HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI TẬP LỚN

HỆ ĐIỀU HÀNH WINDOWS – LINUX/UNIX

Giảng viên: Đinh Trường Duy

Nhóm lớp: 03

Nhóm bài tập: G1906810

Hà Nội, 10/2021

Mục lục

1.Giới thiệu nhóm:

- Gồm các thành viên:
  + Nguyễn Minh Phương (Nhóm trưởng)
  + Nguyễn Minh Hằng
  + Nguyễn Minh Nhật
  + Nguyễn Mậu Cường
  + Phạm Quốc Việt

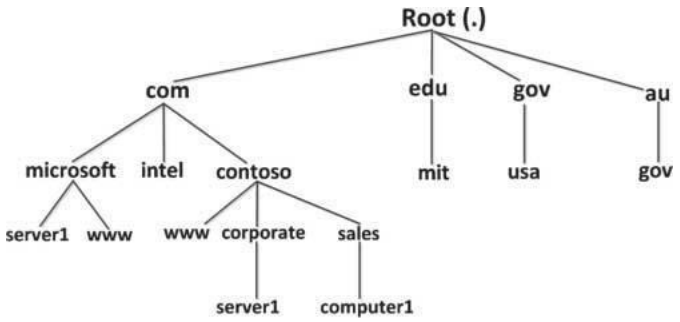
2.Dịch vụ DHCP/DNS:

a. Dịch vụ DNS

DNS là gì

- là dịch vụ thiết yếu trong mạng Internet.
- Máy tính sử dụng dịch vụ DNS để xác định vị trí vật lý (địa chỉ mạng) của máy tính chứa nội dung trang web mà người dùng muốn truy nhập đến.
- DNS tạo ánh xạ từ địa chỉ Internet ra tên miền đầy đủ và ngược lại.
- Người dùng chỉ cần nhớ tên của máy tính hay tài nguyên mạng thay vì các con số của địa chỉ mạng.
- Địa chỉ mạng có thể thay đổi trong khi tên các máy vẫn giữ nguyên.

Cấu trúc DNS



Miền gốc nằm trên đỉnh của cây tên miền

Tên miền gốc .com, .edu, .vn

Tên miền mức 2: microsoft.com

Cài đặt DNS trên Windows và Linux

Linux/Unix

Ubuntu cung cấp dịch vụ DNS qua gói phần mềm BIND.

Để cài đặt máy chủ tên miền chính cho tên miền, người quản trị cần sửa đổi file cấu hình */etc/bind/etc/bind/named.conf.local*

Để tạo cơ sở dữ liệu cho dịch vụ tra cứu địa chỉ/tên miền hay còn gọi là dịch vụ tra cứu

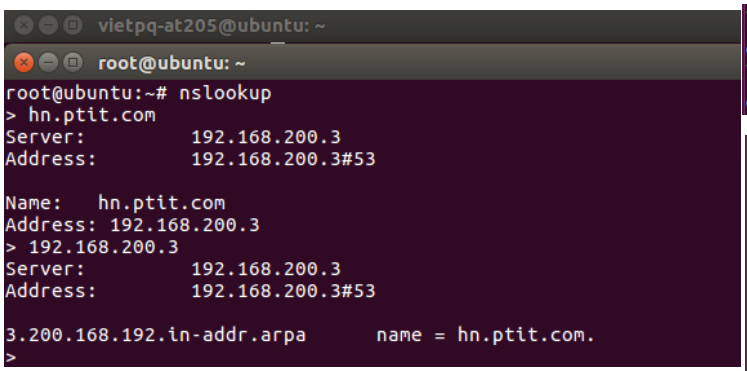
tên miền ngược, người quản trị cần sửa đổi file cấu hình "*/etc/bind/named.conf.local*". Ví dụ:

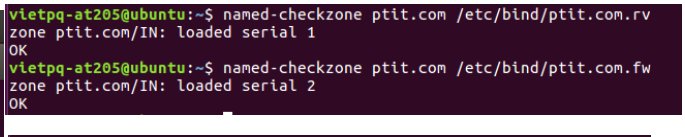
```
zone "200.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/ptit.com.rv";
};
```

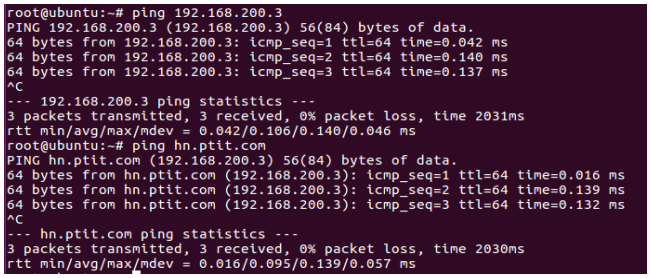
Sau đó, dùng trình soạn thảo văn bản tạo nội dung dữ liệu cho fille */etc/bind/ptit.com.rv*

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

Kiểm tra:

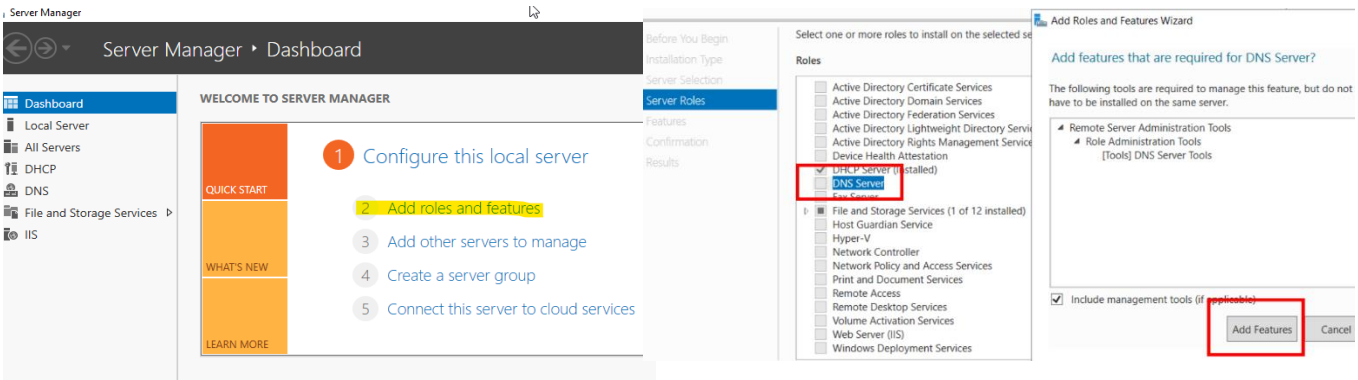






Window

Việc cài đặt máy chủ DNS khá dễ dàng qua tiện ích "*Server Manager*".

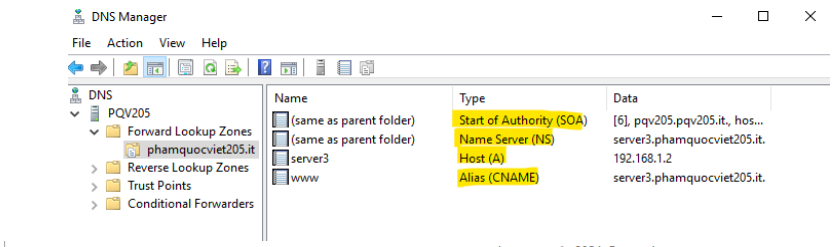


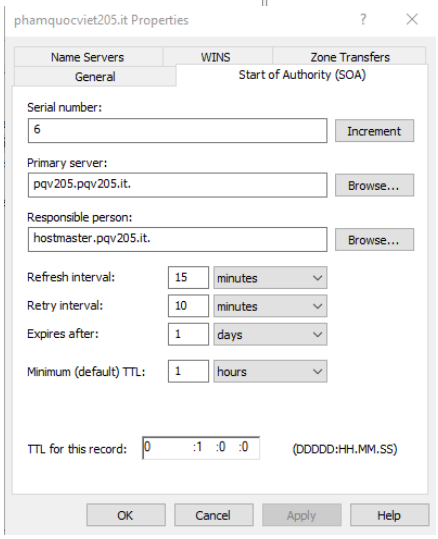
Máy chủ DNS có thể quản lý

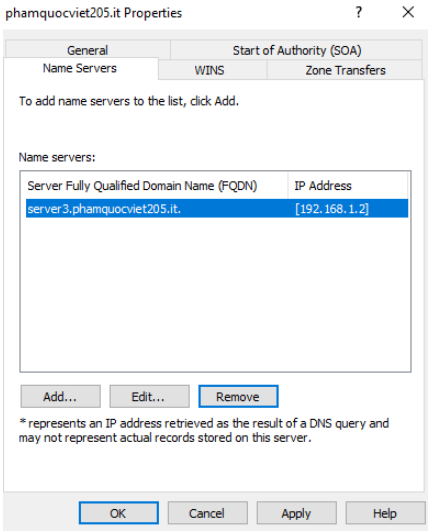
- Miền chính (*primary zone*) chính cho phép cập nhật các bản ghi về tên miền.
- Miền thứ cấp (*secondary zone*) không cho phép sửa đổi các bản ghi tên miền mà chỉ lưu bản sao của miền chính.

