

Tài liệu đọc

Hỗ Trợ Công Nghệ Thông Tin

Khóa 3: Các hệ điều hành

Phần 1: Tài liệu đọc bổ trợ

Bài đọc 1	Thao tác trên hệ điều hành Windows
	<ul style="list-style-type: none">1.1 Giao diện đồ họa người dùng1.2 Hệ thống thư mục và tập tin<ul style="list-style-type: none">- Bố trí thư mục và tập tin- Thao tác trên thư mục và tập tin1.3 Giao diện dòng lệnh Powershell<ul style="list-style-type: none">- Giới thiệu giao diện dòng lệnh- So sánh với giao diện đồ họa người dùng- Các lệnh liên quan đến tập tin và thư mục
Bài đọc 2	Thao tác trên hệ điều hành Linux
	<ul style="list-style-type: none">2.1 Giao diện đồ họa người dùng2.2 Giao diện dòng lệnh Bash<ul style="list-style-type: none">- Terminal, Shell và Bash- Bash và các lệnh liên quan đến tập tin và thư mục
Bài đọc 3	Quyền truy cập hệ thống
	<ul style="list-style-type: none">3.1 Các loại tài khoản người dùng và nhóm<ul style="list-style-type: none">- Phân loại tài khoản người dùng và nhóm- Xem và cấu hình tài khoản trên Windows và Linux3.2 Quản lý mật khẩu

	<ul style="list-style-type: none"> - Cách thức quản lý mật khẩu - Cập nhật mật khẩu - Cách đặt mật khẩu an toàn
3.3	Quản lý tài khoản người dùng
	<ul style="list-style-type: none"> - Thêm và xóa người dùng trên Windows - Thêm và xóa người dùng trên Linux
3.4	Quyền truy cập thư mục và tập tin
	<ul style="list-style-type: none"> - Giới thiệu ACL - Các quyền khác nhau trên Windows - Các quyền khác nhau trên Linux - Thay đổi các quyền truy cập - Quyền truy cập đặc biệt
Bài đọc 4	Cài đặt và quản lý phần mềm
4.1	Các gói phần mềm
	<ul style="list-style-type: none"> - Các dạng gói phần mềm trên Windows - Các dạng gói phần mềm trên Linux
4.2	Đóng gói phần mềm với công cụ nén
4.3	Phụ thuộc gói phần mềm
4.4	Quản lý gói phần mềm
4.5	Quản lý phần mềm thiết bị
4.6	Cập nhật hệ điều hành Windows và Linux
Bài đọc 5	Hệ thống tập tin
5.1	Giới thiệu các hệ thống tập tin
5.2	Ổ đĩa cứng
5.3	Bộ nhớ ảo
	<ul style="list-style-type: none"> - Bộ nhớ ảo và vai trò trong hệ thống - Kỹ thuật phân trang
5.4	Quản lý tập tin
	<ul style="list-style-type: none"> - Siêu dữ liệu của tập tin (file metadata) - Quản lý tập tin trên hệ thống NTFS - Quản lý tập tin trên hệ thống Linux
5.5	Quản lý ổ đĩa
	<ul style="list-style-type: none"> - Tỷ lệ sử dụng và dọn dẹp ổ đĩa - Chống phân mảnh ổ đĩa
5.6	Sửa chữa hệ thống tập tin
Bài đọc 6	Quản lý tiến trình

	<p>6.1 Vòng đời của tiến trình</p> <ul style="list-style-type: none"> - Tiến trình - Tạo và kết thúc tiến trình <p>6.2 Quản lý tiến trình</p> <ul style="list-style-type: none"> - Quản lý tiến trình trên Windows - Quản lý tiến trình trên Linux <p>6.3 Quản lý tài nguyên hệ thống</p> <ul style="list-style-type: none"> - Theo dõi tài nguyên hệ thống trên Windows - Theo dõi tài nguyên hệ thống trên Linux
Bài đọc 7	Quản lý tiến trình
	<p>7.1 Vòng đời của tiến trình</p> <ul style="list-style-type: none"> - Tiến trình - Tạo và kết thúc tiến trình <p>7.2 Quản lý tiến trình</p> <ul style="list-style-type: none"> - Quản lý tiến trình trên Windows - Quản lý tiến trình trên Linux <p>7.3 Quản lý tài nguyên hệ thống</p> <ul style="list-style-type: none"> - Theo dõi tài nguyên trên hệ thống Windows - Theo dõi tài nguyên trên hệ thống Linux

Phần 2: Hướng dẫn trả lời câu hỏi - Quiz

Phần 1

TÀI LIỆU ĐỌC BỔ TRỢ

Bài đọc 1: Thao Tác Trên Hệ Điều Hành Windows

1. Giao diện đồ họa người dùng

Hệ điều hành là phần mềm trung gian giữa người dùng và thiết bị phần cứng. Người dùng cần tương tác với hệ điều hành để thực hiện các công việc của mình trên máy tính. Có 2 cách để người dùng có thể tương tác hay điều khiển hệ điều hành. Một là qua giao diện đồ họa người dùng (Graphical User Interface – GUI), hai là qua giao diện dòng lệnh (Command Line Interface – CLI). Trong phần này, chúng ta tập trung vào giao diện đồ họa người dùng và để ngắn gọn, chúng ta sử dụng dạng viết tắt GUI để nói về chúng.

GUI cho phép người dùng tương tác với những hình ảnh biểu tượng (các icon) bằng chuột và bàn phím nhằm thực hiện các tác vụ xác định. GUI làm cho người mới bắt đầu sử dụng hệ điều hành thao tác dễ dàng hơn thay vì phải bỏ thời gian để học các câu lệnh điều khiển như trong giao diện dòng lệnh. Tuy nhiên, chính vì cần hiển thị đồ họa nên nó gây tiêu tốn tài nguyên máy tính như bộ xử lý và bộ nhớ để hiển thị hình ảnh.

Một điểm quan trọng khác là giao diện đồ họa có thể thay đổi về cấu trúc bố trí tùy thuộc vào phiên bản và loại hệ điều hành. Ví dụ, giao diện của Windows 10 bố trí mặc định các biểu tượng chương trình bên trái, còn Windows 11 bố trí mặc định các biểu tượng ở chính giữa. Người dùng cần thời gian để làm quen với các thay đổi này khi chuyển từ một phiên bản này sang một phiên bản khác của cùng một loại hệ điều hành.



Windows 10



Windows 11

2. Hệ thống thư mục và tập tin

Bố trí tập tin và thư mục

Tập tin máy tính là tài nguyên lưu trữ dữ liệu trong thiết bị máy tính, và được xác định thông qua tên gọi. Bản thân tài liệu chúng ta đang đọc là một tập tin trên máy tính.

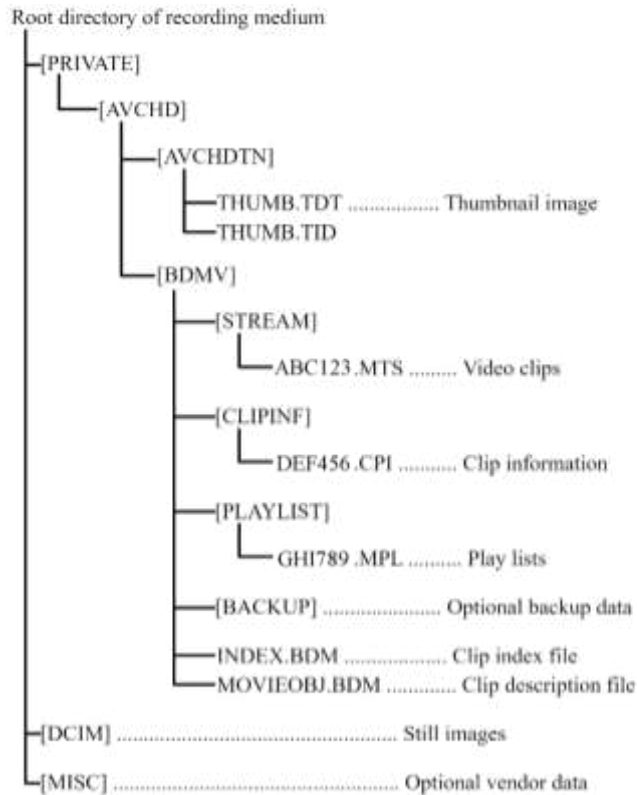
Mỗi ứng dụng có cách lưu trữ, xử lý dữ liệu khác nhau nên tạo thành các tập tin có cấu trúc khác nhau và thường thể hiện qua các đuôi tập tin khác nhau. Đuôi tập tin là phần tên mở rộng thường được viết ở cuối tên tập tin và ngăn cách bởi phần chính bởi dấu chấm. Tuy nhiên, đuôi tập tin chỉ có ý nghĩa dùng để hệ điều hành biết chương trình nào xử lý chúng khi người dùng nhấn vào. Việc thay đổi đuôi này không ảnh hưởng nhiều đến nội dung đang chứa trong đó.



