng hợp khá nhiều cách vào Settings trên Windows 10 đã được Taimienphi.vn chia sẻ trong bài viết trước đó nhé. Cách nhanh nhất là sử dụng cụm phím tắt Windows + I để truy cập vào Settings.

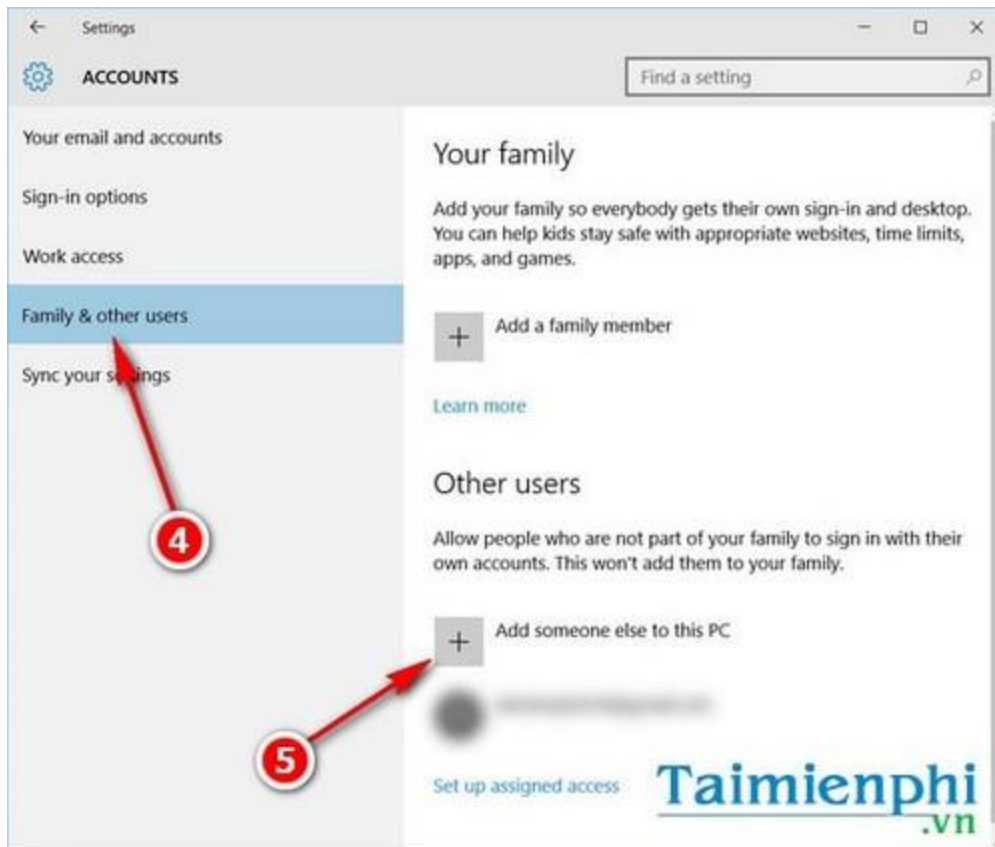


Bước 2: Truy cập mục **Account** trong Settings.

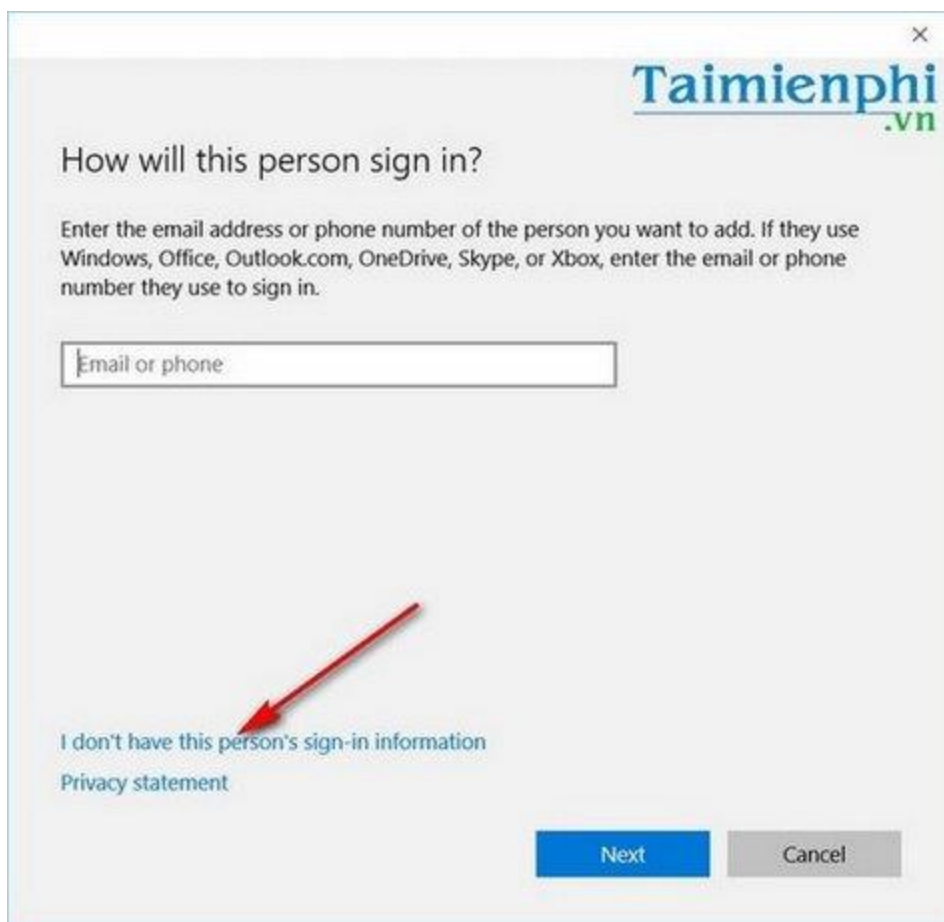


Bước 3: Tại đây, bạn click chọn mục **Family & other user** để truy cập thư mục cài đặt email và tài khoản người dùng. Kéo xuống tại mục **Other users**. Đây là mục cho phép bạn thêm tài khoản người dùng Windows 10 khác đăng nhập vào máy tính.

Click vào mục **Add someone else to this PC** để thêm tài khoản người dùng Windows 10.



Bước 4: Nhập địa chỉ email đăng nhập vào tài khoản người dùng nếu bạn có tài khoản Outlook của Microsoft. Tiếp tục nhấn **Next**.



How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Email or phone

[I don't have this person's sign-in information](#)

[Privacy statement](#)

Next Cancel

Chú ý: Nếu bạn không có tài khoản của Microsoft, bạn click chọn mục **I don't have this person's sign-in information**. Đây là mục cho phép bạn tạo tài khoản người dùng mà không phải là người dùng có tài khoản Microsoft. Đây cũng chính là **tài khoản Local** (tài khoản người dùng trên máy).

Bước 5: Trong bài viết này, Taimienphi.vn giới thiệu tới bạn cách tạo user, tạo tài khoản người dùng Windows 10 bằng tài khoản Microsoft. Nhập lần lượt thông tin vào các ô dưới đây:

- **First name:** tên họ
- **Last name:** tên chính
- **Someone@example.com:** địa chỉ email của bạn. Không yêu cầu phải là tài khoản outlook của Microsoft, bạn có thể đăng nhập tài khoản Gmail để thay thế.
- **Password:** mật khẩu của địa chỉ email

Taimienphi.vn

Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* [Learn more](#)

Taimienphi

.vn

taimienphi216@outlook.com

×

Get a new email address

.....

Vietnam

▼

*If you already use a Microsoft service, go Back to sign in with that account.

[Add a user without a Microsoft account](#)

Next

Back

6

Cuối cùng là chọn quốc gia và nhấn **Next**.

×

Taimienphi
.vn

Add security info

Your security info helps protect your account. We'll use this to help you recover your password, help keep hackers out of your account, and get in if you get blocked. We won't use it for spam.