Khi đặt cấu hình cho máy chủ DNS có hai kiểu vùng khác nhau:

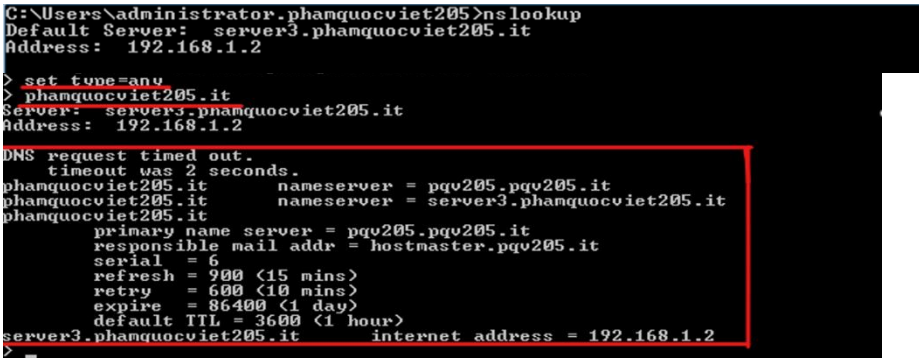
- Vùng tìm kiếm thuận (*Forward Lookup Zone*): cho phép máy tính truy vấn địa chỉ Internet ứng với một tên
- Vùng tìm kiếm nghịch (*Reverse Lookup Zone*): là việc ngược lại trả lại tên miền ứng với địa chỉ Internet







Kết quả



b. Dịch vụ DHCP

DHCP là gì

- Là dịch vụ mạng cho phép gán cấu hình mạng tự động cho các máy tính trong mạng.
- Duy trì danh sách các địa chỉ Internet, cho thuê địa chỉ.
- Giúp cài đặt các tham số khác một cách tự động cho các máy tính trong mạng như địa chỉ máy chủ DNS, cổng kết nối ra bên ngoài.

Thông tin cấu hình có:

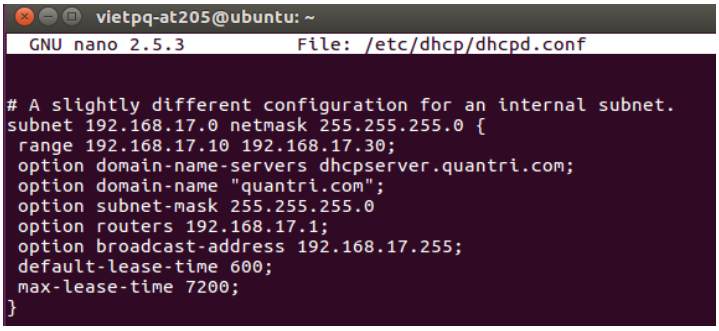
- Địa chỉ Internet và mạng con
- Địa chỉ Internet của máy cổng
- Địa chỉ Internet của máy chủ tên miền

Cài đặt và quản trị trên Windons và Linux

Linux/Unix

Câu lệnh 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*.

Thông tin về địa chỉ cấp cho các máy tính trong mạng được mô tả trong file */etc/dhcp/dhcpd.conf*



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 kiểm tra các yêu cầu cấp phát được bằng cách kiểm tra:

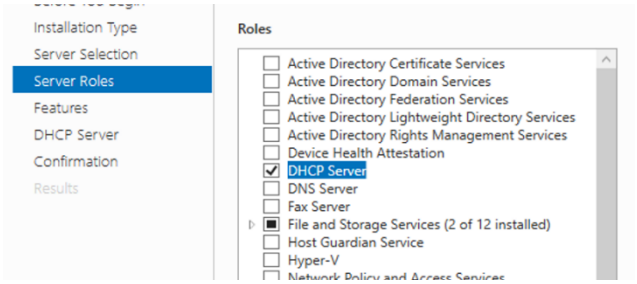
- Nội dung file nhật ký */var/lib/dhcpd.leases*
- Trạng thái của dịch vụ *service isc-dhcp-server status*

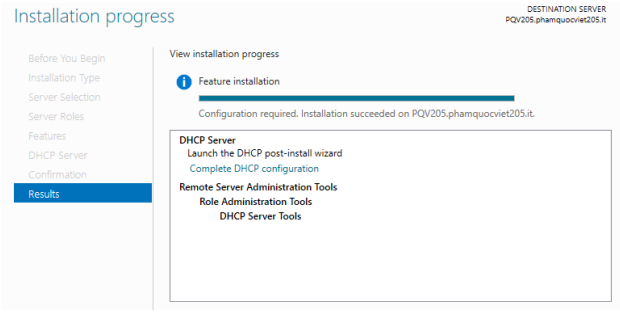
Window

Tham số quan trọng cần xác định là

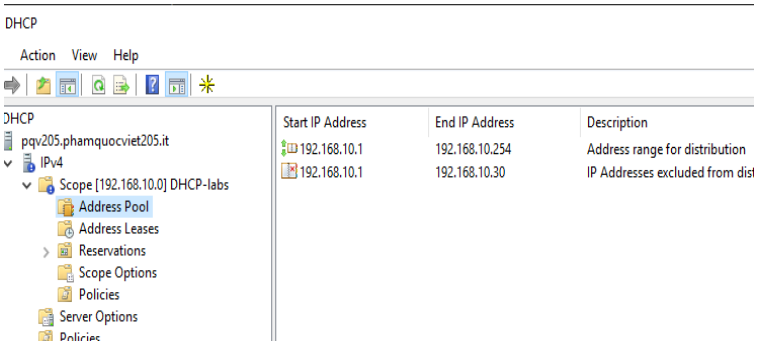
- Dải địa chỉ mà máy chủ DHCP quản lý.
- Các nhóm địa chỉ dành riêng không dùng để cấp phát cho các máy tính trong mạng.
- Nhóm địa chỉ có thể phục vụ mục đích riêng như gán cố định cho các dịch vụ của mạng.
- Không gian địa chỉ còn lại dùng để cấp phát cho các máy trong mạng.

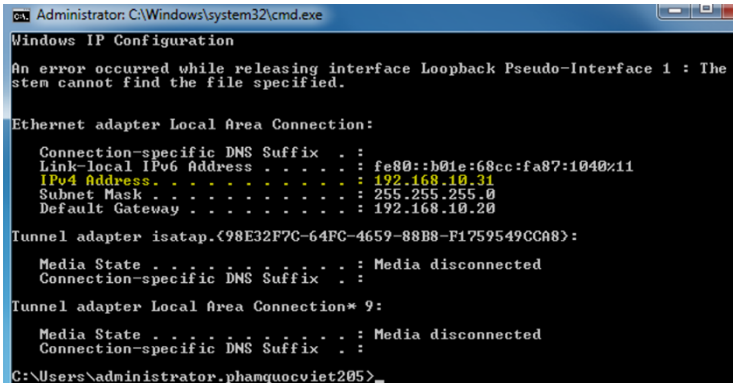
Việc cài đặt dịch vụ DHCP khá dễ dàng thông qua giao diện của tiện ích "*Server Manager*"