Nguồn: flickr

Mặc dù đa dạng về loại tập tin nhưng có thể phân làm hai loại chính là tập tin văn bản và tập tin nhị phân. Tập tin văn bản chứa dữ liệu là các ký tự chữ cái và có thể được hiểu dễ dàng bởi một chương trình xử lý đơn giản. Mặc dù dữ liệu bên dưới ổ cứng cũng là tập hợp các số nhị phân nhưng tập tin văn bản thể hiện các nhóm bit theo mã ký tự chuẩn phổ biến như ASCII hay Unicode. Trong khi đó, tập tin nhị phân lưu trữ dữ liệu theo cách mã hóa riêng và có thể không công bố bởi bên phát triển. Việc đọc dữ liệu để diễn giải cho người dùng thường cần sử dụng chính chương trình được tạo ra bởi nhà phát triển đó. Một điểm khác biệt quan trọng giữa tập tin văn bản và tập tin nhị phân ở chỗ nếu xảy ra hư hỏng ở một chỗ nào đó của tập tin thì khả năng tập tin văn bản vẫn còn đọc được, trong khi đó tập tin nhị phân có khả năng không thể xử lý được. Trong Windows, tập tin văn bản thường có đuôi mở rộng là .txt và chương trình mặc định xử lý chúng là Notepad.

Khi tập tin nhiều lên, chúng ta cần một cách tổ chức, phân loại, bố trí để phục vụ quá trình tìm kiếm các tập tin một cách dễ dàng. Khái niệm thư mục ra đời để giải quyết vấn đề này. Thư mục (directory) là cách thức tổ chức các tập tin vào thành một nhóm. Thư mục cũng cho phép chứa các thư mục khác. Từ đó tạo thành một cấu trúc phân tầng dạng cây, được gọi là cây thư mục (directory tree). Để phân biệt thư mục này với thư mục khác, ta đặt tên cho chúng. Tuy nhiên, tên thư mục thường đơn giản hơn tên tập tin vì chúng không có tên mở rộng để phân biệt các loại cũng như mục tiêu của thư mục chỉ nhằm tổ chức các tập tin.

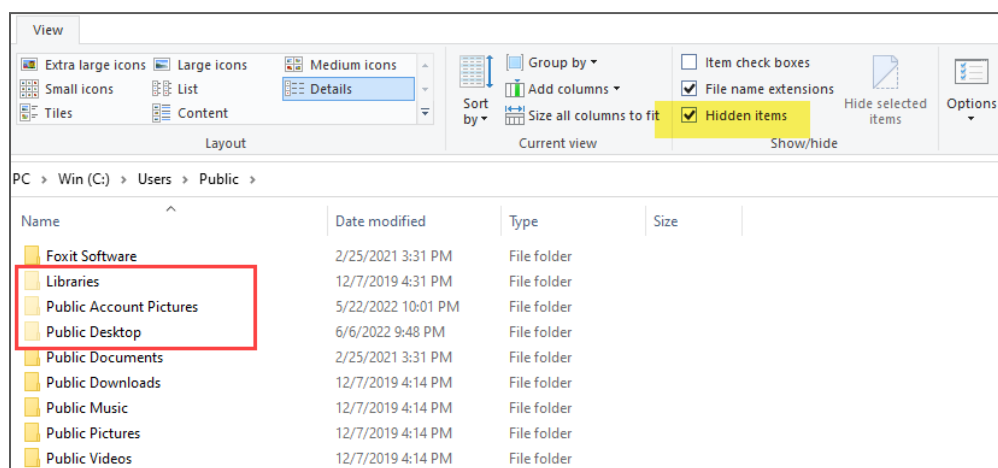


Nguồn: wikipedia

Trong phân cấp của cây thư mục, chúng ta có một thư mục trên cùng nhất được gọi là thư mục gốc. Thư mục gốc trong Windows bắt đầu với các ký tự ổ đĩa như C:, D:, mỗi ký tự đại diện cho một hệ thống tập tin riêng biệt. Để mô tả vị trí một thư mục hay tập tin, ta sử dụng đường dẫn (path). Đường dẫn là một chuỗi ký tự mô tả đường đi từ thư mục gốc đến thư mục hay tập tin hiện tại. Mỗi thư mục phân cấp trên chuỗi đường đi này tách biệt với nhau bằng dấu gạch (slash). Trong Windows, ta dùng dấu gạch lui (\, backslash). Ví dụ, C:\Users\Cindy\Documents\Example.txt là đường dẫn đến một tập tin có tên là Example.txt trong Windows. Ngoài ra, đường dẫn trong hệ điều hành cũng được biểu diễn dưới hai dạng: đường dẫn tuyệt đối và đường dẫn tương đối. Đường dẫn tuyệt đối là đường dẫn bắt đầu từ thư mục gốc. Ví dụ, đường dẫn đầy đủ đến thư mục Desktop của người dùng vutaviva trong Windows là C:\Users\vutaviva\Desktop. Đường dẫn tương đối là đường dẫn tính từ thư mục

hiện tại. Giả sử chúng ta đang đứng ở thư mục C:\Users\vutaviva thì đường dẫn .\Desktop là đường dẫn tương đối đến thư mục Desktop.

Trong hệ điều hành cũng có một số tập tin và thư mục không thể hiện trong cấu trúc cây khi xem ở chế độ mặc định. Một số lý do tập tin bị ẩn như đây là các tập tin cấu hình hệ thống, hệ điều hành không muốn người dùng tác động đến như vô tình xóa hay thay đổi. Hoặc có thể vì tính riêng tư nên chúng ta không muốn để chế độ xem thông thường.



Thao tác trên tập tin và thư mục

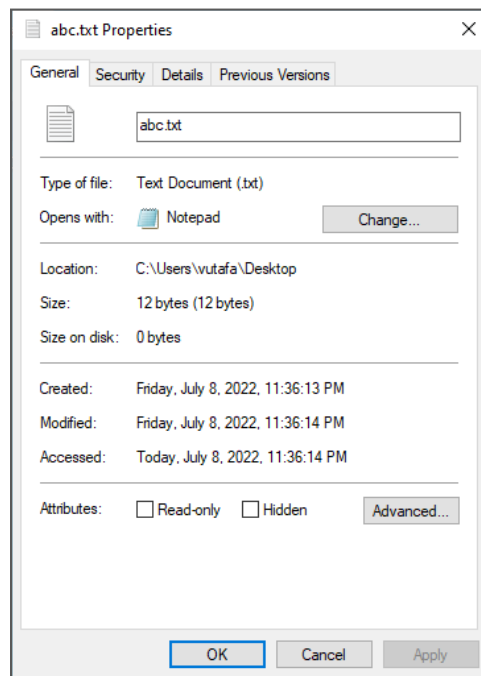
Trong quá trình sử dụng hệ điều hành, chúng ta thường thực hiện rất nhiều thao tác khác nhau trên tập tin và thư mục. Các thao tác cơ bản trên tập tin bao gồm:

- Tạo một tập tin mới
- Đặt/đổi tên
- Thay đổi quyền truy cập và thuộc tính của tập tin
- Mở một tập tin
- Đọc, ghi dữ liệu của tập tin

- Xóa một tập tin
- Đóng tập tin
- Di chuyển tập tin sang nơi khác
- Nén tập tin
- Thay đổi ứng dụng mở

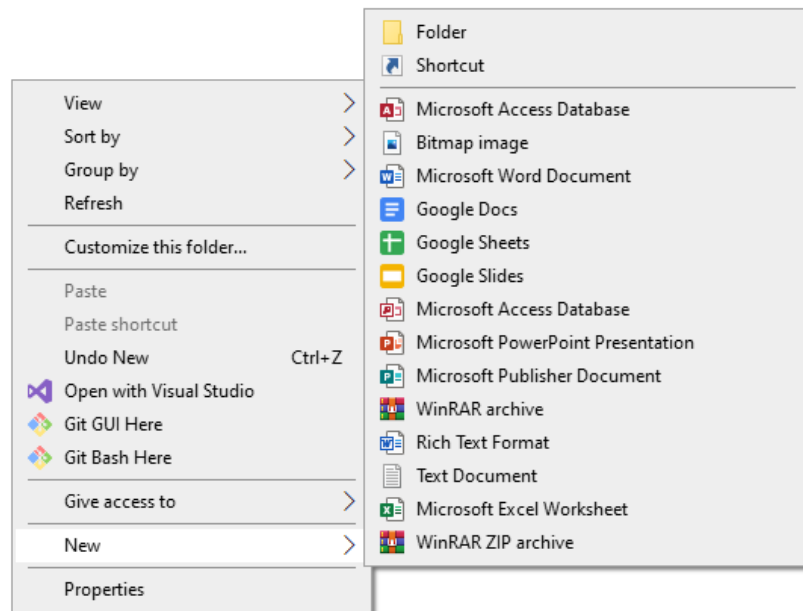
Đối với thư mục, chúng ta cũng có thao tác tương tự như trên tập tin.

Trên GUI, người dùng có thể sử dụng chuột để thực hiện hầu hết các chức năng đã nêu. Ví dụ, để xem thông tin về tập tin/thư mục, ta nhấp chuột phải trên GUI chọn Properties. Sau đó, trên cửa sổ Properties, ta có thể thay đổi các trạng thái của tập tin như chỉ đọc, ẩn.



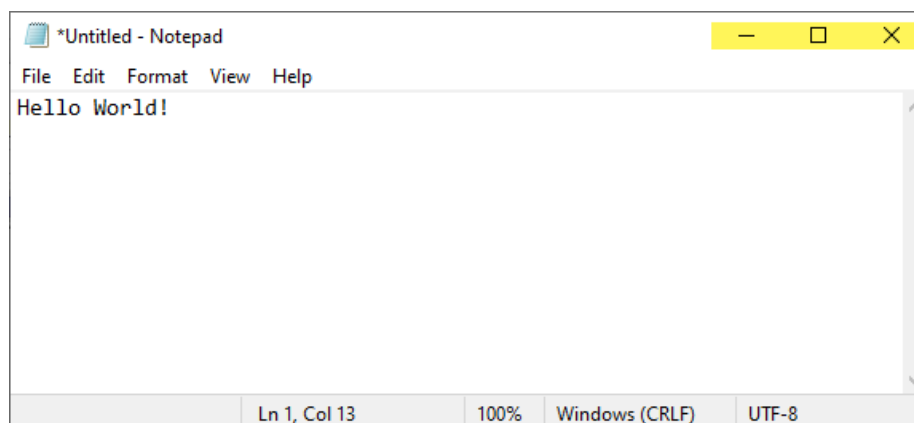
Để tạo tập tin/thư mục mới, ta dùng chương trình File Explorer, di chuyển đến vị trí mong muốn tạo. Sau đó, nhấp phải chuột lên khoảng trống trong cửa sổ thư mục. Một danh mục ngữ cảnh hiện ra chứa một dòng New. Khi rê chuột lên

mục New này, một danh mục ngữ cảnh mới được trình duyệt cho phép tạo thư mục cũng như các tập tin của một số ứng dụng phổ biến.

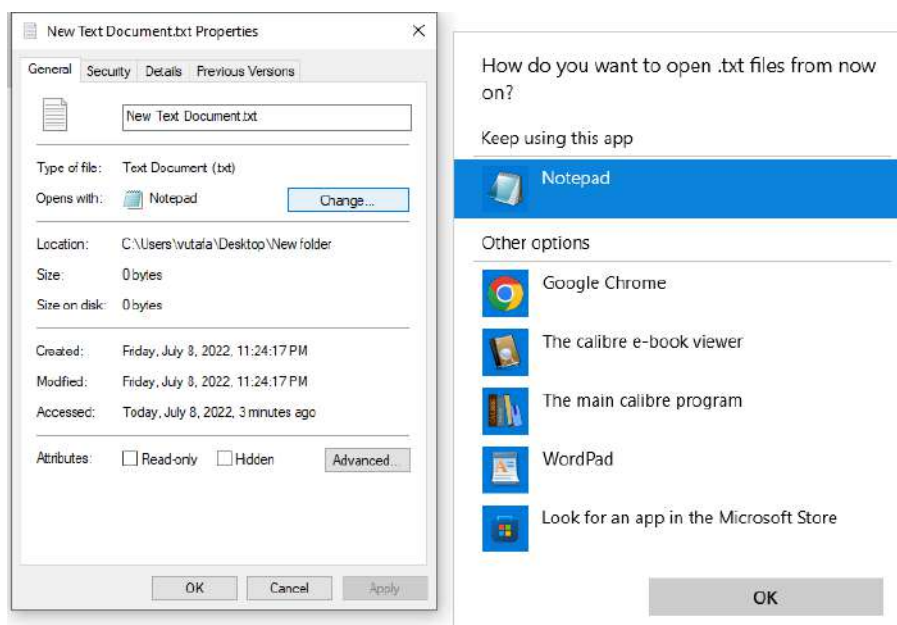


Các tập tin/thư mục khi được tạo mới sẽ có tên mặc định ví dụ New Folder hay New Microsoft Word Document.docx. Để thay đổi tên này, chỉ cần nhấp phải trên tập tin/thư mục đó. Danh mục ngữ cảnh hiện ra cùng nhiều chức năng cho tập tin/thư mục như đổi tên (Rename), xóa (Delete), điều chỉnh (Edit), v.v... Ngoài ra, tùy thuộc vào loại tập tin mà danh mục ngữ cảnh này có thể khác nhau đôi chút.

Để mở tập tin/thư mục, người dùng nhấp đôi chuột trái lên biểu tượng của chúng. Chương trình mặc định dành cho đuôi của tập tin này sẽ được gọi để thực thi. Thông thường, các cửa sổ đều có nút đóng (dấu chéo), phóng lớn (hình vuông), thu nhỏ (dấu gạch ngang) ở góc phải trên cùng. Khi nhấn vào nút đó, các hành động tương ứng sẽ xảy ra.



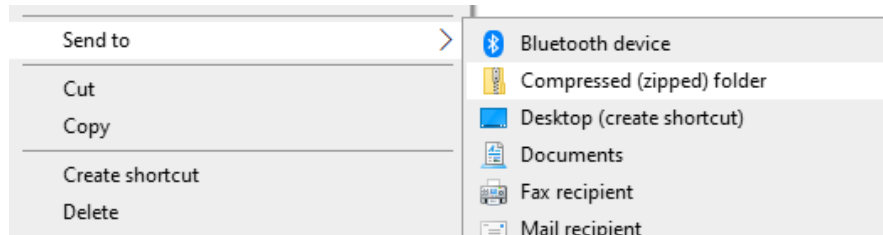
Khi muốn thay đổi ứng dụng mặc định mở một loại tập tin xác định, ta nhấp phải chuột, chọn Properties. Cửa sổ Properties trình diễn dòng Opens with thể hiện chương trình đang được sử dụng để mở tập tin. Ta thay đổi ứng dụng này bằng cách nhấn vào nút Change bên cạnh và chọn các ứng dụng mong muốn trong cửa sổ tiếp theo hiện ra.