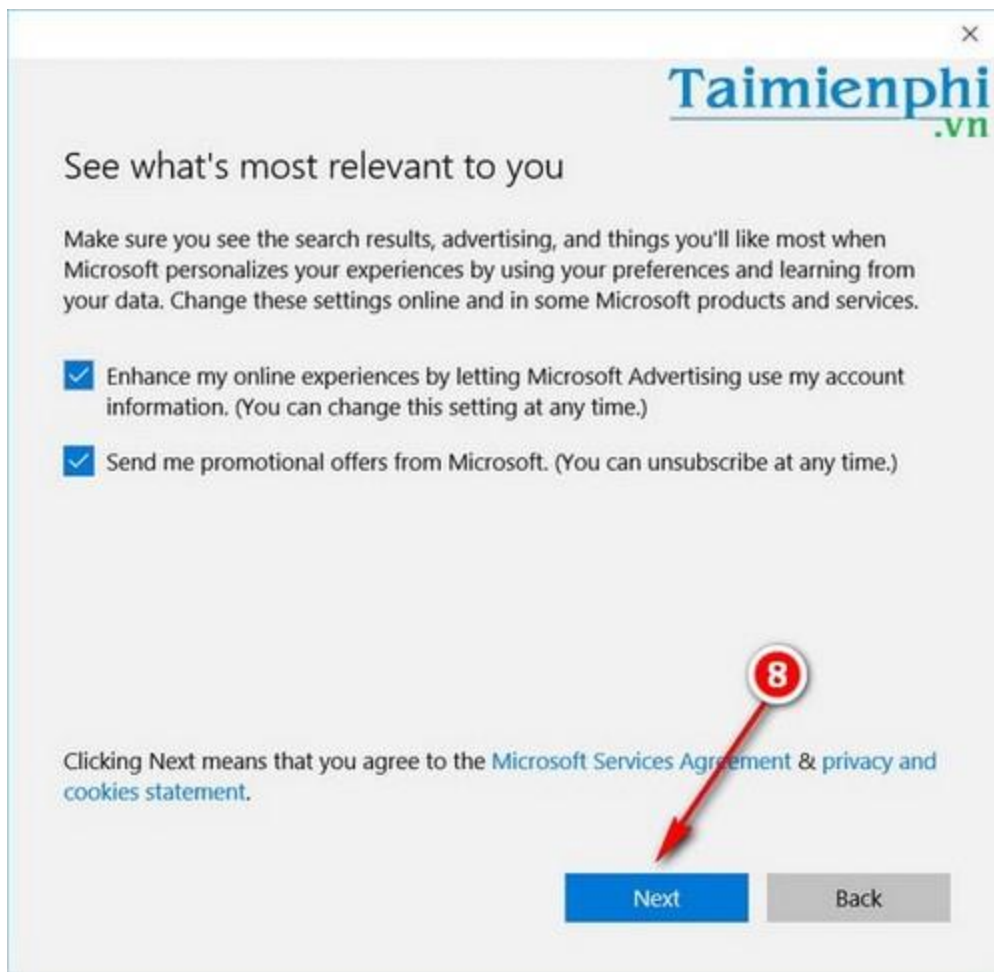
Vietnam (+84) ▾

▢ ×

[Add an alternate email instead](#)

Next Back

Nếu có số điện thoại hoặc email khác hãy nhập tại bước này để có thể khôi phục mật khẩu tài khoản Microsoft trong trường hợp bị mất.



Đồng ý với các điều khoản người dùng của Microsoft và tạo thành công tài khoản người dùng trên Windows 10.



Bạn đã tạo được một tài khoản Windows 10 mới.

Đối với tài khoản user, tài khoản người dùng vừa mới được tạo, bạn cũng có thể chuyển quyền quản trị từ tài khoản chính sang cho tài khoản này trong chính thiết lập **Account** của Windows 10

Cách 2: Tạo tài khoản Windows 10, tạo user Windows 10 mới bằng User Account

Bước 1: Truy cập **User Account** trên Windows 10 bằng cách vào **Control Panel > UserAccount > Change Account type**.



Vào Control Panel trên Windows 10 > chọn **User Account** sau đó nhấn trực tiếp vào tùy chỉnh **Change Account type**.



Hoặc cách nhanh nhất để truy cập vào trang cài đặt, tạo tài khoản Windows 10, tạo user Win 10 mới bằng cách nhấn **Start Menu** > gõ **User** và nhấn vào kết quả tìm kiếm.



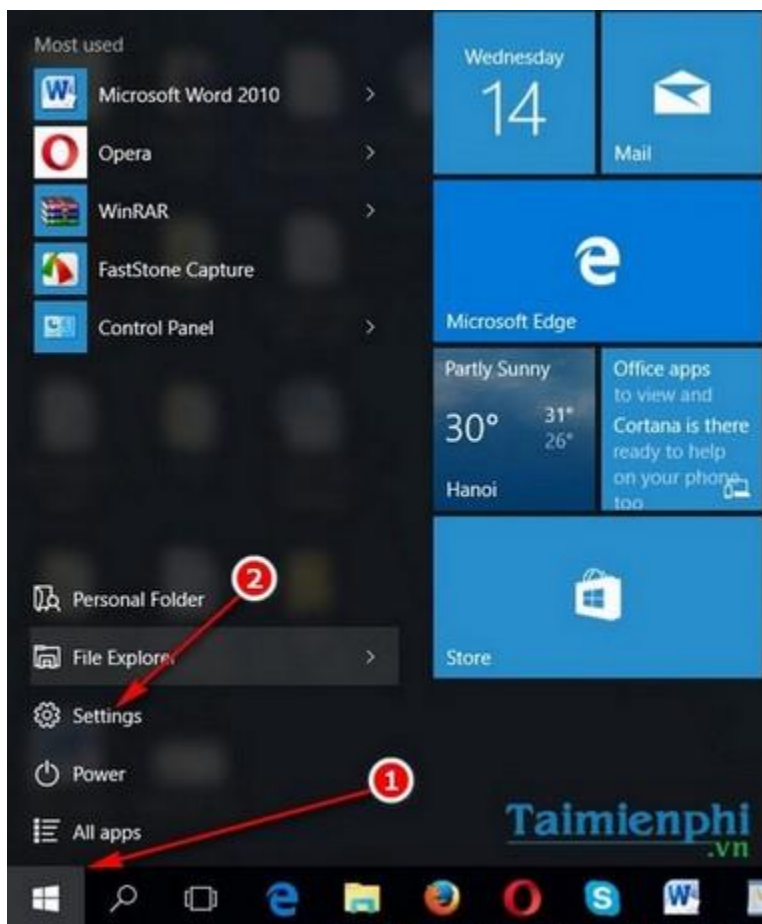
Trong chức năng **User Accounts**, các bạn nhấn chọn mục **Manage Other Account**, sau đó click chọn mục **Add a new user in PC settings** như cách trên.



Bước 3: Hệ thống sẽ tự động đưa bạn tới chức năng **Family & other user** trên Windows 10. Tại đây, bạn thực hiện theo các bước mà Taimienphi.vn đã hướng dẫn ở **Cách 1**.

XÓA TÀI KHOẢN NGƯỜI DÙNG TRÊN WINDOWS 10

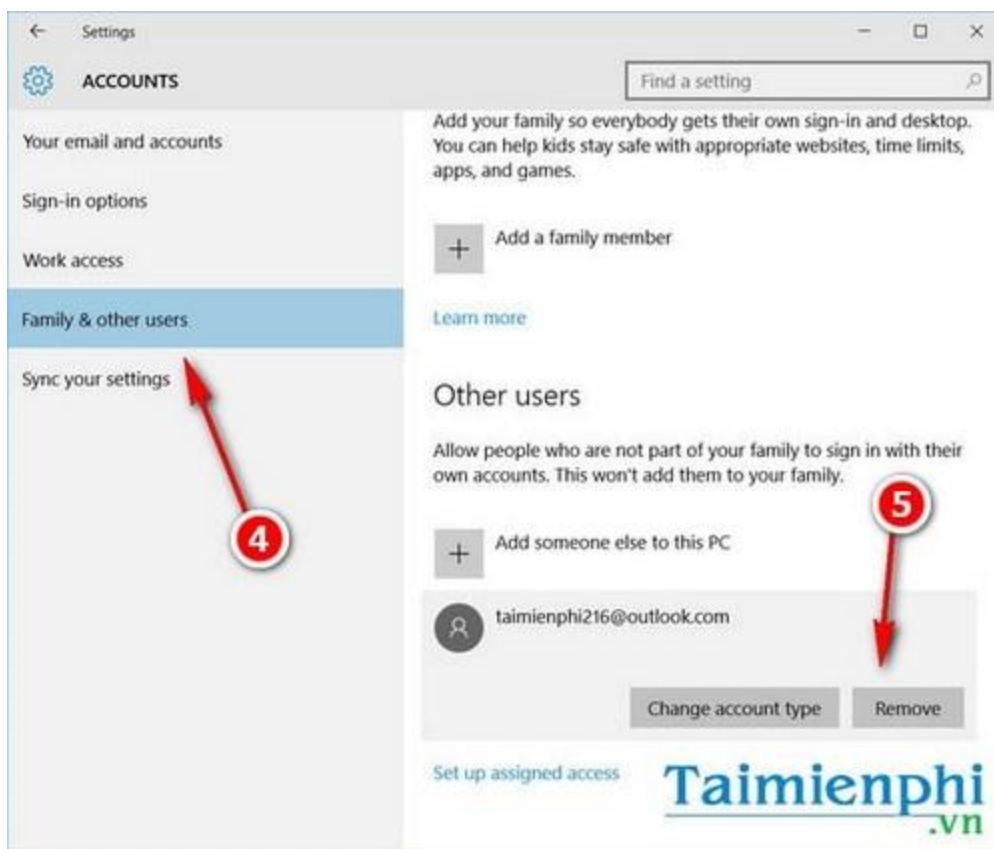
Bước 1: Truy cập Settings trên Windows 10 giống như cách đã thực hiện ở thao tác tạo tài khoản người dùng trên Windows 10.