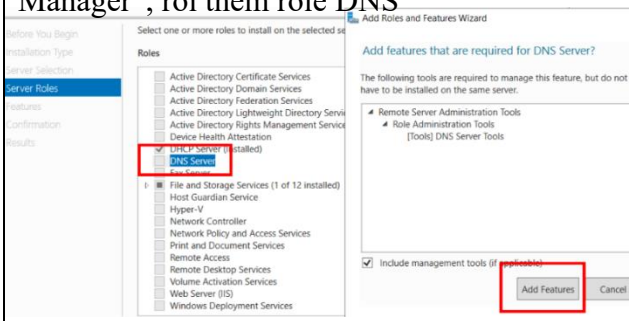
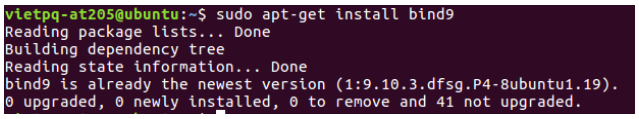
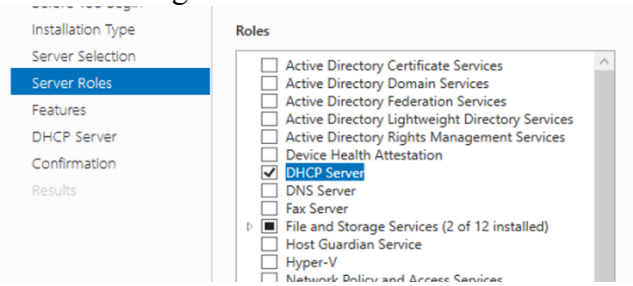
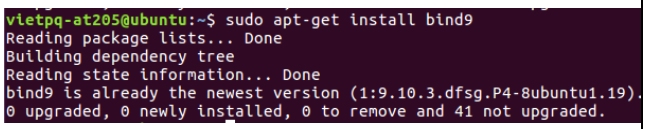


Kết quả:





So sánh

Windows Server	Linux Server (Ubuntu Server)
Cung cấp dịch vụ DNS qua tiện ích "Server Manager", rồi thêm role DNS 	Cung cấp DNS qua gói phần mềm BIND (Berkley Internet Naming Daemon). Sử dụng câu lệnh: *sudo apt-get install bind9* 
Cài đặt thông qua giao diện của tiện ích "ServerManager" 	Cài đặt phần mềm dịch vụsử dụng câu lệnh: *sudo apt-get install isc-dhcp-server* 
Các file database được lưu trong *%systemroot%/System32/dns*	Các file cấu hình dịch vụ DNS được đặt trong thư mục /etc/bind.
Database của DHCP được lưu ở đường dẫn *%systemroot%/System32/*dhcp	-Các thông tin cài đặt cho máy chủ DHCP được lưu tại /etc/default/isc-dhcp-server. -Thông tin về địa chỉ cấp cho các máy tính trong

	mạng được mô tả trong /etc/dhcp/dhcpd.conf
- Cấu hình cho dịch vụ DHCP khá thuận tiện nhờ giao diện đồ họa của phần quản trị DHCP..	-Sử dụng giao diện dòng lệnh -Thông tin về địa chỉ cấp cho các máy tính trong mạng, chỉnh sửa các thông tin mở file: /etc/dhcp/dhcpd.conf

3. Chia sẻ file và máy in:

A. Chia sẻ file trên Windows và Ubuntu

a, Tổng quan

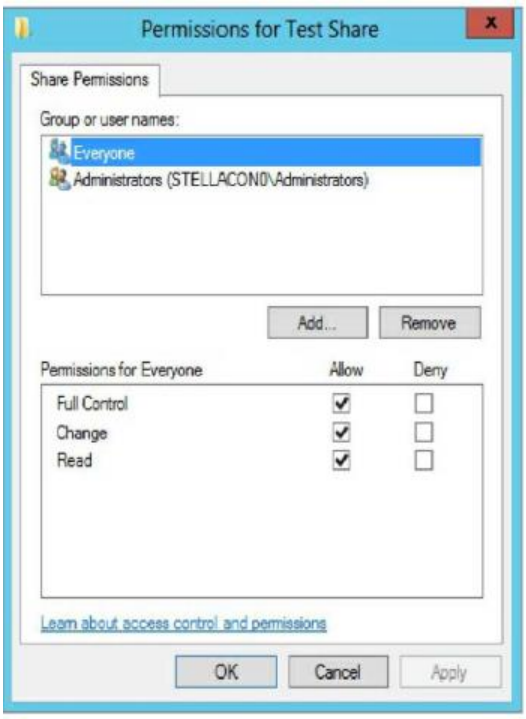
- Chia sẻ file là dịch vụ căn bản trong môi trường làm việc Windows và Ubuntu
- Dịch vụ file cho phép người dùng lưu trữ và chia sẻ dữ liệu, chương trình với người dùng khác trong mạng.
- Cung cấp công cụ làm đơn giản hóa việc chia sẻ và quản lý

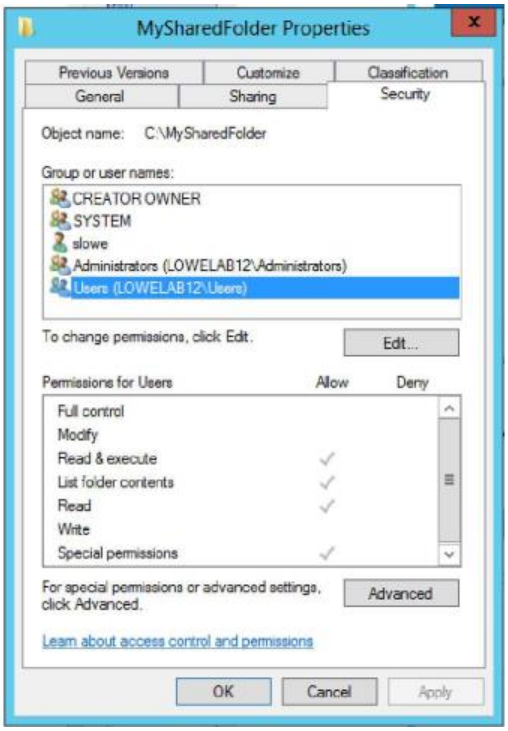
b, Cài đặt

➢ Trên Windows

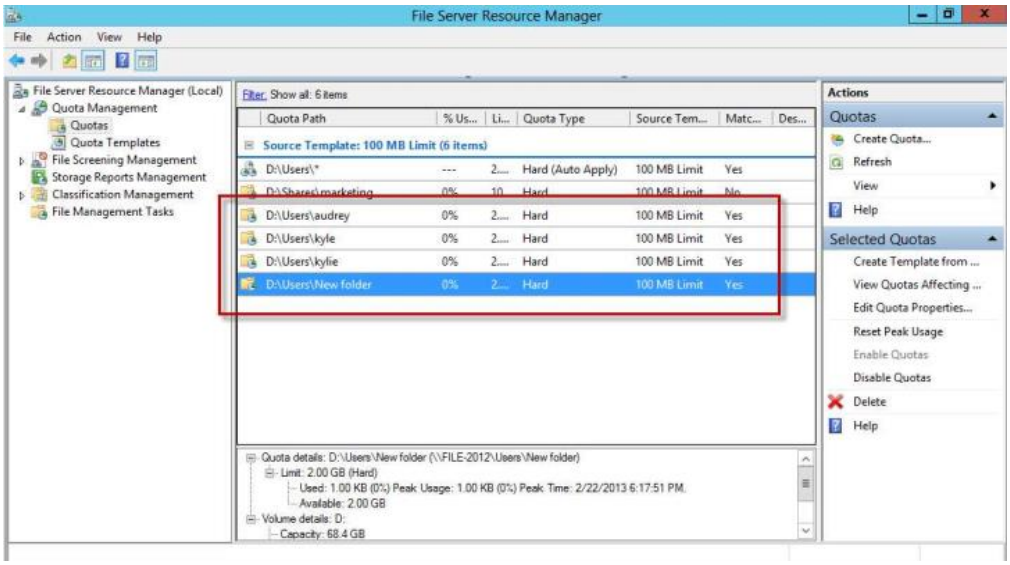
- Để chia sẻ file trên Windows người dùng phải có tài khoản phù hợp, chẳng hạn cùng một group, một domain hoặc cùng mạng LAN

-Phân quyền, kiểm soát việc truy nhập trên Windows





-Giao diện giới hạn lưu trữ



➢ Trên Ubuntu

- Cài đặt dịch vụ NFS trên Ubuntu / Server

sudo apt-get update

sudo apt-get install-kernel-server

- Cài đặt dịch vụ NFS trên Ubuntu / Client

sudo apt-get install nfs-common

- Các quyền truy nhập

- *ro*: chỉ đọc
- *rw*: đọc và ghi
- *noaccess*: không cho truy nhập và thư mục chia sẻ
- *root_squash*: Từ chối đặc quyền (root) của người dùng từ xa
- *no_root_squash*: Cho phép đặc quyền

c, So sánh

➢ Giống nhau :