Việc sao chép hay di chuyển tập tin/thư mục sang nơi khác, ta dùng chức năng sao chép (Copy) hay cắt (Cut) trong danh mục ngữ cảnh của chúng. Sau

đó, di chuyển đến nơi mong muốn và chọn dán (Paste) trong danh mục ngữ cảnh.

Trong Windows cũng hỗ trợ chức năng nén dữ liệu cơ bản. Sau khi chọn các tập tin/thư mục cần nén, ta cũng nhấp phải chuột để mở danh mục ngữ cảnh. Chọn tiếp mục Send to và Compressed (zipped) folder.

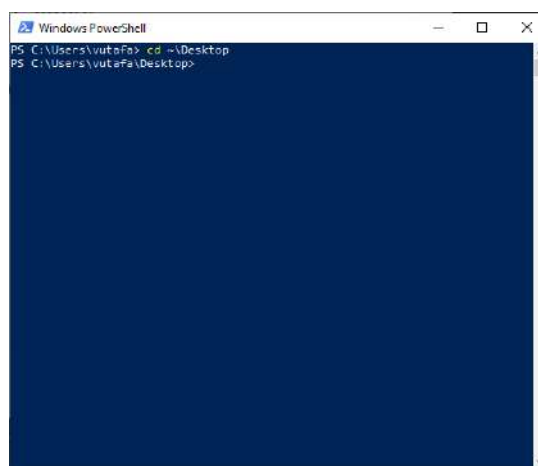


Chức năng thay đổi hay cấp quyền truy cập cho người dùng đối với tập tin/thư mục sẽ được đề cập trong một bài đọc khác.

3. Giao diện dòng lệnh PowerShell

Giới thiệu giao diện dòng lệnh

Giao diện dòng lệnh (command line interface) là giao diện nhận lệnh từ người dùng thông qua các dòng văn bản. Giao diện này thường đơn giản và gần như không sử dụng chuột để thao tác.



Trong thời buổi ban đầu của kỷ nguyên máy tính, các kỹ sư đều sử dụng giao diện dòng lệnh để giao tiếp với máy tính. Nguyên nhân là lúc đó các hệ thống đồ họa chưa được phát triển, các điều khiển giao tiếp với máy tính được thực hiện bởi các kỹ sư thay vì đa số người dùng như ngày nay. Thêm vào đó, hệ thống phần cứng còn yếu nên các hiển thị đồ họa chưa thể triển khai một cách mượt mà.

So sánh với giao diện đồ họa người dùng

Khi so sánh với giao diện đồ họa người dùng, một số điểm khác nhau quan trọng có thể thấy như:

- Giao diện đồ họa người dùng làm cho người mới bắt đầu sử dụng hệ điều hành thao tác dễ dàng hơn thay vì phải bỏ thời gian để học các câu lệnh điều khiển như trong giao diện dòng lệnh. Tuy nhiên, chính vì cần hiển thị đồ họa nên nó sẽ gây tiêu tốn tài nguyên máy tính như bộ nhớ để hiển thị. Trong khi đó, giao diện dòng lệnh chỉ có văn bản nên tiêu tốn rất ít tài nguyên và khi truyền qua mạng để điều khiển máy tính sẽ nhanh chóng hơn.
- Trong giao diện đồ họa, chúng ta phối hợp cả bàn phím lẫn chuột để thao tác nên tốc độ chậm. Giao diện dòng lệnh chủ yếu dùng bàn phím nên thao tác nhanh và hiệu quả hơn.
- Giao diện đồ họa có thể thay đổi về cấu trúc bố trí tùy thuộc vào phiên bản và loại hệ điều hành. Còn giao diện dòng lệnh ít khi có sự thay đổi.

Nhìn chung, mỗi loại đều có những ưu điểm và khuyết điểm riêng cũng như phù hợp vào từng ngữ cảnh, từng nhu cầu cụ thể của mỗi người dùng. Đối với đội ngũ hỗ trợ CNTT, giao diện dòng lệnh là một sự lựa chọn khuyến khích vì có nhiều trường hợp chúng ta cần thao tác sâu xuống hệ thống, thậm chí trên nhiều hệ thống cùng lúc và từ xa.

PowerShell và các lệnh liên quan đến tập tin và thư mục

PowerShell là một shell dòng lệnh được phát triển chủ yếu cho các hệ điều hành Windows mặc dù chúng có thể chạy được cả trên Linux và MacOS. Điểm mạnh của PowerShell trên hệ điều hành Windows là hỗ trợ mạnh các đối tượng .NET. Windows PowerShell là một chương trình thực thi PowerShell.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vutafa>
```

Để liệt kê thư mục tập tin, ta sử dụng lệnh `ls` và sau đó một khoảng trắng là đường dẫn nơi muốn xem cấu trúc thư mục. Nếu để trống phần này thì đường dẫn mặc định là thư mục hiện hành mà chúng ta đang đứng.

```
ls path
```

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> ls C:\

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          10/5/2017   3:40 PM             Intel
d-----          3/18/2017   2:03 PM             PerfLogs
d-r---          10/5/2017   3:46 PM          Program Files
d-r---          10/5/2017   3:29 PM          Program Files (x86)
d-r---          10/5/2017   3:38 PM             Users
d-----          10/5/2017   3:44 PM          Vacation Pictures
d-----          10/5/2017   3:42 PM             Windows
```

Mỗi lệnh có cách thức sử dụng khác nhau, để tra cứu trực tiếp thông tin về lệnh nào đó, ta sử dụng lệnh `Get-Help`, theo sau là tên lệnh cần xem thông tin. Ví dụ, `Get-Help ls` sẽ trả về các thông tin mô tả về lệnh `ls` như tên thay thế, các tham số, v.v..

Get-Help command

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vutafa> Get-Help ls

NAME
    Get-ChildItem

SYNTAX
    Get-ChildItem [[-Path] <string>] [[-Filter] <string>] [-Include <string>] [-Exclude <string>] [-Recurse]
    [-Depth <uint32>] [-Force] [-Name] [-UseTransaction] [-Attributes {ReadOnly | Hidden | System | Directory |
    Archive | Device | Normal | Temporary | SparseFile | ReparsePoint | Compressed | Offline | NotContentIndexed |
    Encrypted | IntegrityStream | NoScrubData}] [-Directory] [-File] [-Hidden] [-ReadOnly] [-System]
    [<CommonParameters>]

    Get-ChildItem [[-Filter] <string>] -LiteralPath <string> [-Include <string>] [-Exclude <string>] [-Recurse]
    [-Depth <uint32>] [-Force] [-Name] [-UseTransaction] [-Attributes {ReadOnly | Hidden | System | Directory |
    Archive | Device | Normal | Temporary | SparseFile | ReparsePoint | Compressed | Offline | NotContentIndexed |
    Encrypted | IntegrityStream | NoScrubData}] [-Directory] [-File] [-Hidden] [-ReadOnly] [-System]
    [<CommonParameters>]

ALIASES
    gci
    ls
    dir
  
```

Mỗi lệnh thường có một tập các tham số để cấu hình thêm cho lệnh. Ví dụ, để thể hiện các tập tin ẩn và tập tin hệ thống, ta sử dụng thêm tham số -Force.

ls -Force path