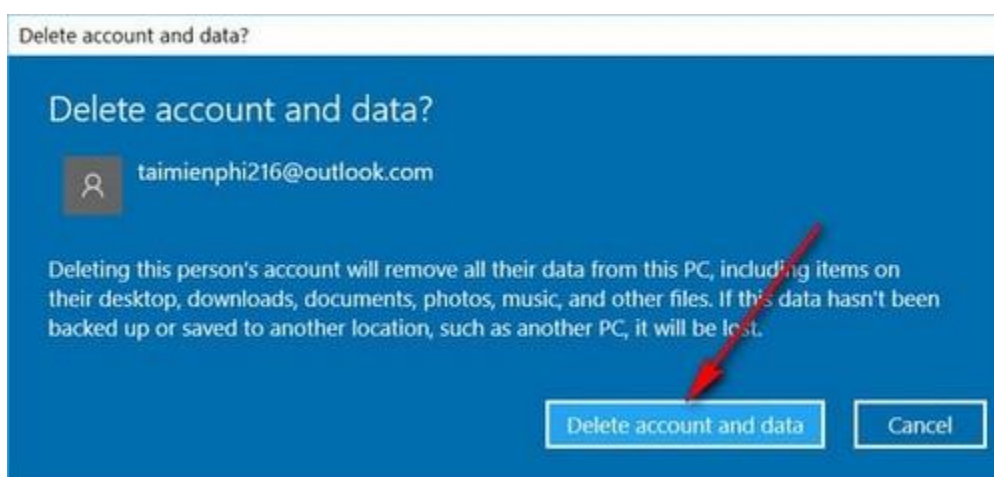
Bước 2: Truy cập **Accounts > Family & other user > Other user**



Bước 3: Click chuột vào tài khoản người dùng trên Windows 10 vừa mới tạo. Tại đây bạn sẽ thấy có hai tùy chọn **Change account type** và **Remove**. Bạn click chọn **Remove** để xóa tài khoản người dùng.



Hệ thống sẽ hỏi lại người dùng để xác nhận xóa, sau khi xóa mọi dữ liệu của người dùng này bao gồm file download, thư mục, hình ảnh, nhạc trên máy tính sẽ bị xóa sạch, do đó bạn cần hết sức cẩn nhắc nhé. Nhấn **Delete account and data** để xóa tài khoản người dùng Win 10.



TẠO VÀ QUẢN LÝ USER – LINUX.

Giới thiệu chung

Khi thêm một user vào hệ thống, người quản trị cần biết vai trò của các tập tin sau (trong thư mục /etc): passwd, shadow, group, gshadow

/etc/passwd: chứa thông tin của tất cả các user: login name, user ID, Group ID, Full Name, Home directory, loại shell

/etc/shadow chứa các thông số điều khiển quá trình user login:

user password (dạng hash, không đọc được), và thông tin thời hạn mật khẩu

/etc/group chứa thông tin về group của users

/etc/gshadow chứa password của group dưới dạng hash (ít khi dùng đến).

2. Nội dung

+ Thêm nhóm người dùng

Mỗi dòng trong file /etc/group chứa thông tin về một nhóm người dùng trong hệ thống.

Các câu lệnh để chỉnh sửa thông tin về group: groupadd, groupmod, groupdel

/etc/passwd

Mỗi dòng trong file /etc/passwd ứng với một người dùng trong hệ thống.

Cấu trúc mỗi dòng:

name:password:UID:GID:User Name:home directory:shell

more /etc/passwd

root:x:0:0:Super User:/root:/bin/bash

henry:x:101:101:Thiery Henry:/home/henry:/bin/ksh

...

+ Cấp phát User ID

Hệ thống Linux thường cấu hình sẵn một số user, nhằm phục vụ cho công việc quản trị (như user administrator và guest trên Windows), các users này thường có ID < 100: root, bin, daemon, sys...

Các user khác khi được thêm vào hệ thống thường có ID > 100.

+useradd

Lệnh useradd dùng để thêm một user vào hệ thống. Công cụ sẽ tự động thêm các dòng tương ứng vào file /etc/passwd và /etc/shadow

Các thông số thường dùng của lệnh useradd:

-u UID user ID (default: next available number)

-g GID default (primary) group (mặc định tạo group cùng tên với user)

-c comment Mô tả về user (default: blank)

- d directory Đường dẫn home directory (default /home/username)
- m Tự tạo home directory
- k skel_dir Thư mục chứa template mẫu (default /etc/skel)
- s shell login shell (default /bin/bash)

+Thay đổi thuộc tính của user

Chúng ta có thể thay đổi các thuộc tính của user bằng cách thay đổi nội dung file /etc/passwd, tuy nhiên để thuận tiện hơn ta có thể dùng công cụ usermod:

```
# usermod -g users -c "Henry Blake" henry
# usermod -u 321 -s /bin/ksh majorh #change id
# usermod -f 10 henry #disable tài khoản sau 10 ngày kể từ khi password hết hạn
# usermod -e 2004-12-20 majorh #expire_date
# usermod -L majorh #lock user
# usermod -U majorh #unlock user
```

Mỗi user thuộc vào một group chính (primary group), có thể thay đổi bằng lệnh

```
usermod -g
```

User có thể thuộc các group khác (secondary group), có thể điều khiển bởi lệnh:

```
usermod -G
```

```
# grep blofeldt /etc/passwd
blofeldt:x:416:400:./home/blofeldt:/bin/bash #thông tin user blofeldt
```

```
# groups blofeldt #xem primary group của user
Blofeldt mash #user thuộc 2 group
```

```
# groupadd -g 600 fleming #thêm group fleming
# usermod -G fleming blofeldt #chuyển user vào group fleming
# grep blofeldt /etc/group #tìm thông tin group fleming
fleming:x:600: blofeldt
```

+Xóa user

Khi một user không còn dùng hệ thống, ta có 2 vấn đề cần quan tâm:

Xóa tài khoản của user này, không cho người khác sử dụng account này để truy cập

Xóa các file/thư mục của user này ra khỏi hệ thống

Câu lệnh userdel có thể dùng để xóa tài khoản của user, đồng thời xóa các file trong thư mục home directory của user (/home/username)

Command format:

userdel [option] <login_name>

-r This option will remove home directory

+Lock tài khoản, xóa các file của user

Để khóa tài khoản của 1 user, ta dùng lệnh chage

```
# chage -E 1999-01-01 henry
```

Để tìm và xóa tất cả các file/thư mục của user nằm ngoài home directory:

```
# find / -user henry -type f -exec rm -f {} \;
```

```
# find / -user henry -type d -exec rmdir {} \;
```

Thay đổi password

Để thay đổi password của user ta dùng câu lệnh passwd

```
# passwd henry
```

current password :

new password:

retype new password:

Lời khuyên khi chọn password:

Not use proper words or names

Use letters and digits

Include symbols: !, @, #, \$, %, ...

Không cho phép các tài khoản “guest” login vào hệ thống

Mật khẩu của user sẽ được băm (hash) và lưu trong file này.

name:password:lastchange:min:max:warn:inactive:expire:flag

Với

:name User login name, mapped to /etc/passwd
password Encrypted password. If this field is blank, then there is no password ; “*”,”!” : account is locked, ...
lastchange Number of days since the last password change, from 1/1/70
min Minimum number of days between password changes
max Maximum number of days password is valid
warn Number of days before expiration that user will be warned
inactive Number of inactivity days allowed for this user
expire Absolute date, beyond which the account will be disabled

Bảo mật tài khoản

Một số việc có thể làm để tăng độ an toàn:
Đặt ngày hết hạn cho những tài khoản tạm thời

```
# usermod -e 2003-12-20 henry
```

Khóa những tài khoản lâu không dùng đến:

```
# usermod -f 5 henry
```

Change passwords known by someone who leaves. If they know the root password, change ALL password

Thay đổi thời hạn password với chage :

```
chage [options] <user>
```

Options:

-m <mindays> Minimum days

-M <maxdays> Maximum days

-d <lastdays> Day last changed

-I <inactive> Inactive lock, sau khi mật khẩu hết hạn bao lâu sẽ lock tài khoản.