- Đều hoạt động theo cơ chế chủ / khách

➢ Khác nhau :

	Windows	Ubuntu
Cấu trúc file	Thư mục	Cây dữ liệu

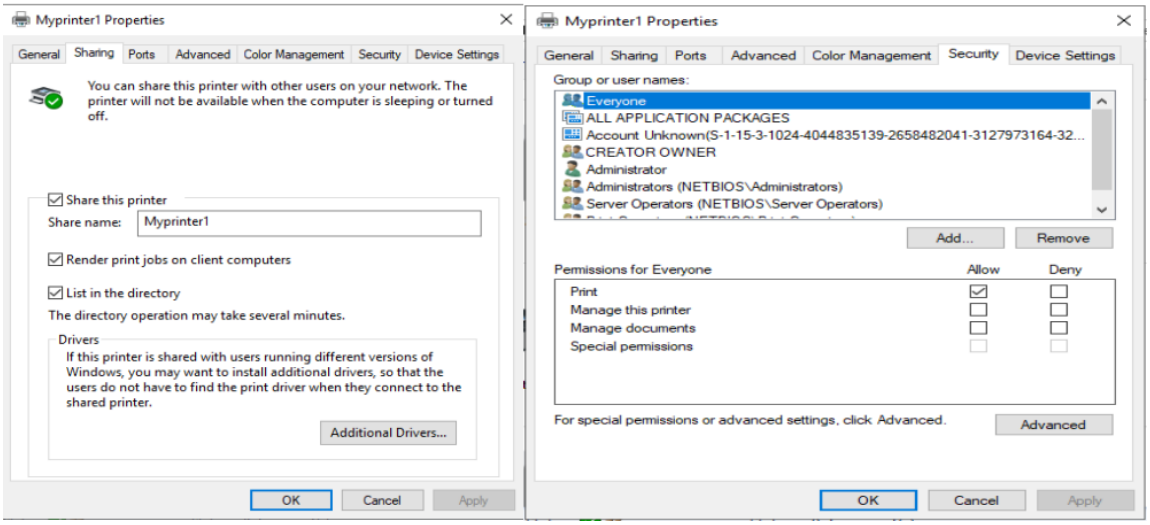
Hình thức đảm bảo an ninh	Quyền chia sẻ: read, change, full control (tuy nhiên không áp dụng cho người dùng đăng nhập cục bộ) Phân quyền NTFS để kiểm soát quyền truy nhập	Quyền chia sẻ: ro, rw, noaccess, root_squash , no_root_squash
Giao thức	SMB	FTP, Samba, NFS (phổ biến)
Cài đặt	Người dùng phải có quyền và tài khoản phù hợp (vd cùng 1 group hoặc domain)	Cài đặt các dịch vụ chia sẻ file trên máy chủ và khách
Không gian lưu trữ	Nằm trên máy khách và bị sự kiểm soát của người quản trị	Dữ liệu dùng chung được cất trên máy chủ giúp tiết kiệm không gian lưu trữ Người dùng không cần có thư mục gốc
Truy cập dữ liệu share	\\{địa chỉ IP hoặc hostname}	sudo mount máy_chủ:/thư_mục_chia_sẻ/local/thư_mục_chia_sẻ

B. Chia sẻ máy in trên win và ubuntu

- Chia sẻ file là một trong những dịch vụ quan trọng là in ấn
- Trong Windows (cụ thể là windows 10) có thể chia sẻ máy in của mình với nhiều PC trên mạng của mình.
- Khi chia sẻ máy in, đảm bảo rằng cài đặt chia sẻ được thiết lập trên máy tính chính và máy tính phụ. Ngoài ra, hãy chắc chắn rằng phải biết tên của máy tính chính.

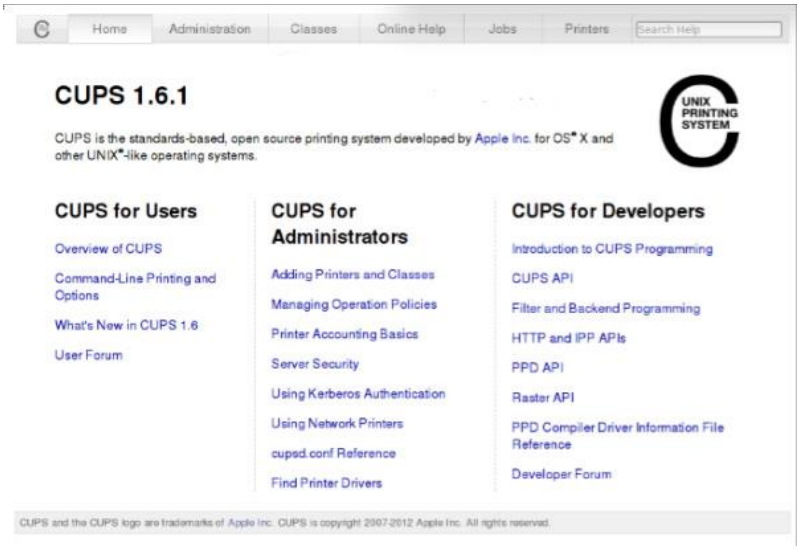
a, Cài đặt và quản trị trên Windows

- 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 Windows phân biệt.



a, Cài đặt và quản trị trên Ubuntu

- Ubuntu sử dụng dịch vụ CUPS cung cấp dịch vụ in ấn và quản lí in cho người dùng sử dụng giao thức chuẩn in ấn
- Hỗ trợ tự động phát hiện máy in mạng và cung cấp các dịch vụ quản trị và đặt cấu hình đơn giản qua Web

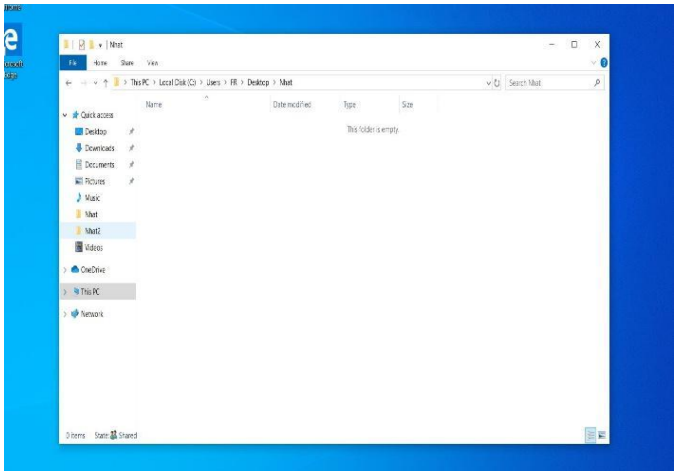


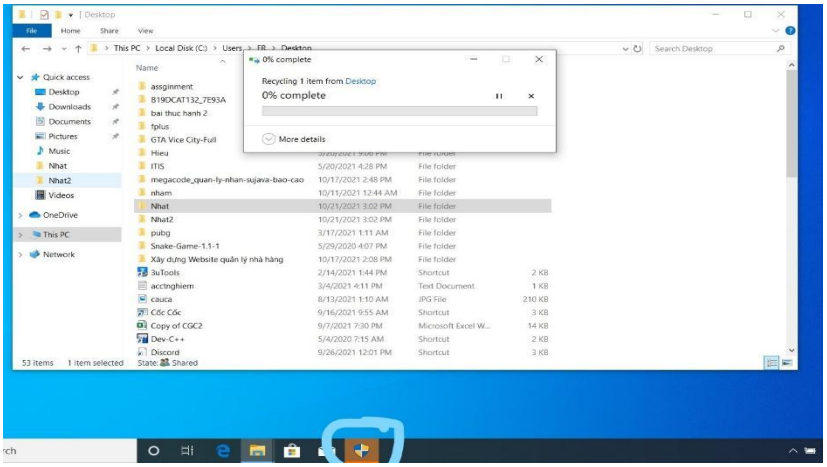
4.Quản lí người dùng và máy tính:

1. Windows

- Để sử dụng máy tính chạy HĐH Windows -> cần có tài khoản người dùng -> sử dụng khi:
  + Truy nhập vào mạng
  + Đăng nhập vào máy hoặc miền thư mục động

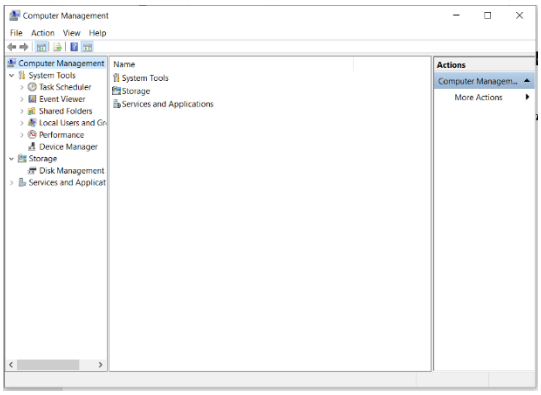
- Một số tài khoản có sẵn: Administrator, Guest,…





⇨ ***NMN1 có thể truy cập file NMN1 nhưng không thể truy cập file NMN2***

Hình ảnh về Computer Management



Linux

Quản trị người dùng

- Tài khoản người dùng: Mọi truy nhập vào hệ thống Linux đều thông qua một tài khoản người dùng (User Account).