```

PS C:\Users\cindy> ls -Force C:\

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d--hs-             10/5/2017   3:32 PM             $Recycle.Bin
d--hs-             10/5/2017   6:07 PM          Documents and Settings
d-----            10/5/2017   3:40 PM             Intel
d-----            3/18/2017   2:03 PM             PerfLogs
d-r---             10/5/2017   3:46 PM          Program Files
d-r---             10/5/2017   3:29 PM        Program Files (x86)
d--h--             10/5/2017   3:34 PM          ProgramData
d--hs-             10/5/2017   6:07 PM          Recovery
d--hs-             10/7/2017  12:25 PM        System Volume Information
d-r---             10/5/2017   3:38 PM             Users
d-----            10/5/2017   3:44 PM        Vacation Pictures
d-----            10/5/2017   3:42 PM             Windows
-a-hs-             10/7/2017   8:44 AM        6607331328 hiberfil.sys
-a-hs-             10/7/2017   8:44 AM        3087007744 pagefile.sys
-a-hs-             10/7/2017   8:44 AM        16777216  swapfile.sys
  
```


Khi muốn biết đang ở đâu trong cây thư mục, sử dụng lệnh pwd.

pwd

```
PS C:\Users\cindy> pwd
Path
----
C:\Users\cindy
```

Để thay đổi thư mục hiện hành sang một nơi khác, ta sử dụng lệnh cd. Chuỗi mô tả đường dẫn sau lệnh cd có thể là đường dẫn tuyệt đối hoặc tương đối.

cd path

```
PS C:\Users\cindy> pwd
Path
----
C:\Users\cindy

PS C:\Users\cindy> cd C:\Users\cindy\Documents
PS C:\Users\cindy\Documents>
```

Ngoài đường dẫn tuyệt đối và tương đối, lệnh cd còn hỗ trợ một số ký hiệu đặc biệt như hai dấu chấm là đường dẫn của thư mục cha của thư mục hiện tại. Dấu ngã âm chỉ đến đường dẫn của thư mục chính của mỗi người dùng. Ngoài ra, còn có ký hiệu một dấu chấm để cập đến thư mục hiện hành. Trong quá trình gõ đường dẫn, ta có thể dùng phím Tab để shell dự đoán đường dẫn và tự động hoàn thành đường dẫn giúp chúng ta.

cd ..

cd ~

Để tạo thư mục, sử dụng lệnh mkdir và đặt tên cho thư mục. Lưu ý tên thư mục khi dùng lệnh mkdir hoặc không có khoảng trắng trong tên, hoặc phải để trong các dấu nháy. Trong Powershell, còn hỗ trợ đặt dấu ngoặc kép thấp (backtick) trước khoảng trắng.

mkdir directory_name
mkdir 'directory name'
Powershell: **mkdir** directory` name

```
PS C:\Users\cindy> mkdir my_cool_folder

Directory: C:\Users\cindy

Mode                LastWriteTime         Length Name
----                -
d-----          10/7/2017   1:03 PM             my_cool_folder
```

Đôi khi ta muốn xem lại các lệnh đã gõ để biết các thực thi vừa qua trên hệ thống, lệnh history sẽ giúp thực hiện điều này. Ngoài ra, ta có thể dùng các phím mũi tên lên, mũi tên xuống để duyệt qua các lệnh đã gõ theo thứ tự thời gian từ gần nhất đến xa nhất. Các shell cũng hỗ trợ để tìm kiếm các lệnh có trong history.

history

```
Windows PowerShell
PS C:\Users\cindy> history_

Id CommandLine
--
1 cd ~
2 clear
3 pwd
4 cd C:\Users\cindy\Documents
5 cd ..
6 pwd
7 cd C:\Users\cindy\Documents
8 cd ..\Desktop
9 cd ..\Documents
10 clear
11 cd ..\Desktop
12 pwd
```

Khi có quá nhiều thông tin hiển thị trên màn hình dòng lệnh, ta có thể xóa trống màn hình bằng lệnh clear.

clear

Để sao chép một tập tin đến một nơi khác, sử dụng lệnh cp.

cp file_name new_path

```
PS C:\Users\cindy\Documents> cp mycoo1file.txt C:\Users\cindy\Desktop\  
PS C:\Users\cindy\Documents> _
```

Lệnh cp cũng cho phép sao chép cùng lúc nhiều tập tin. Để làm được điều này, chúng ta sử dụng ký tự đại diện là dấu hoa thị trong tên các tập tin. Dấu hoa thị hay nói ngắn gọn là dấu sao, là ký tự ám chỉ có thể thay thế bất kỳ ký tự nào vào đó trong tên tập tin. Nếu tập tin nào khớp với mẫu này, sẽ được thực hiện sao chép. Ví dụ, *.jpg là đại diện cho bất kỳ tập tin nào có đuôi là jpg.

```
PS C:\Users\cindy\Documents> cp *.jpg C:\Users\cindy\Desktop\  
PS C:\Users\cindy\Documents> _
```

Để chép toàn bộ thư mục đến nơi khác, ta vẫn sử dụng lệnh cp nhưng bổ sung thêm tham số là -Recurse cho Powershell.

cp -Recurse directory_name new_path

Lệnh mv dùng để di chuyển tập tin đến một nơi khác. Nếu trong đường dẫn có chứa tên file thì lệnh mv sẽ thực hiện đổi tên của tập tin đó. Khi chỉ muốn đổi tên tập tin mà không di chuyển, ta chỉ cần gõ tên mới thay vì ghi đường dẫn vào lệnh. Tương tự như lệnh sao chép (cp), để di chuyển cùng lúc nhiều tập tin, ta dùng ký tự đại diện là dấu hoa thị trong tên của tập tin.

mv file_name new_path

```
PS C:\Users\cindy\Desktop> mv .\yellow_document.txt C:\Users\cindy\Documents\  
PS C:\Users\cindy\Desktop> _
```

Để xóa tập tin/thư mục, sử dụng lệnh `rm`. Đối với xóa thư mục, các tham số như `-recurse` trong PowerShell khi được thiết lập sẽ xóa các tập tin/thư mục con mà không cần phải xác nhận.

`rm file_name`

```
PS C:\Users\cindy> rm ~\misc_folder

Confirm
The item at C:\Users\cindy\misc_folder has children and the Recurse parameter was not specified. If you
continue, all children will be removed with the item. Are you sure you want to continue?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): N
PS C:\Users\cindy> rm ~\misc_folder -Recurse
```

Tập tin văn bản có thể xem trực tiếp trong giao diện dòng lệnh với lệnh `cat`.

`cat file_name`

```
PS C:\Users\cindy> cat .\important_document.txt
This is a very important document.
```

Đối với tập tin văn bản có kích thước lớn, việc hiển thị toàn bộ nội dung sẽ không chứa vừa trong một màn hình khi dùng lệnh `cat`. Để trình diễn nội dung một cách dần dần, ta sử dụng lệnh `more` nếu dùng PowerShell. Khi các lệnh này thực thi, nó sẽ mở một cửa sổ tương tác để trình bày nội dung văn bản. Trong cửa sổ tương tác này, chúng ta có thể dùng các lệnh để di chuyển, tìm kiếm, v.v.

`more file_name`

Nếu chỉ muốn xem một số dòng đầu trong tập tin văn bản, ta bổ sung thêm tham số `-Head` vào lệnh `cat` trong PowerShell.