-E <expiredate> Expiration (YYYY-MM-DD or MM/DD/YY)

-W <warndays> Warning days

Thêm group vào hệ thống

Câu lệnh groupadd: Thêm 1 group vào hệ thống

Cú pháp:

```
groupadd group
```

Ví dụ:

groupadd sinhvien

Sửa thông tin group

Câu lệnh groupmod:

groupmod -n newname -g gid groupname

Mỗi group chiếm 1 dòng trong file /etc/group

root:x:0:root

pppusers:x:230:jdean,jdoe

finance:x:300:jdean,jdoe,bsmith

jdean:x:500:

jdoe:x:501:

bsmith:x:502

Mỗi trường cách nhau dấu “:”, trường đầu là tên group, trường thứ 3 là group ID, trường cuối là các user trong group, mỗi user cách nhau bằng dấu “,”.

Xóa một group

Câu lệnh:

groupdel groupname

3. Quản lý WEB

a. Khái niệm

- Windows : Web là hệ thống các tài liệu dạng siêu văn bản liên kết với nhau (trang web) mà người dùng có thể xem được nhờ trình duyệt. Các tài liệu Web được soạn thảo nhờ vào ngôn ngữ đánh dấu HTML. Các trang web truyền thống là trang web tĩnh. Các trang web được lưu trong máy chủ web và dùng cổng số 80 để người dùng truy nhập vào.

- Linux : Máy chủ Web là phần mềm chịu trách nhiệm nhận các truy vấn dưới chuẩn giao thức truyền siêu văn bản từ máy khách, sau đó gửi trả kết quả xử lý thường dưới dạng các tài liệu theo chuẩn HTML.

b. Cài đặt

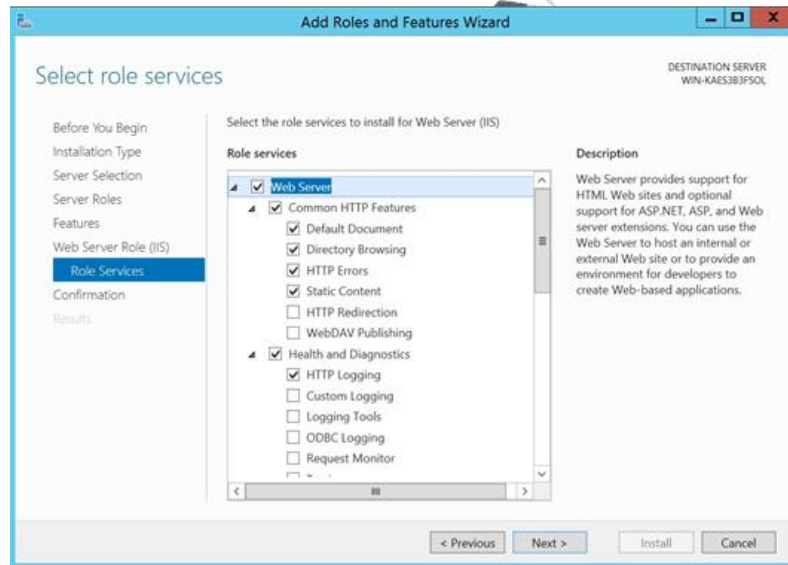
❖ Giống nhau:

- Cả hai môi trường đều sử dụng cổng 80 để cài đặt dịch vụ và cho

người dùng truy cập.

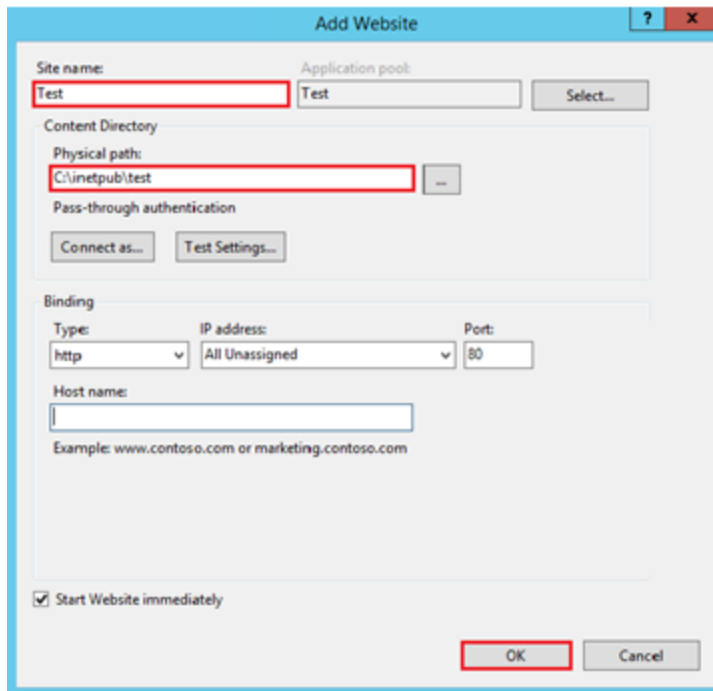
❖ Khác nhau:

- Windows : dịch vụ Web được cung cấp thông qua dịch vụ thông tin Internet IIS (Internet Information Services). Việc cài đặt máy chủ IIS đơn giản thông qua tiện ích thêm chức năng của máy chủ từ chương trình “Server Manager”



Cài đặt máy chủ IIS.

Toàn bộ công việc quản trị các trang web đều được thực hiện dễ dàng và thuận tiện qua giao diện đồ họa của tiện ích quản lý IIS. Để tạo trang chủ Web, người quản trị chỉ cần lựa chọn tính năng “Add Website” và các tham số cấu hình được hiển thị như trong hình sau.



Tham số quan trọng đầu tiên là nơi lưu trữ các file dữ liệu cho trang chủ trong mục “*Physical path*”. Tham số “*Application pool*” xác định các ứng dụng được sử dụng trong trang chủ Web. Người quản trị có thể gán trang chủ web cho các địa mạng và cổng khác nhau tùy theo cách bố trí của cơ quan và tổ chức.

Sau khi tạo trang chủ web thành công, người quản trị có thể bổ sung thêm nội dung bằng cách sử dụng thư mục ảo (*Virtual Directory*) để gắn vào đường dẫn trang web các file dữ liệu nằm trong một thư mục khác trong ổ cứng.

- Linux:

Cài đặt dịch vụ máy chủ Web Apache, là máy chủ Web sử dụng mã nguồn mở. Khi khởi động Apache sử dụng quyền cao nhất (root) để đăng ký hoạt động ở cổng 80 (ngành định cho web). Sau khi kết thúc quá trình này, máy chủ Apache hoạt động như người dùng bình thường. Việc này giúp giảm thiểu rủi ro khi bị chèn mã độc vào trang Web.

Việc cài đặt máy chủ Apache có thể được thực hiện thông qua chương trình quản lý phần mềm: `sudo apt-get install apache2`. Các mô-đun cơ bản đi kèm theo cài đặt có:

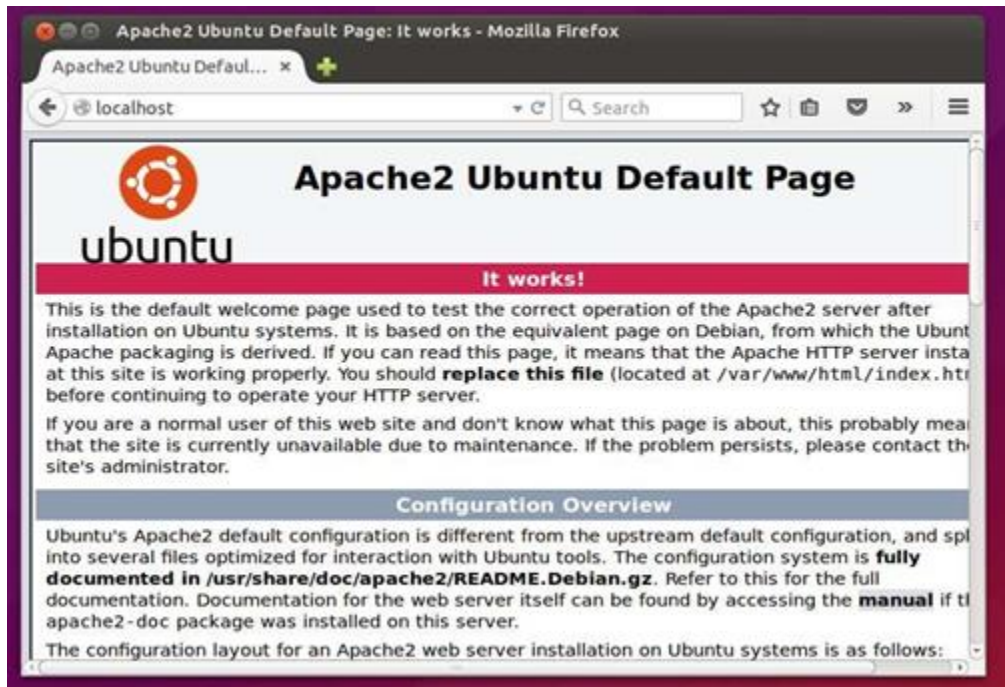
`mod_cgi`: hỗ trợ Common Gateway Interface

mode_perl: tích hợp trình thông dịch Perl

mod_aspdotnet: cung cấp giao tiếp ASP.NET

mod_ftp: hỗ trợ giao thức truyền file

Người quản trị có thể kiểm tra kết quả của quá trình cài đặt bằng cách truy nhập vào địa chỉ cục bộ qua trình duyệt như trong hình dưới đây:



Máy chủ Apache hoạt động trên địa chỉ cục bộ.