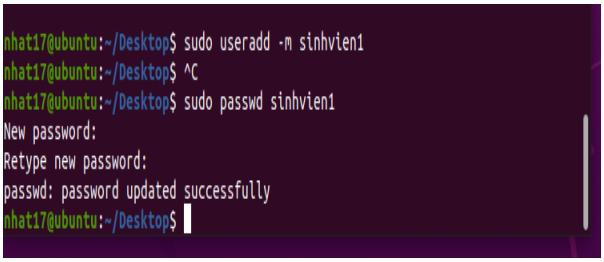
- Có thể xóa, đổi mật khẩu hay sửa thông tin người dùng và nhóm bằng các lệnh *useradd*, *userdel*, *usermod*, *groupadd*, *groupdel*, *groupmod*, *passwd* trong Linux.

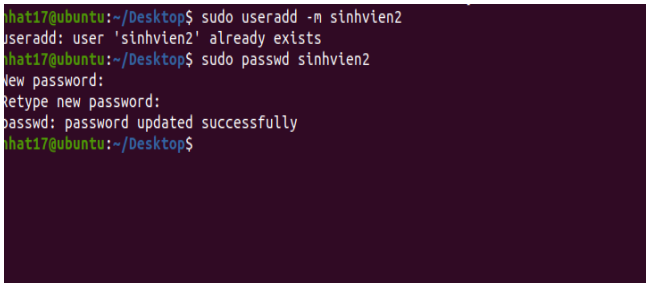
- Ta có thể phân quyền cho người dùng hành động với file/folder như read,write hay execute

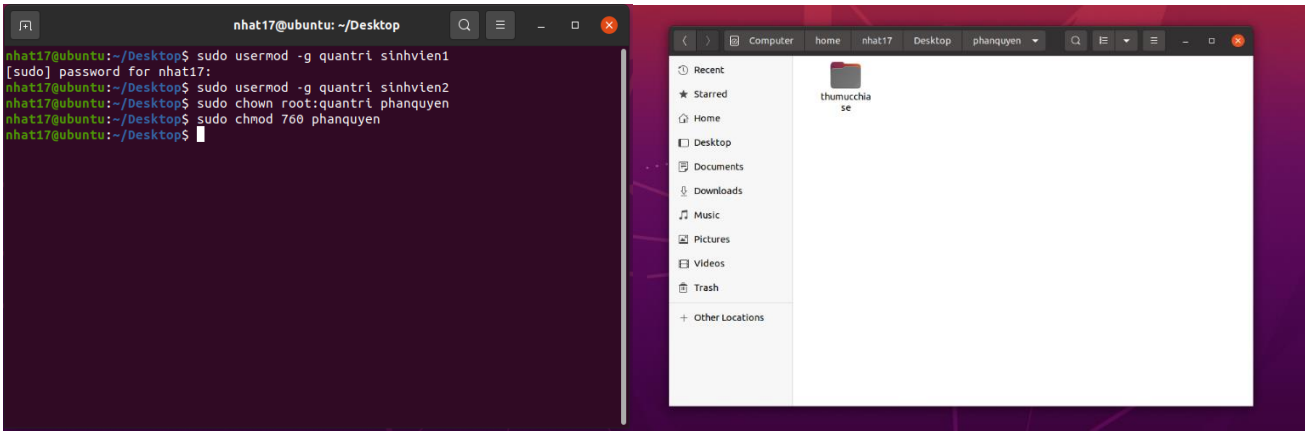
Quản trị máy tính

- Trong Linux ta có thể dùng các lệnh cơ bản đến nâng cao để kiểm tra vận hành và thông số của máy như thông tin CPU,RAM,dung lượng thư mục,thông tin file.
- Kiểm tra thời gian vận hành của hệ thống,theo dõi DiskActivity
- Kiểm tra thông tin phần cứng của hệ thống Linux..

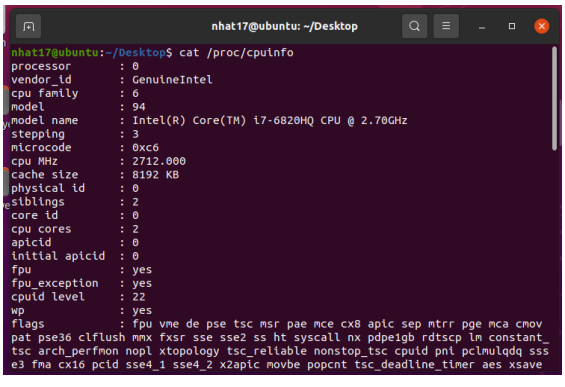
Hình ảnh về thêm người dùng và thay đổi mật khẩu

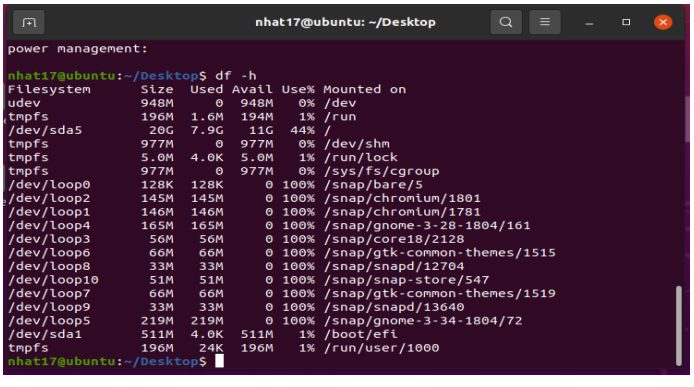






Hình ảnh về quản trị máy tính trong Ubuntu Linux





So sánh Windows và Linux

-

Windows	Linux
- Thư mục *Document* là thư mục chính mặc định. - Có các thư mục khác và các ổ đĩa như C: và D: - Người dùng quản trị viên (Administrator) có tất cả đặc quyền quản trị của máy tính. - Có 4 loại người dùng: Administrator, Standard, Child, Guest. ***Kết luận: Windows hỗ trợ giao diện đồ họa dễ dàng sử dụng. Tính bảo mật kém hơn.***	- Một thư mục mới được tạo dưới dạng */home/*. Nghĩa là user đó chỉ có thể làm việc với thư mục của mình và không có quyền truy cập vào thư mục của người dùng khác (VD: user A không thể truy cập thư mục home/B là thư mục chính của user B) - Quản lý máy tính và thư mục theo kiểu cây dữ liệu - Người dùng gốc(root) là người dùng cấp cao và có tất cả đặc quyền quản trị. - Có 3 loại người dùng: Regular, Root và Service ***Kết luận: Linux thiên về giao diện dòng lệnh để quản lí người dùng và máy tính. Có tính bảo mật cao hơn.***

5. Sao lưu và khôi phục

Sao lưu là bản sao dữ liệu đuược sử dụng để khôi phục bản gốc sau khi sảy ra sự kiện mất dữ liệu. Khôi phục là quá trình truy xuất dữ liệu không thể truy cập, bị mất, bị hỏng hoặc được định dạng về trạng thái ban đầu.

HỆ ĐIỀU HÀNH WINDOWS

Microsoft cung cấp chương trình sao lưu khôi phục “Windows Server Backup”.

❖ **Cài đặt**: có thể cài đặt *Windows Server Backup* trong Server Manager -> *Add Roles and Features Wizard* hoặc dùng câu lệnh.

Mở Windows PowerShell và gõ câu lệnh: Get-WindowsFeature -Name *Backup* để kiểm tra. Ở đây ta thấy Windows Server Backup services chưa được cài.

```
PS C:\Users\Administrator> Get-WindowsFeature -Name *Backup*

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[ ] Windows Server Backup                               Windows-Server-Backup       Available
```

Gõ câu lệnh: Install-WindowsFeature -Name Windows-Server-Backup để cài đặt.