```
PS C:\Users\cindy> cat fruits.txt -Head 10
apple
apricot
avocado
banana
berry
blackberry
elderberry
fig
grape
grapefruit
```

Tìm kiếm trong tập tin văn bản có thể dùng lệnh Select-String trong PowerShell. Lệnh này cũng hỗ trợ tìm kiếm trên nhiều tập tin bằng cách chỉ định các tập tin với ký tự đại diện (dấu hoa thị). Ví dụ, trong hình, ta tìm từ cow trong tập tin farm_animals.txt, kết quả sẽ xuất ra dòng có từ cow nếu tìm thấy

Select-String keyword file_name

```
PS C:\Users\cindy> Select-String cow farm_animals.txt
farm_animals.txt:1:cow chicken horse

PS C:\Users\cindy> Select-String cow *.txt
farm_animals.txt:1:cow chicken horse
ranch_animals.txt:1:cow sheep horse
```

Một lệnh trong CLI có thể xuất các thông báo ra màn hình, đó là lệnh echo. Mặc dù việc xuất thông báo như thế này không mang nhiều ý nghĩa, nhưng khi được sử dụng trong các đoạn mã khác sẽ giúp chuyển các thông báo đến thiết bị nhập xuất chuẩn.

echo message

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vutafa> echo "Hello fit@hcmus"
Hello fit@hcmus
PS C:\Users\vutafa>
```

Ngoài việc xuất thông báo ra màn hình, echo còn xuất thông báo ra tập tin văn bản. Dấu lớn hơn (>) được gọi là toán tử chuyển hướng. Chúng ta dùng toán tử này để chuyển thông báo thay ra tập tin thay vì ra màn hình. Nếu tập tin đã tồn tại, tập tin này sẽ bị ghi đè.

echo message > text_file

```
PS C:\Users\cindy\Desktop> echo woof > dog.txt
PS C:\Users\cindy\Desktop> ls

Directory: C:\Users\cindy\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----          10/5/2017   3:45 PM             CoolFiles
d-----          10/5/2017   3:45 PM             ShareMe
-a-----          10/5/2017   3:45 PM              0 blue.txt
-a-----          10/5/2017   2:00 PM          475 colors.zip
-a-----          10/7/2017   3:27 PM           14 dog.txt
-a-----          10/3/2017   4:46 PM         4096 hello.exe
```

Để tránh việc ghi đè tập tin, ta có thể sử dụng toán tử lớn hơn, lớn hơn (>>). Toán tử này sẽ viết thêm nội dung vào tập tin đang tồn tại. Trong hình, tập tin dog.txt đã có từ woof, khi dùng lệnh echo với toán tử >>, tập tin này được viết thêm nội dung mới, trong khi đó nội dung cũ không bị xóa.

echo message >> text_file

```
PS C:\Users\cindy\Desktop> echo woof >> dog.txt
PS C:\Users\cindy\Desktop> cat dog.txt
woof
woof
PS C:\Users\cindy\Desktop> _
```

Một số lệnh có thể gặp lỗi khi thực thi, để điều hướng chỉ thông báo lỗi ra tập tin, ta sử dụng toán tử 2>.

command 2> text_file

```
PS C:\Users\cindy> rm secure_file 2> errors.txt
PS C:\Users\cindy> cat errors.txt
rm : Cannot remove item C:\Users\cindy\secure_file: You do not have
At line:1 char:1
+ rm secure_file 2> errors.txt
+ ~~~~~
```

Nếu chỉ muốn bỏ qua các thông báo lỗi, ta có thể sử dụng một số dạng đặc biệt trong thành phần tên tập tin xuất ra. Ví dụ như đối với PowerShell, \$null được sử dụng.

command 2> \$null

Ngoài gửi thông báo trực tiếp, chúng ta có thể chuyển thông báo được xuất ra từ một ứng dụng để làm đầu vào cho một ứng dụng khác. Để thực hiện được thao tác này, chúng ta sử dụng toán tử ống, pipe, được biểu diễn với ký tự dấu gạch đứng. Ta có thể xâu chuỗi nhiều thực thi với các toán tử ống.

command_1 | command_2 | command_3 ...

```
PS C:\Users\cindy> cat words.txt
street
tree
blast
last
PS C:\Users\cindy> cat words.txt | select-string st
street
blast
last
```


Bài đọc 2: Thao Tác Trên Hệ Điều Hành Linux

1. Giao diện đồ họa người dùng

Hệ điều hành Linux là một tên gọi chung cho các hệ điều hành sử dụng nhân Linux và cũng được gọi là các bản phân phối của Linux. Tương tự như Windows, chúng cũng có các giao diện đồ họa người dùng và giao diện dòng lệnh. Tuy nhiên, những người sử dụng hệ điều hành này thường hướng tới sử dụng giao diện dòng lệnh nhiều hơn do một phần các gói phần mềm được cài theo cách này và phần khác được sử dụng bởi các nhà khoa học, nhà kỹ thuật hơn là các đối tượng người dùng phổ thông. Dù vậy, bất kỳ người dùng nào cũng có thể sử dụng do giao diện đồ họa ngày càng trở nên dễ thao tác. Đa số hệ điều hành Linux đều miễn phí hoặc có chi phí thấp hơn đáng kể so với hệ điều hành Windows nên đây cũng là một lý do để thu hút người dùng.

Bố trí giao diện trong mỗi bản phân phối Linux cũng khác nhau. Do đó cần thời gian làm quen khi người dùng hướng tới sử dụng giao diện đồ họa người dùng.



Ubuntu 20.04



Fedora Kinoite 35 20.04

Nguồn : wikimedia

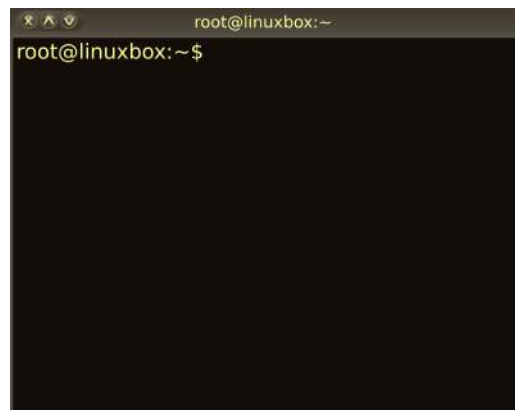
Các thao tác như tạo, sao chép, di chuyển, xóa, nén, xem thuộc tính các tập tin/thư mục cũng được thao tác tương tự như trên Windows. Trong Linux, hệ thống tập tin bắt đầu với một thư mục gốc duy nhất là thư mục có ký hiệu dấu gạch tới (/). Nếu có thêm các ổ đĩa khác thì các ổ đĩa này cũng được xem như tập tin. Chi tiết về thiết bị như ổ cứng sẽ đề cập trong các bài sau. Đường dẫn

trong Linux còn có một điểm khác nữa là dấu phân cách. Trong Linux, dấu phân cách giữa các thư mục là dấu gạch tới (/).

2. Giao diện dòng lệnh Bash

Terminal, Shell, và Bash

Khi làm việc với giao diện dòng lệnh trong Linux hay MacOS, chúng ta thường nghe một số thuật ngữ như terminal, shell và bash. Terminal là một chương trình giúp chúng ta thực hiện các giao tiếp với máy tính thông qua dòng lệnh, hay nói cách khác là nơi để gõ các lệnh điều khiển hệ thống. Trên Linux, chúng ta còn có một khái niệm là virtual terminal, nó không hẳn là một chương trình mà có thể hiểu đơn giản là một môi trường thực thi cho hệ điều hành không có giao diện đồ họa. Bên dưới mỗi terminal là shell. Nó được xem là bộ thông dịch dòng lệnh. Nghĩa là khi chúng ta gõ xong câu lệnh, nó sẽ phân tích câu lệnh này làm gì hay gọi một chương trình gì. Sau đó sẽ thực hiện các lệnh này nếu nó hiểu được.



Có nhiều loại shell được phát triển cho các hệ điều hành nhưng Bash được xem là loại shell phổ biến nhất.

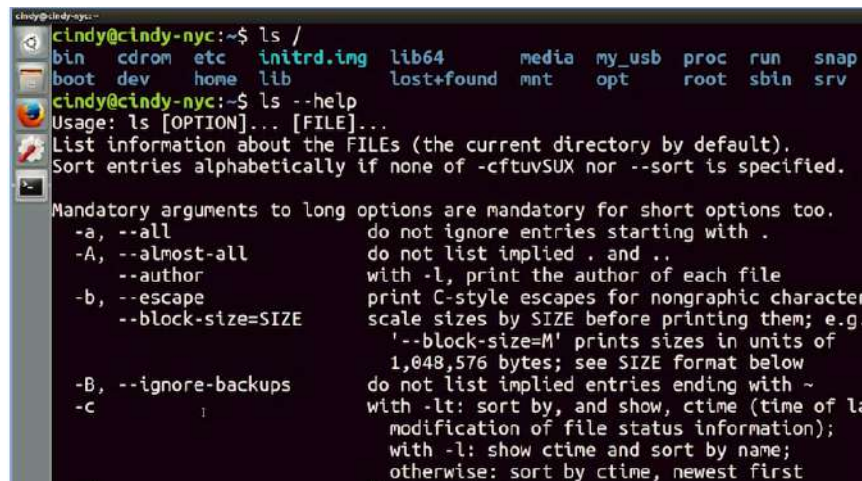
Bash và các lệnh liên quan đến tập tin và thư mục

Các lệnh trong Bash cũng tương tự như trong PowerShell. Do đó, nếu chúng ta đã làm quen với các câu lệnh trong Windows PowerShell ở bài trước, thì phần này có thể xem để biết cách trình bày kết quả trong Linux. Chúng tôi cũng mô tả lại các lệnh để bạn đọc chưa xem qua bài trước cũng có thể nắm được ý nghĩa của các câu lệnh. Ngoài ra, bản phân phối Linux được sử dụng

chính trong xuyên suốt khóa học là hệ điều hành Ubuntu. Các bản phân phối khác sử dụng Bash cũng có kết quả tương tự.

Để liệt kê thư mục tập tin, ta sử dụng lệnh ls và sau đó một khoảng trắng là đường dẫn nơi muốn xem cấu trúc thư mục. Nếu để trống phần này thì đường dẫn mặc định là thư mục hiện hành mà chúng ta đang đứng.

ls path