Việc cấu hình máy chủ Apache được thực hiện thông qua các file và thư mục như sau:

- *apache2.conf*: file lưu thông tin cài đặt chung cho apache
- *sites-available*: Thư mục chứa file cấu hình cho máy chủ ảo
- *mods-available*: thư mục chứa các file cấu hình để nạp và cấu hình các mô-đun
- */etc/apache2/mods-available/mime.conf*: cấu hình các dạng file
- */etc/apache2/sites-available/000-default.conf* chứa thông tin cấu hình cho web ngầm định

- Để tạo địa chỉ Web mới sử dụng cấu hình ngầm định, người quản trị tiến hành cấu hình ngầm định sang địa chỉ web mới qua câu lệnh

```
sudo cp /etc/apache2/sites-available/000-  
default.conf /etc/apache2/sites-  
available/mynewsite.conf
```

c. Quản trị

❖ Giống nhau:

- Hai môi trường đều cho phép quản trị viên kiểm soát truy cập tới trang web và thay đổi cài đặt, kiểm soát tài nguyên.

❖ Khác nhau :

- Windows: Để kiểm soát việc truy nhập tới các trang chủ Web, người quản trị có thể đặt hạn chế về địa chỉ mạng thông qua chức năng thiết lập luật hạn chế (*Add Allow Restriction Rule*) của máy chủ IIS, thiết lập các cơ chế xác thực để xác định người dùng được phép truy nhập vào trang web. Có một số cách thức như sau:
 - Nặc danh (*Anonymous*):
 - Xác thực cơ bản (*Basic Authentication*)
 - Xác thực số (*Digest Authentication*)
 - Xác thực Windows (*Windows Authentication*)
- Linux: Người quản trị sử dụng các bản ghi và các file cấu hình, nhật ký các cấp cảnh báo của máy chủ web trong đó có các file cấu hình sau :
 - *access.log*: cho biết toàn bộ các lần thử truy nhập vào máy chủ, liệt kê địa chỉ của máy khách, thời gian, yêu cầu cụ thể và thông tin về trình duyệt được sử dụng.
 - *error.log*: cho biết toàn bộ các lỗi và mức độ cảnh báo mà dịch vụ Web gặp phải khi xử lý các yêu cầu truy nhập, bao gồm các trang không tìm thấy, các thư mục bị từ chối truy nhập.

Việc ghi nhật ký có thể hạn chế theo các cấp độ cảnh báo của máy chủ Web. Điều này hữu ích cho việc kiểm soát lượng thông tin

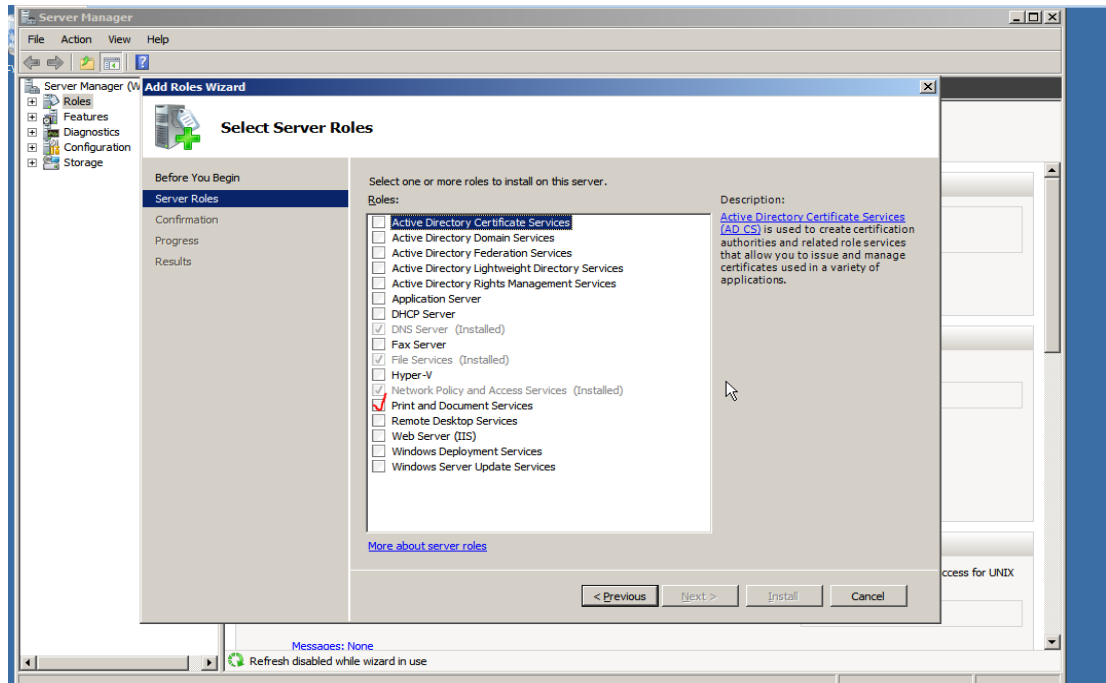
được ghi.

- *khẩn*: tình trạng khẩn cấp khiến cho dịch vụ Web không hoạt động ổn định
- *cảnh báo*: cần có hành động ứng phó tức thì có thể xác định vấn đề trong hệ thống máy chủ
- *ngghiêm trọng*: các lỗi nghiêm trọng có thể là các vấn đề về hệ thống, máy chủ, hay an toàn.
- *lỗi*: thông báo lỗi không nghiêm trọng như thiếu trang, cấu hình lỗi hay các tình huống lỗi nói chung
- *cảnh báo*: các thông điệp cảnh báo các vấn đề không nghiêm trọng cần được điều tra.
- *thông báo*: thông báo tình huống bình thường nhưng đáng quan tâm và vẫn cần phải chú ý tới.
- *thông tin*: các thông điệp giúp xác định các vấn đề tiềm tàng hay khuyến cáo cấu hình lại.
- *sửa lỗi*: các thông tin về thay đổi trạng thái của hệ thống như các file được mở, hoạt động của các máy chủ trong khi khởi động hay chạy và những thứ khác.