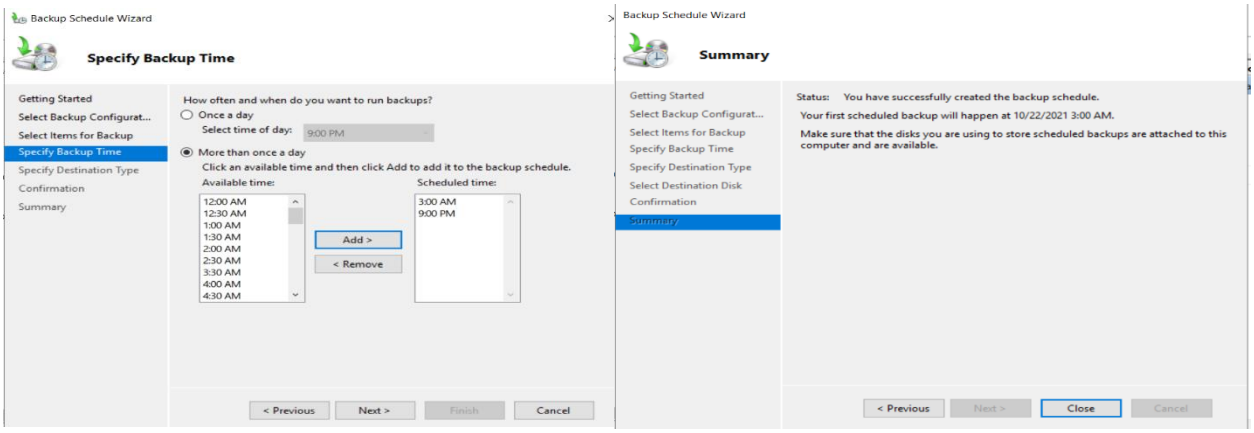
```
PS C:\Users\Administrator> Install-WindowsFeature -Name Windows-Server-Backup

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Windows Server Backup}
```

Tại Server Manager, chọn Tools -> Windows Server Backup để tiến hành cấu hình.

❖ **Backup**: Việc sao lưu có thể được tiến hành theo lịch của người quản trị.

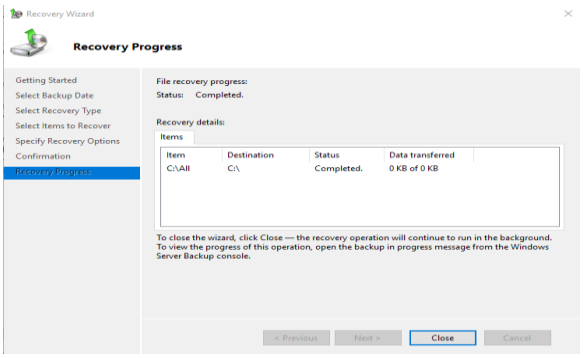
Chuột phải vào *Action* chọn *Backup Schedule* để đặt lịch sao lưu. Có thể chọn sao lưu



Once a day (một lần 1 ngày) hoặc *More than once a day* (nhiều hơn 1 lần 1 ngày).

⇨ Sao lưu hoàn tất.

❖ **Restore**: người quản trị có thể chọn việc khôi phục được thực hiện căn cứ vào dữ liệu được sao lưu: chọn *Recover…* để tiến hành khôi phục.



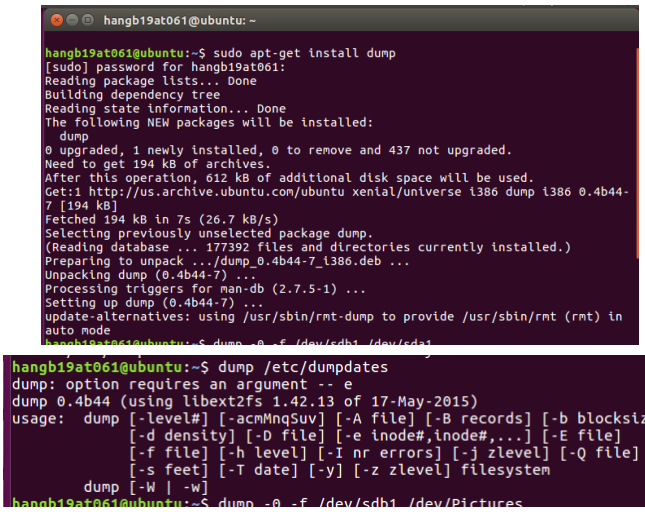
Khi tiến hành sao lưu người quản trị cần quan tâm tới một số vấn đề sau:

- Khối lượng dữ liệu
- Phần cứng và phương tiện sao lưu
- Năng lực (băng thông) mạng
- Tốc độ và khả năng khôi phục dữ liệu

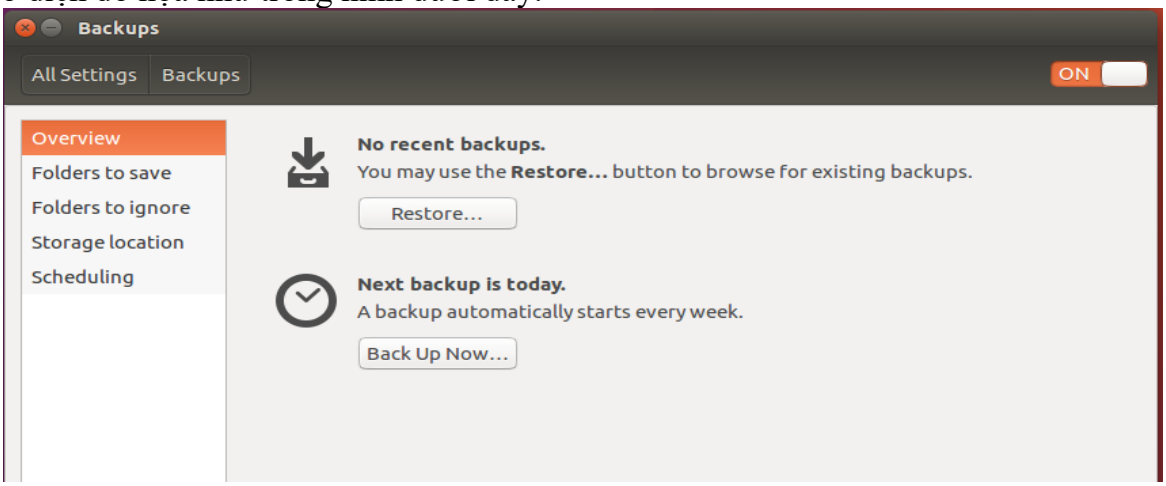
- Thông tin về các file sao lưu ghi trong file /etc/dumpdates cho biết thông tin về các file sao lưu của hệ thống. Dưới đây là câu lệnh sao lưu toàn bộ phân vùng của ổ đĩa vật lý thứ nhất vào ổ đĩa vật lý thứ hai: ***dump –0 –f /dev/sdb1 /dev/sda1***

- Khôi phục file và thư mục được thực hiện qua câu lệnh ***restore –ivf /dev/sdb1.*** Hay để khôi phục lại hệ thống file, người quản trị dùng lệnh: ***restore –rf /dev/sdb1***.

Cài đặt sao lưu:

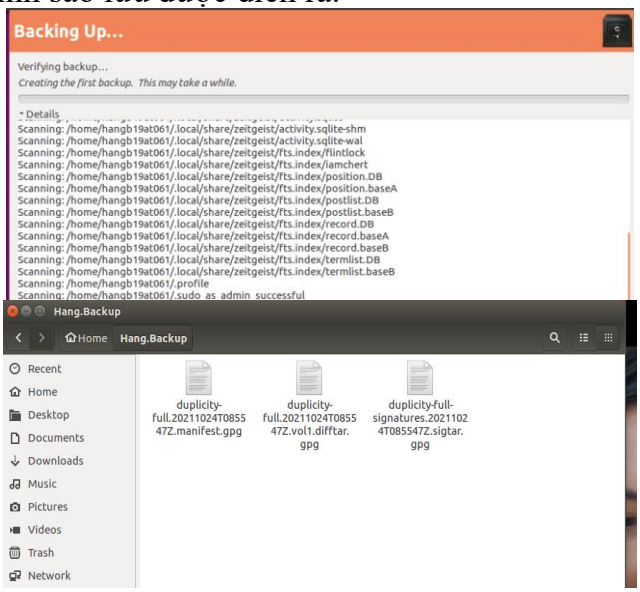


Ngoài câu lệnh, người dùng Ubuntu có thể sử dụng phần mềm sao lưu và khôi phục qua giao diện đồ họa như trong hình dưới đây.