```
cindy@cindy-nyc:~$ ls /
bin  cdrom  etc  initrd.img  lib64  media  my_usb  proc  run  snap
boot  dev  home  lib  lost+found  mnt  opt  root  sbin  srv
cindy@cindy-nyc:~$ ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILES (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
-a, --all                do not ignore entries starting with .
-A, --almost-all        do not list implied . and ..
--author                with -l, print the author of each file
-b, --escape             print C-style escapes for nongraphic characters
--block-size=SIZE       scale sizes by SIZE before printing them; e.g.
                        '--block-size=M' prints sizes in units of
                        1,048,576 bytes; see SIZE format below
-B, --ignore-backups     do not list implied entries ending with ~
-c                       with -lt: sort by, and show, ctime (time of last
                        modification of file status information);
                        with -l: show ctime and sort by name;
                        otherwise: sort by ctime, newest first
```

Lệnh ls cũng có các tham số thêm. Các tham số cũng được gọi là cờ (flag). Để tìm hiểu thông tin về lệnh, ta viết - - help sau tên lệnh. Cờ help chỉ cung cấp thông tin ngắn gọn về lệnh, để có được thông tin mô tả đầy đủ hơn, trong Linux ta có một lệnh riêng là man. Sau khi gõ lệnh man với tên lệnh cần tham khảo, một màn hình với thông tin đầy đủ sẽ hiện ra.

man command

Quay trở lại với một số tham số thêm của lệnh ls như -l nghĩa liệt kê tập tin và thư mục dưới dạng danh sách dài, mỗi dòng mô tả một tập tin/thư mục. Để hiện đầy đủ kể cả các tập tin ẩn hay tập tin hệ thống, ta dùng cờ -a. Và hiển nhiên, ta có thể phối hợp nhiều cờ lại với nhau, thậm chí là viết tắt với chỉ một dấu gạch.

```
ls -l path
ls -a path
ls -l -a path
ls -la path
```

```
drwxr-xr-x 20 root root 4100 Oct 9 16:35 dev
drwxr-xr-x 130 root root 12288 Oct 5 16:32 etc
drwxr-xr-x 3 root root 4096 Oct 5 13:30 home
lrwxrwxrwx 1 root root 33 Oct 5 13:30 initrd.img
drwxr-xr-x 22 root root 4096 Oct 5 13:31 lib
drwxr-xr-x 2 root root 4096 Aug 1 07:19 lib64
drwx----- 2 root root 16384 Oct 5 13:28 lost+found
drwxr-xr-x 3 root root 4096 Oct 5 15:27 media
drwxr-xr-x 2 root root 4096 Aug 1 07:17 mnt
drwxr-xr-x 2 root root 4096 Oct 5 16:40 my_usb
drwxr-xr-x 3 root root 4096 Oct 5 16:32 opt
dr-xr-xr-x 219 root root 0 Oct 8 10:11 proc
drwx----- 4 root root 4096 Oct 5 16:16 root
drwxr-xr-x 26 root root 820 Oct 9 16:36 run
drwxr-xr-x 2 root root 12288 Oct 5 13:37 sbin
drwxr-xr-x 2 root root 4096 Apr 29 04:38 snap
drwxr-xr-x 2 root root 4096 Aug 1 07:17 srv
dr-xr-xr-x 13 root root 0 Oct 8 10:11 sys
drwxrwxrwt 12 root root 4096 Oct 9 16:36 tmp
drwxr-xr-x 11 root root 4096 Aug 1 07:24 usr
drwxr-xr-x 14 root root 4096 Aug 1 07:34 var
lrwxrwxrwx 1 root root 30 Oct 5 13:30 vmlinuz ->
```

Khi muốn biết đang ở đâu trong cây thư mục, sử dụng lệnh pwd.

```
pwd
```

```
cindy@cindy-nyc:~/Desktop$ pwd
/home/cindy/Desktop
```

Để thay đổi thư mục hiện hành sang một nơi khác, ta sử dụng lệnh cd. Chuỗi mô tả đường dẫn sau lệnh cd có thể là đường dẫn tuyệt đối hoặc tương đối.

```
cd path
```

```
cindy@cindy-nyc:~/Desktop$ pwd
/home/cindy/Desktop
cindy@cindy-nyc:~/Desktop$ cd /home/cindy/Documents
```

Ngoài đường dẫn tuyệt đối và tương đối, lệnh `cd` còn hỗ trợ một số ký hiệu đặc biệt như hai dấu chấm là đường dẫn của thư mục cha của thư mục hiện tại. Dấu ngã âm chỉ đến đường dẫn của thư mục chính của mỗi người dùng. Ngoài ra, còn có ký hiệu một dấu chấm để cập đến thư mục hiện hành. Trong quá trình gõ đường dẫn, ta có thể dùng phím Tab để shell dự đoán đường dẫn và tự động hoàn thành đường dẫn giúp chúng ta.

```
cd ..  
cd ~
```

```
cindy@cindy-nyc:~/Desktop$ pwd  
/home/cindy/Desktop  
cindy@cindy-nyc:~/Desktop$ cd ../Documents  
cindy@cindy-nyc:~/Documents$ cd ~/Desktop  
cindy@cindy-nyc:~/Desktop$
```

Để tạo thư mục, sử dụng lệnh `mkdir` và đặt tên cho thư mục. Lưu ý tên thư mục khi dùng lệnh `mkdir` hoặc không có khoảng trắng trong tên, hoặc phải để trong các dấu nháy. Trong Powershell, còn hỗ trợ đặt dấu ngoặc kép thấp (backtick) trước khoảng trắng.