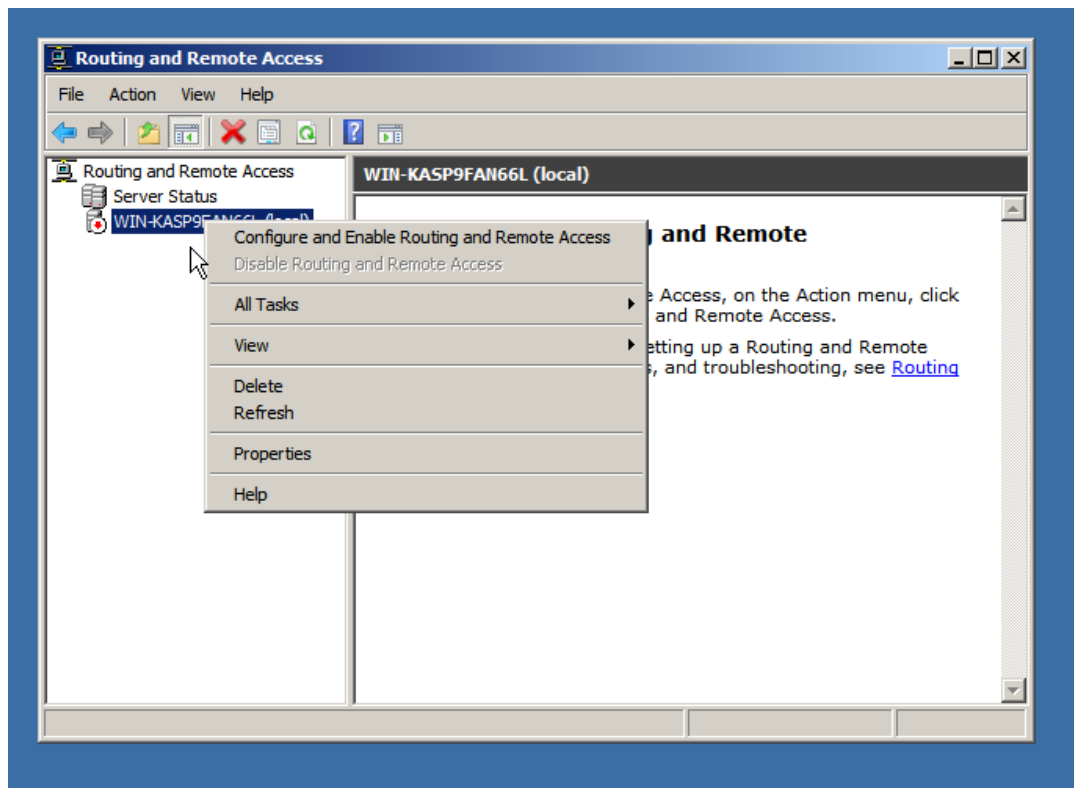
Về cơ bản không cần thiết đặt mức ghi nhật ký thấp hơn mức nghiêm trọng, việc lựa chọn các mức thấp hơn như thông báo hay sửa lỗi khi dịch vụ gặp những vấn đề về hiệu năng hay tính đáp ứng.

4. Truy nhập từ xa

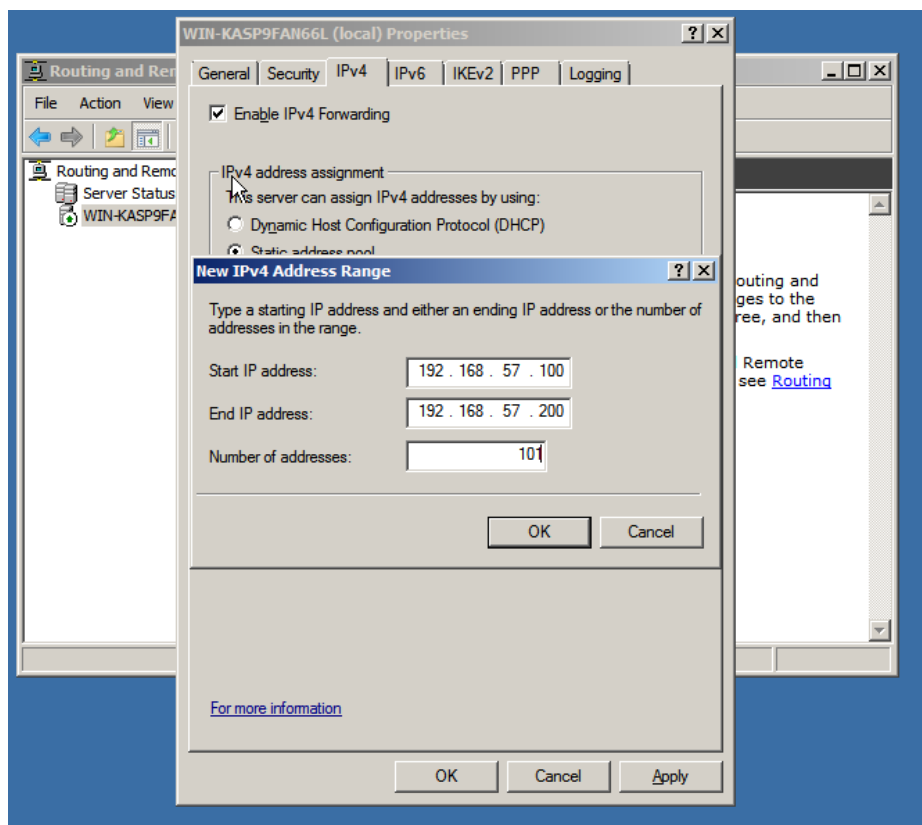
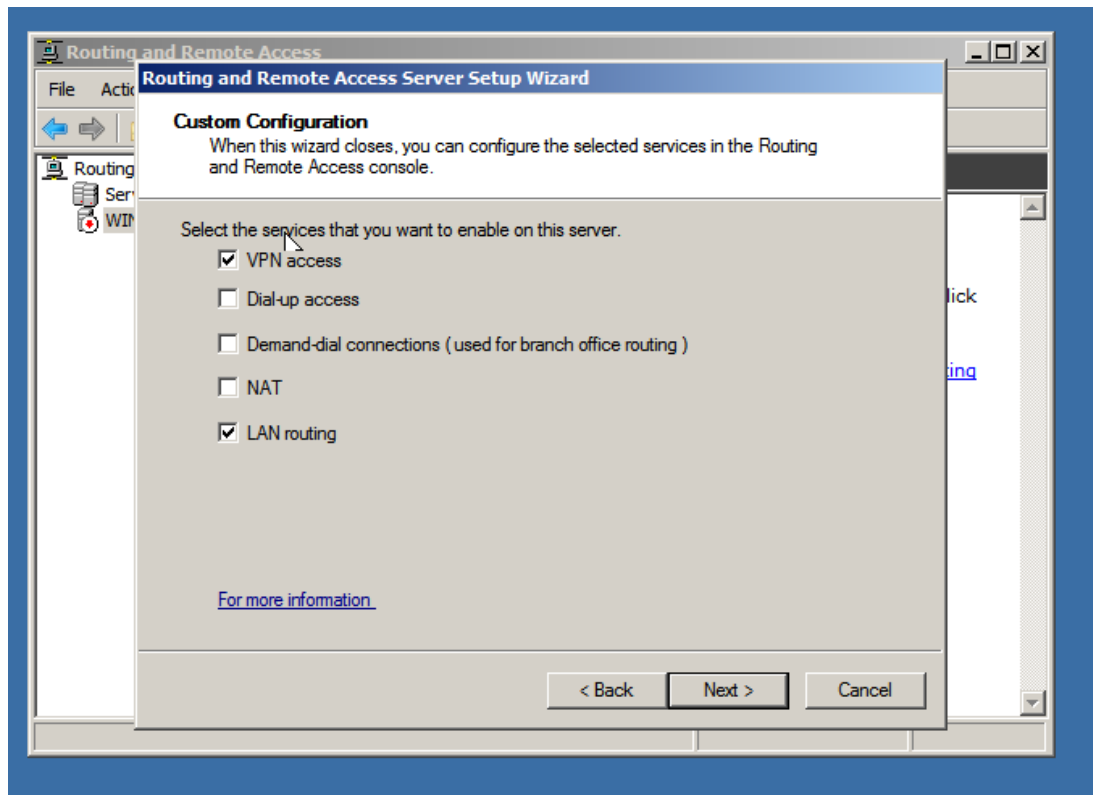
- Có thể sử dụng dịch vụ màn hình làm việc từ xa (*Remote Desktop Connections*) để kết nối với máy chủ nhưng số lượng kết nối hạn chế.
- Ở đây chúng ta sử dụng dịch vụ VPN để truy nhập từ xa. VPN cho phép thiết lập một kết nối an toàn đến máy chủ. Để thiết lập VPN ta dùng dịch vụ Routing and Remote Access Services có sẵn trên Server Manager.