Cài đặt Backup:

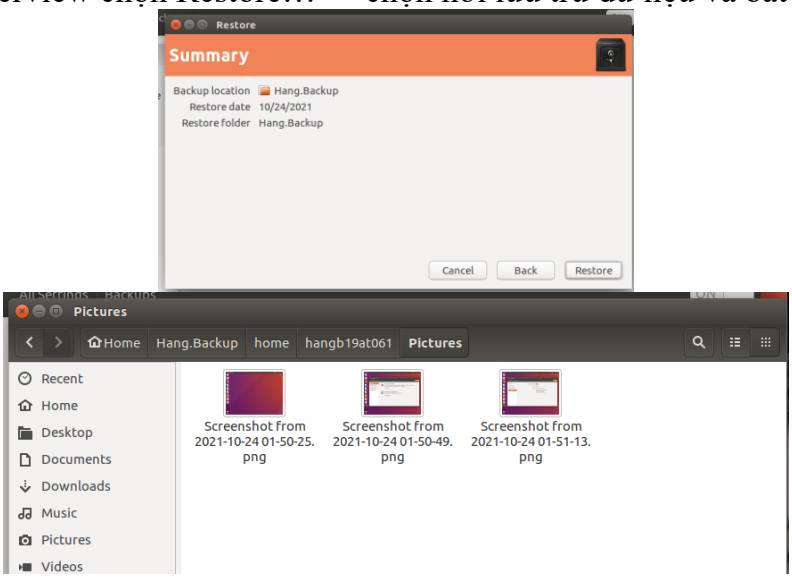
Folders to save để chọn thư mục cần sao lưu -> *Folders to ignore* để chọn các thư mục rỗng -> *Storage location* để chọn vị trí lưu bản sao lưu -> *Scheduling* lựa chọn lịch sao lưu -> *Overview*, tiến hành sao lưu bằng cách chọn *Back Up Now…* -> đặt pasword và chọn Continue, quá trình sao lưu được diễn ra.



⇨ Kết quả, bản sao lưu được lưu dưới dạng .gpg

Restore

Tại Backups Overview chọn Restore… -> chọn nơi lưu trữ dữ liệu và bắt đầu khôi phục



Khôi phục hoàn tất => kết quả các dữ liệu có thể mở được dưới dạng của nó. tiến hành tự động theo thời gian người dùng xác định.

SO SÁNH

Hệ điều hành Windows	Hệ điều hành Linux
Hướng tới đa số người dùng và các doanh nghiệp.	Dành cho số ít người có trình độ CNTT cao.
Windows server backup giới hạn phạm vi công nghệ lưu trữ có thể sử dụng. Do đó cài đặt sao lưu và khôi phục phần mềm cần phải làm việc trong giới hạn này hoặc yêu cầu mua thêm phần mềm sao lưu.	Dễ sao lưu hơn Windows. Linux đơn giản hơn nhiều, coi mọi thứ như một file-cấu hình, cơ sở dữ liệu. sử dụng các tiện ích hệ thống tích hợp sẵn.
Theo mặc định thì mã hóa Windows Server Backup không được bật.	Linux có mã nguồn mở, người dùng có thể sửa đổi nhanh chóng.
Window Server Backup quản lý các bản sao lưu trên cơ sở mỗi máy chủ. Phụ thuộc nhiều vào hệ điều hành.	Ít phụ thuộc vào hệ điều hành hơn, công việc của nó là đóng gói và nén các tập tin.

6.Giám sát hoạt động và kiểm toán:

Các công cụ giám sát và kiểm toán không chỉ giúp người quản trị được thông báo kịp thời về tình trạng chung của hệ thống mà còn có thông tin chính xác để khắc phục hay giúp cho các dịch vụ và hệ thống hoạt động được đảm bảo hơn.

a.Giám sát hoạt động:

Đối với hai hệ điều hành Windows và hệ điều hành Linux/Unix, giám sát và tinh chỉnh hiệu năng đều là quá trình theo dõi việc vận hành của hệ thống để xác lập tiêu chuẩn cơ sở, xác định và xử lý vấn đề tiềm năng.

Hệ Điều Hành Windows	**Hệ điều hành Linux/Unix**
Microsoft cung cấp một số công cụ cho người quản trị theo dõi hiệu năng và việc sử dụng tài nguyên hệ thống như giám sát hiệu năng (Performance Monitor), quản lý công việc (Task Manager), giám sát tài nguyên (Resource Monitor), và xem bản ghi sự kiện (Event Viewer).	Các file nhật ký cung cấp thông tin về tình trạng hoạt động chung của các dịch vụ và hệ thống máy chủ và được lưu trong thư mục "var/log/" như: - syslog: nhật ký về hoạt động chung của hệ thống - mail: nhật ký về hệ thống thư điện tử
Người quản trị có thể xác định được tình trạng chung của hệ thống thông qua chương trình quản lý nhiệm vụ	Linux/Unix cung cấp một số công cụ cho phép theo dõi tình trạng sử dụng các tài nguyên hệ thống của các

theo dõi thông tin. Về chức năng, chương trình cung cấp các thông tin như sau: + Mục ứng dụng + Tiến trình + Dịch vụ + Hiệu năng + Kết nối mạng + Người dùng Có hai kiểu file nhật ký sự kiện là: + Nhật ký Windows: lưu lại các sự kiện hệ thống nói chung liên quan đến ứng dụng, an ninh, cài đặt và các thành phần hệ thống; + Nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng hay dịch vụ cụ thể. Với nhật ký sự kiện, người quản trị sử dụng chương trình "Event Viewer", mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau: + Thông tin + Cảnh báo + Lỗi + Nghiêm trọng + Kiểm toán thành công + - Kiểm toán thất bại	chương trình và dịch vụ qua các câu lệnh: + ps: liệt kê các chương trình đang hoạt động và số lượng tài nguyên hệ thống chúng sử dụng + df: cho biết dung lượng lưu trữ đã được sử dụng trong hệ thống + netstat: cho biết thông tin về các cổng và các giao thức mạng đang hoạt động của hệ thống Sysstat là công cụ giám sát hiệu năng tốt cho môi trường Linux. Công cụ này cho phép ghi lại các thống kê tình trạng hệ thống tiêu biểu như: + Tải của bộ xử lý + Thao tác vào/ra và tốc độ truyền theo từng chương trình, ổ đĩa, kết nối mạng, … + Sử dụng bộ nhớ và bộ nhớ hoán đổi, Bộ nhớ ảo, lỗi trang + Sử dụng mạng, … Để cài đặt công cụ này, người quản trị cần sử dụng câu lệnh *sudo apt-get install sysstat* và *sudo dpkg-reconfigure sysstat* để cấu hình. Để lấy thông tin về các thao tác vào/ra, người quản trị có thể sử dụng câu lệnh *sar –b*.

b. Kiểm toán :

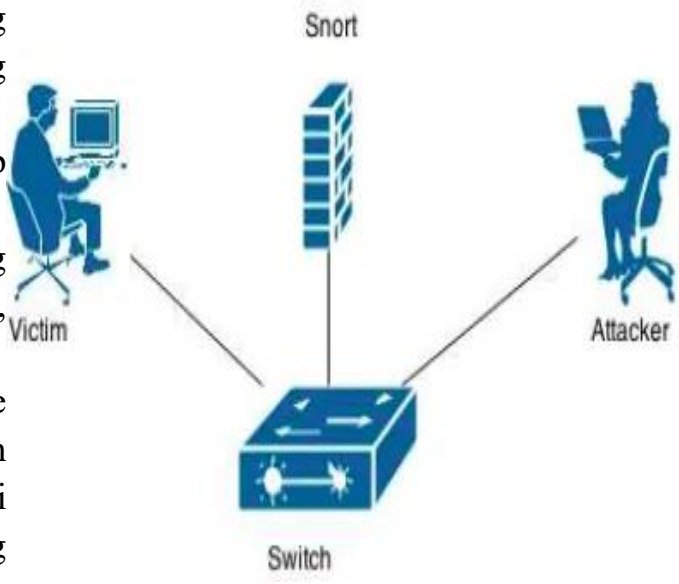
Mục tiêu cơ bản của việc kiểm toán là đảm bảo hệ thống được vận hành một cách an toàn, giảm thiểu các rủi ro, và ứng phó một cách hữu hiệu khi có trục trặc xảy ra.