- Sau khi install vào Administrative Tools chọn chức năng Routing and Remote Access ,sau đó chọn Configure and Enable Routing and Remote Access

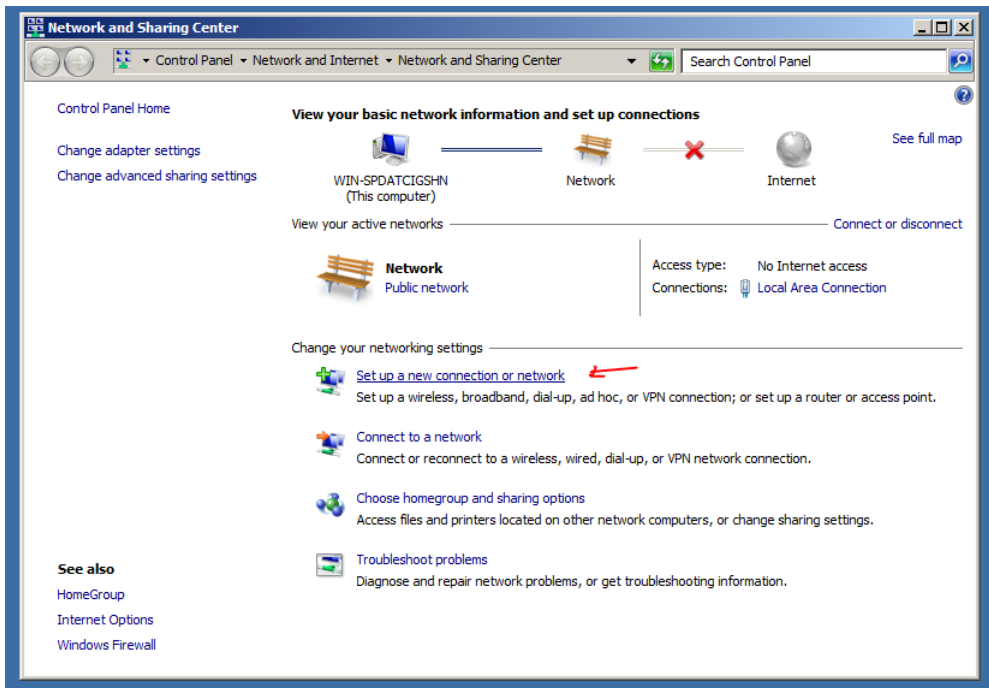


Chọn VNP access ở Custom Configuration

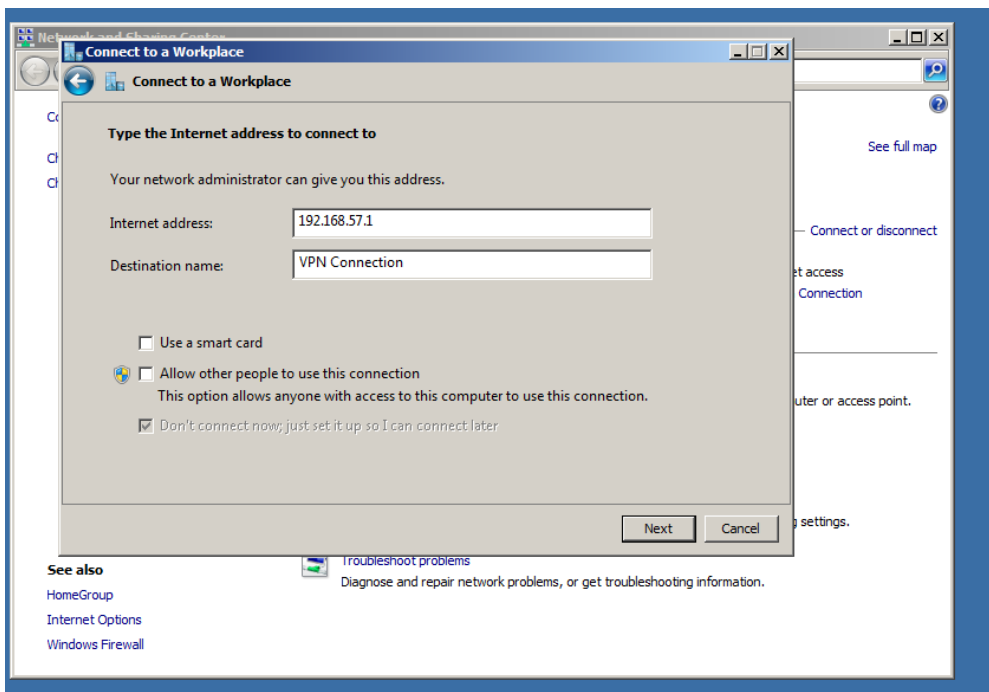


Cấp phát IP4 address range cho các máy client

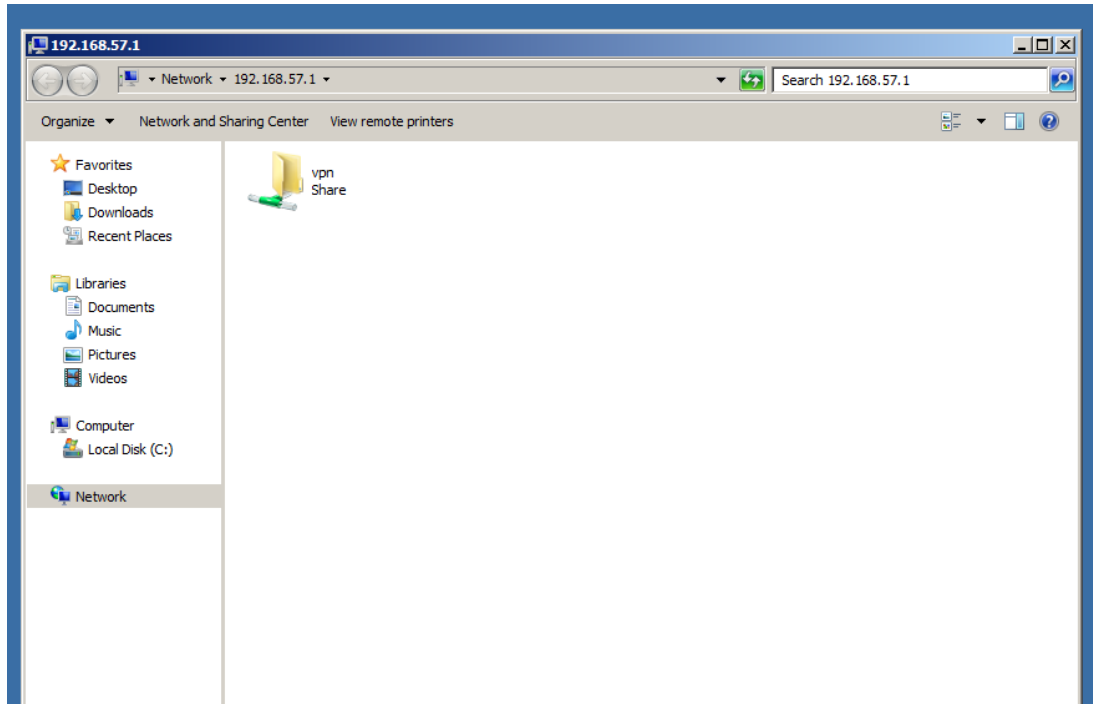
Vậy là trên Server đã thiết lập xong kết nối VPN để các thiết bị khác có thể truy cập từ xa. Chúng ta demo trên Win 7 để kết nối đến server này. Trên Win 7 vào network and sharing center chọn set up a new connection or network:



Nhập địa chỉ IP server vào:



Nhập username và password vào. Username và pass ở đây ta phải tạo trước ở Server. Khi đó ta kết nối thành công vào server



* Truy nhập từ xa trên Ubuntu Server

- Nếu như trên windows có remote desktop thì linux thông dụng hơn với chức năng telnet cho phép điều khiển từ xa qua dòng lệnh, tuy nhiên hạn chế của nó là không an toàn.
- OpenSSH là phiên bản miễn phí của dịch vụ truy nhập bảo mật SSH (*Secure Shell*) cung cấp công cụ hữu hiệu cho việc truy nhập máy chủ Linux/Unix qua mạng. SSH dựa trên cơ chế mã hóa khóa công khai để đảm bảo việc xác thực người dùng và trao đổi khóa bí mật giúp chống lại việc xâm phạm dữ liệu trao đổi trên đường truyền Internet.
- Để sử dụng SSH từ Linux, trước tiên chúng ta phải cài đặt trên máy chúng ta muốn truy cập (máy chủ). Gói này được gọi là "openssh-server" :

sudo apt-get install openssh-server

```

practicas@ALDA:~$ sudo apt-get install openssh-server
[sudo] password for practicas:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  rssh molly-guard monkeysphere
Se instalarán los siguientes paquetes NUEVOS:
  openssh-server
0 actualizados, 1 se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 0 B/319 kB de archivos.
Se utilizarán 951 kB de espacio de disco adicional después de esta operación.
Preconfigurando paquetes ...
Seleccionando el paquete openssh-server previamente no seleccionado.
(Leyendo la base de datos ... 378817 ficheros o directorios instalados actualme
te.)
Preparing to unpack .../openssh-server_1%3a6.6p1-2ubuntu2.3_amd64.deb ...
Unpacking openssh-server (1:6.6p1-2ubuntu2.3) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Configurando openssh-server (1:6.6p1-2ubuntu2.3) ...

```

- Để ngừng dịch vụ ta dùng lệnh **sudo service ssh stop**
- Bây giờ để kết nối vào Ubuntu Server chúng ta phải cài đặt SSH trên máy khách : **sudo apt-get install openssh-client**
- Để kết nối với máy từ xa, chúng ta sẽ sử dụng lệnh **ssh -l <user> <IP>**
- IP là địa chỉ máy chủ, user là tài khoản mà ta đã tạo trước.

```

santi@santi-linuxvm:~$ ssh -l santi 192.168.0.106
The authenticity of host '192.168.0.106 (192.168.0.106)' can't be established.
ECDSA key fingerprint is SHA256:Qva0fgR2vvk8C1SUKFmBvh4qF1a4YHnG1A1VqYIVwZk.
Are you sure you want to continue connecting (yes/no)?