Hệ Điều Hành Windows	**Hệ điều hành Linux/Unix**
Cách chính sách kiểm toán hỗ trợ việc đảm bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần để ý: + Đăng nhập + Quản lý tài khoản + Theo dõi chi tiết + Truy nhập thư mục động + - Truy nhập đối tượng	Việc kiểm toán hệ thống cho phép người quản trị thực hiện các nhiệm vụ tiêu biểu như sau: + Theo dõi truy nhập file và thay đổi + Giám sát các lời gọi và chức năng hệ thống + Phát hiện các bất thường như các tiến trình bị hỏng/ngưng. + - Các câu lệnh thực hiện bởi người dùng
Người dùng có thể sử dụng chương trình Group Policy Management Editor để giúp dễ dàng hiểu, triển khai, quản lý, khắc phục sự cố triển khai Group Policy, cũng như tự động hóa các hoạt động Group Policy thông qua tập lệnh.	Người quản trị có thể thao tác kiểm toán bằng bộ công cụ auditd được cài đặt qua câu lệnh *udo apt-get install auditd.* Một số tình huống cụ thể: - Giám sát các thay đổi trong việc truy nhập file và thư mục. + File: sử dụng câu lệnh: *sudo auditctl -w/etc/passwd -p rwxa* + Thư mục: sử dụng câu lệnh *sudo auditctl -w /var/www/html* - Giám sát các tiến trình: sử dung câu lệnh: *sudo autrace –r /bin/ls* - Báo cáo giám sát: sử dụng tiện ích *aureport*

c. Xây dựng kịch bản tấn công vào máy chủ:

Mô hình hệ thống trong mạng LAN gồm 3 thành phần chính:

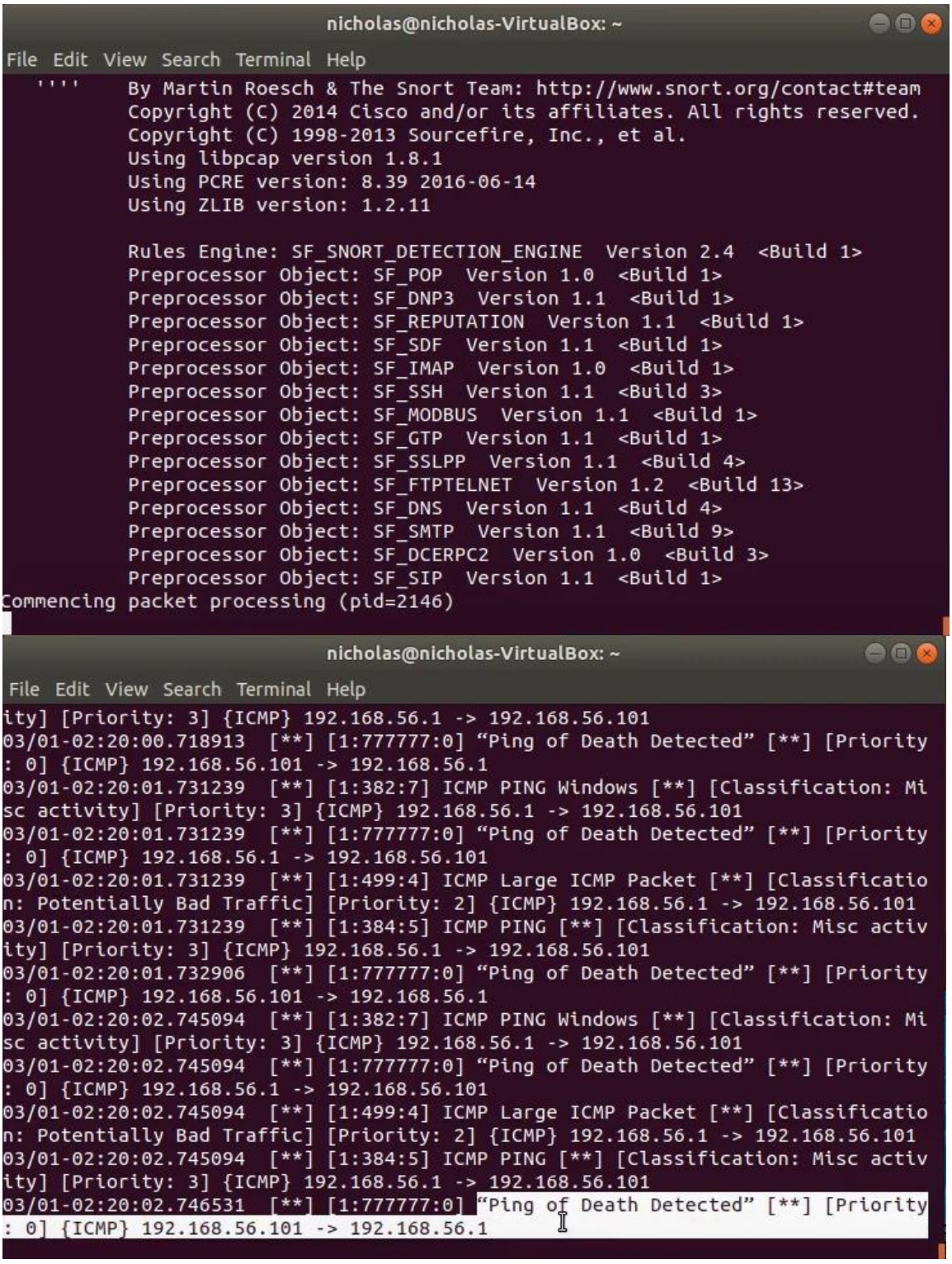
- Victim: đại diện cho người dùng hoặc máy chủ trong hệ thống mạng LAN
- Snort: thiết bị phát hiện xâm nhập chạy Snort
- Attacker: đối tượng tấn công mạng LAN, có thể là hacker, virus, trojan, worm, …
- Switch: để snort có thể lắng nghe được các cuộc tấn công, switch hoặc thiết bị chuyển mạch phải cài đặt hỗ trợ forward các gói tin trong mạng về Snort Sensor.



Kịch bản thử nghiệm phát hiện xâm nhập bằng Snort IDS:

- Bước 1: Cài đặt và cấu hình Snort IDS
    - Snort được cài đặt trên máy ảo Ubuntu, đồng thời chạy bổ sung các công cụ cho phép theo dõi và giám sát các cảnh báo từ snort gồm: Sguil, Snortby, Squert
- Bước 2: Thêm rule để thử nghiệm, ở đây ta chỉ thêm một rule đơn giản để đánh giá khả năng phát hiện của Snort:
    - Sửa file: */etc/nsm/rules/local.rule và thêm vào rule sau:*

  dert iamp any any → any any (msg: "Ping of Death Detected"; sid: 777777;)
    - Khởi động lại Snort bằng lệnh: "/etc/init.d/nsm restart"
- Bước 3: Từ máy tính attacker thực hiện lệnh ping đến máy victim: "ping 192.168.1 -t"
- Bước 4: Theo dõi cảnh báo của Snort từ Terminal


nicholas@nicholas-VirtualBox: ~
File Edit View Search Terminal Help
'''' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Commencing packet processing (pid=2146)
nicholas@nicholas-VirtualBox: ~
File Edit View Search Terminal Help
ity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:00.718913 [**] [1:777777:0] “Ping of Death Detected” [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/01-02:20:01.731239 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:01.731239 [**] [1:777777:0] “Ping of Death Detected” [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:01.731239 [**] [1:499:4] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:01.731239 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:01.732906 [**] [1:777777:0] “Ping of Death Detected” [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/01-02:20:02.745094 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:02.745094 [**] [1:777777:0] “Ping of Death Detected” [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:02.745094 [**] [1:499:4] ICMP Large ICMP Packet [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:02.745094 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/01-02:20:02.746531 [**] [1:777777:0] “Ping of Death Detected” [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix,
Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
[2] Tom Carpenter, Microsoft
Windows Server Operating System Essentials, Sybex, 2011.
[3] Wale Soyinka, Linux
Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.
Và một số tài liệu khác.

Cảm ơn thầy đã theo dõi bài báo cáo của chúng em.