```

Server Linux cũng bắt nhập pass như VPN Windows

```

santi@192.168.0.106's password:
Welcome to Ubuntu 15.10 (GNU/Linux 4.2.0-18-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri Nov  6 20:24:00 2015 from 192.168.0.102

```

- Done!
- Như vậy chúng ta đã cài đặt thành công Dịch vụ truy nhập từ xa sử dụng VPN trên Windows và SSH trên Linux, nếu như trên Windows giao diện đồ họa thân thiện người dùng thì trên linux đòi hỏi người quản trị phải thông thạo giao diện dòng lệnh, bù lại trên Linux quy trình thực hiện cũng nhanh hơn rất nhiều

5. Sao lưu và khôi phục

+Hệ điều hành Windows:

Ở các hệ điều hành Window thịnh hành hiện tại(Win 7,8,10) ta đều có thể sao lưu dữ liệu trong mục Back Up.

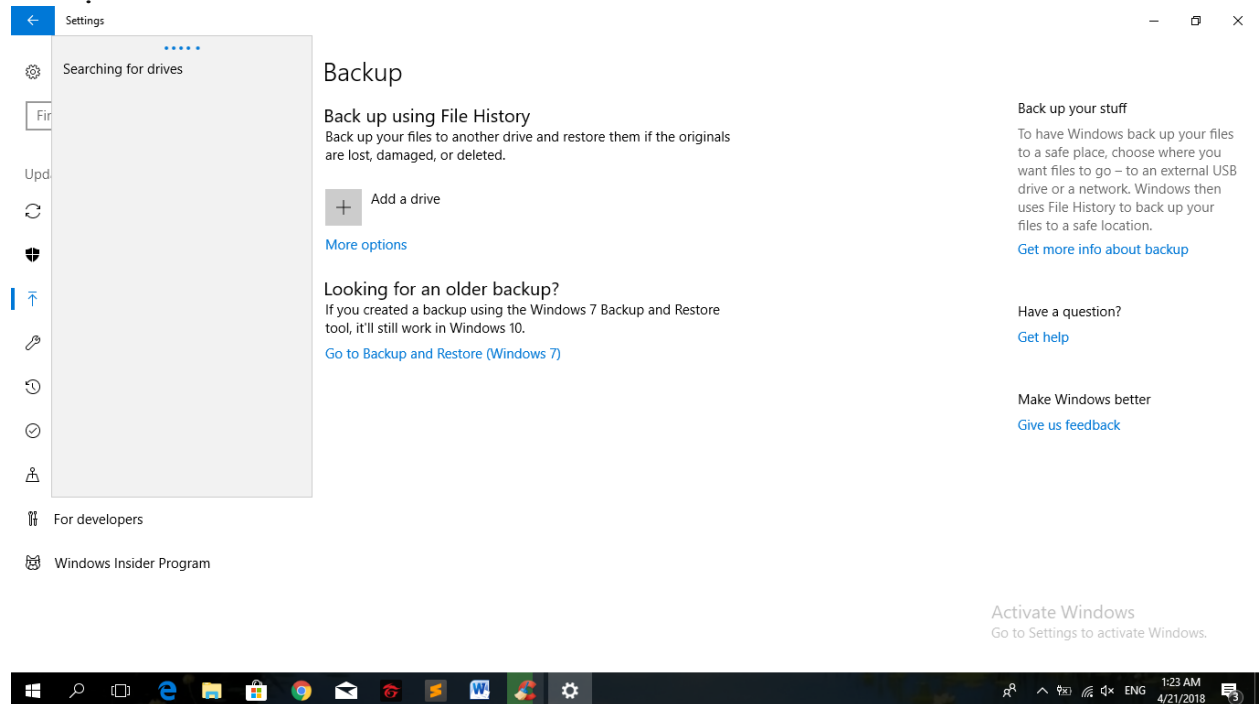
***Với Windows 10:**

1) Sao lưu với File History-dùng để sao lưu file:

Bước 1: Chọn Settings-> Update & Security -> Backup

Bước 2:Ở mục "Backup using File History", chọn Add a drive

Bước 3:Gắn ổ cứng rời hoặc ổ USB vào máy tính, rồi chọn ổ muốn lưu dữ liệu.



Chúng ta cũng có thể tùy chỉnh 1 số chức năng sao lưu trong mục More Options -> See advance settings -> Advance settings để chọn thời gian lưu trữ dữ liệu và cài đặt sao lưu tự động.

***Khôi phục lại dữ liệu:**

-Cách 1:

Chọn Settings-> Update & Security -> Backup

Chọn More options -> Restore files from a current backup.Chọn file muốn khôi phục lại.

-Cách 2:

Sử dụng File Explorer. Click chuột phải vào file cần khôi phục chọn Restore previous versions .

2) System Restore – sao lưu và khôi phục khi cài app hoặc update gặp vấn đề

Bước 1: Tìm "Create a restore point" trong thanh Search của Windows

Bước 2: Chọn Configure trong cửa sổ mới xuất hiện -> Turn on system protection. Có thể chỉnh mức dung lượng mà System Restore được phép sử dụng. Click OK.

Bước 3: Sau đó nhấn nút "Create" để tạo một điểm restore point, nhập tên cho nó.

Khi gặp vấn đề , ta có thể vào lại giao diện này, nhấn nút "System Restore" để quay trở về các điểm khôi phục đã tạo.

3) System Image Backup-sao lưu mọi thứ từ phiên bản window hiện tại:

1. Settings > Update & Security > Backup > Go to Backup & Restore
2. Nhấn vào dòng Create a system image
3. Chọn ổ đĩa để chứa file backup, có thể là HDD, DVD hay một ổ mạng.
4. Chọn phân vùng sẽ backup -> Start Backup.

***VỚI Windows 7:**

-Back up and Restore:

Bước 1: Chọn Settings -> Update & Security -> Backup -> Backup & Restore.

Bước 2: Chọn ổ cứng để sao lưu.

***Khôi phục dữ liệu:**

Có thể dùng chính chức năng Back up and Restore hoặc File Explorer tương tự Windows 10.

+Hệ điều hành Linux(Ubuntu):

-Sao lưu bằng các câu lệnh:

1) Tar

Lệnh tar (tape archive) là công cụ dùng để gom nhiều file vào một file duy nhất – file này được gọi là archive. Ngoài ra, tar cũng hỗ trợ bung các file trong archive

Cú pháp cơ bản:

tar option(s) archive_name file_name(s)

option có thể có nhiều tùy chọn:

- *-c hoặc –create : tạo lưu trữ mới
- *-x hoặc –extract : bung lưu trữ
- *-l hoặc –list : xem nội dung trong file lưu trữ
- *-W, –verify :kiểm tra lại bản backup sau khi hoàn tất
- *-r, –append :cho phép bổ sung tiếp vào một bản backup sẵn có
- *-u, –update :cập nhật một backup sẵn có, các file trùng tên sẽ bị ghi đè
- *-delete: xóa file

2)Dump

Lệnh dump thực hiện sao lưu tăng dần theo mức độ từ 0->9.Với cấp 0 là cấp cơ sở và các cấp sau sao lưu bổ sung so với cấp trước.

Cú pháp cơ bản:

dump -0uf /dev/st0 /dev/sda1

Lệnh này thực hiện việc sao lưu cơ sở ra 1 ổ đĩa khác .

Một vài tùy chọn của dump gồm có:

- *-B Số lượng các khối 1k của nơi lưu backup
- *-F script được thực hiện khi đổi tape

3)Restore

Lệnh Restore được dùng để bung dữ liệu từ dump backup

Ví dụ: restore -rf /dev/st0

Câu lệnh trên phục hồi tất cả các tệp vào thư mục hiện tại . Ta có các tùy chọn:

-i: Chế độ tương tác. Phần mềm cung cấp giao diện cho phép người quản trị lựa

chọn thư mục và file để khôi phục

- r: Khôi phục lại hệ thống file
- f tên_file: Đọc từ file sao lưu
- v: Hiển thị kết quả khôi phục

-Sao lưu và khôi phục bằng các phần mềm:

+Có rất nhiều phần mềm trợ giúp việc sao lưu và khôi phục dữ liệu:

1. Sbackup
2. Bacula
3. Rsync
4. Amanda
5. Arkeia Network Backup
6. Back In Time
7. Box Backup
8. Kbackup