```
mkdir directory_name  
mkdir 'directory name'  
Powershell: mkdir `directory` name
```

```
cindy@cindy-nyc:~/Desktop$ mkdir my_cool_folder  
cindy@cindy-nyc:~/Desktop$ ls  
blue_document.txt  google-chrome-stable_current_amd64.deb  my_cool_folder  my_important_file  
file_input.txt     green_document.txt                       myfile.txt      red_document.txt  
cindy@cindy-nyc:~/Desktop$
```

Đôi khi ta muốn xem lại các lệnh đã gõ để biết các thực thi vừa qua trên hệ thống, lệnh `history` sẽ giúp thực hiện điều này. Ngoài ra, ta có thể dùng các phím mũi tên lên, mũi tên xuống để duyệt qua các lệnh đã gõ theo thứ tự thời

gian từ gần nhất đến xa nhất. Các shell cũng hỗ trợ để tìm kiếm các lệnh có trong history.

history

```
indy-nyc: ~/Desktop
cindy@cindy-nyc:~/Desktop$ history
188 cd ~/Desktop/
189 touch myfile.txt
190 cd ~/Downloads/
191 ls
192 rm p7zip-full_16.02+dfsg-3_amd
193 clear
194 ls /
195 ls --help
196 man ls
197 ls -l /
198 ls -la /
199 clear
```

Khi có quá nhiều thông tin hiển thị trên màn hình dòng lệnh, ta có thể xóa trống màn hình bằng lệnh clear.

clear

Để sao chép một tập tin đến một nơi khác, sử dụng lệnh cp.

cp file_name new_path

```
cindy@cindy-nyc:~/Documents$ cp my_very_cool_file.txt ~/Desktop
cindy@cindy-nyc:~/Documents$
```

Lệnh cp cũng cho phép sao chép cùng lúc nhiều tập tin. Để làm được điều này, chúng ta sử dụng ký tự đại diện là dấu hoa thị trong tên các tập tin. Dấu hoa thị hay nói ngắn gọn là dấu sao, là ký tự ám chỉ có thể thay thế bất kỳ ký tự nào vào đó trong tên tập tin. Nếu tập tin nào khớp với mẫu này, sẽ được thực hiện sao chép. Ví dụ, *.jpg là đại diện cho bất kỳ tập tin nào có đuôi là jpg.

```
cindy@cindy-nyc:~/Documents$ cp *.png ~/Desktop
```

Để chép toàn bộ thư mục đến nơi khác, ta vẫn sử dụng lệnh cp nhưng bổ sung thêm tham số là `-r`.

```
cp -r directory_name new_path
```

Lệnh mv dùng để di chuyển tập tin đến một nơi khác. Nếu trong đường dẫn có chứa tên file thì lệnh mv sẽ thực hiện đổi tên của tập tin đó. Khi chỉ muốn đổi tên tập tin mà không di chuyển, ta chỉ cần gõ tên mới thay vì ghi đường dẫn vào lệnh. Tương tự như lệnh sao chép (cp), để di chuyển cùng lúc nhiều tập tin, ta dùng ký tự đại diện là dấu hoa thị trong tên của tập tin.

```
mv file_name new_path
```

```
cindy@cindy-nyc:~/Desktop$ mv blue_document.txt ~/Documents
```

Để xóa tập tin/thư mục, sử dụng lệnh rm. Đối với xóa thư mục, các tham số như `-r` khi được thiết lập sẽ xóa các tập tin/thư mục con mà không cần phải xác nhận.

```
rm file_name
```

```
cindy@cindy-nyc:~$ rm text1.txt
```

Tập tin văn bản có thể xem trực tiếp trong giao diện dòng lệnh với lệnh cat.

```
cat file_name
```

```
cindy@cindy-nyc:~$ cat important_document.txt
This is a very important document.
```

Đối với tập tin văn bản có kích thước lớn, việc hiển thị toàn bộ nội dung sẽ không chứa vừa trong một màn hình khi dùng lệnh cat. Để trình diễn nội dung

một cách dần dần, ta sử dụng lệnh `less`. Khi các lệnh này thực thi, nó sẽ mở một cửa sổ tương tác để trình bày nội dung văn bản. Trong cửa sổ tương tác này, chúng ta có thể dùng các lệnh để di chuyển, tìm kiếm, v.v.

less file_name

Nếu chỉ muốn xem một số dòng đầu trong tập tin văn bản, ta sử dụng lệnh `head`.

```
cindy@cindy-nyc:~$ head fruits.txt
apple
apricot
avocado
banana
berry
blackberry
elderberry
fig
grape
grapefruit
```

Tìm kiếm trong tập tin văn bản có thể dùng lệnh `grep`. Lệnh `grep` cũng hỗ trợ tìm kiếm trong một nhóm các tập tin hoặc tập tin với ký tự đại diện.

grep keyword file_name1 file_name2 ...

```
cindy@cindy-nyc:~$ grep cow farm_animals.txt
cow chicken horse
cindy@cindy-nyc:~$ grep cow *_animals.txt
farm_animals.txt:cow chicken horse
ranch_animals.txt:cow sheep horse
```

Một lệnh trong CLI có thể xuất các thông báo ra màn hình, đó là lệnh `echo`. Mặc dù việc xuất thông báo như thế này không mang nhiều ý nghĩa, nhưng khi được sử dụng trong các đoạn mã khác sẽ giúp chuyển các thông báo đến thiết bị nhập xuất chuẩn.

echo message

```
root@private: ~  
root@private:~# echo "Hello fit@hcmus"  
Hello fit@hcmus  
root@private:~#
```

Ngoài việc xuất thông báo ra màn hình, echo còn xuất thông báo ra tập tin văn bản. Dấu lớn hơn (>) được gọi là toán tử chuyển hướng. Chúng ta dùng toán tử này để chuyển thông báo thay ra tập tin thay vì ra màn hình. Nếu tập tin đã tồn tại, tập tin này sẽ bị ghi đè.

echo message > text_file

```
cindy@cindy-nyc:~/Desktop$ echo woof > dog.txt  
cindy@cindy-nyc:~/Desktop$ cat dog.txt  
woof  
cindy@cindy-nyc:~/Desktop$
```

Để tránh việc ghi đè tập tin, ta có thể sử dụng toán tử lớn hơn, lớn hơn (>>). Toán tử này sẽ viết thêm nội dung vào tập tin đang tồn tại. Trong hình, tập tin dog.txt đã có từ woof, khi dùng lệnh echo với toán tử >>, tập tin này được viết thêm nội dung mới, trong khi đó nội dung cũ không bị xóa.

echo message >> text_file

```
cindy@cindy-nyc:~/Desktop$ echo woof > dog.txt  
cindy@cindy-nyc:~/Desktop$ cat dog.txt  
woof  
cindy@cindy-nyc:~/Desktop$ echo woof >> dog.txt  
cindy@cindy-nyc:~/Desktop$ cat dog.txt  
woof  
woof  
cindy@cindy-nyc:~/Desktop$
```

Một số lệnh có thể gặp lỗi khi thực thi, để điều hướng chỉ thông báo lỗi ra tập tin, ta sử dụng toán tử 2>.

command 2> text_file

```
cindy@cindy-nyc:~/Desktop$ ls /dir/fake_dir 2> error_output.txt
cindy@cindy-nyc:~/Desktop$ cat error_output.txt
ls: cannot access '/dir/fake_dir': No such file or directory
cindy@cindy-nyc:~/Desktop$
```

Nếu chỉ muốn bỏ qua các thông báo lỗi, ta có thể sử dụng một số dạng đặc biệt trong thành phần tên tập tin xuất ra. Ví dụ như đối với Bash trong Linux, tập tin /dev/null được sử dụng.

command 2> /dev/null

Ngoài gửi thông báo trực tiếp, chúng ta có thể chuyển thông báo được xuất ra từ một ứng dụng để làm đầu vào cho một ứng dụng khác. Để thực hiện được thao tác này, chúng ta sử dụng toán tử ống, pipe, được biểu diễn với ký tự dấu gạch đứng. Ta có thể xâu chuỗi nhiều thực thi với các toán tử ống.

command_1 | command_2 | command_3 ...

```
cindy@cindy-nyc:~/Desktop$ ls -la /etc | grep bluetooth
drwxr-xr-x  2 root root  4096 Oct  5 13:38 bluetooth
cindy@cindy-nyc:~/Desktop$
```

Bài đọc 3: Quyền Truy Cập Hệ Thống

1. Các loại tài khoản người dùng và nhóm

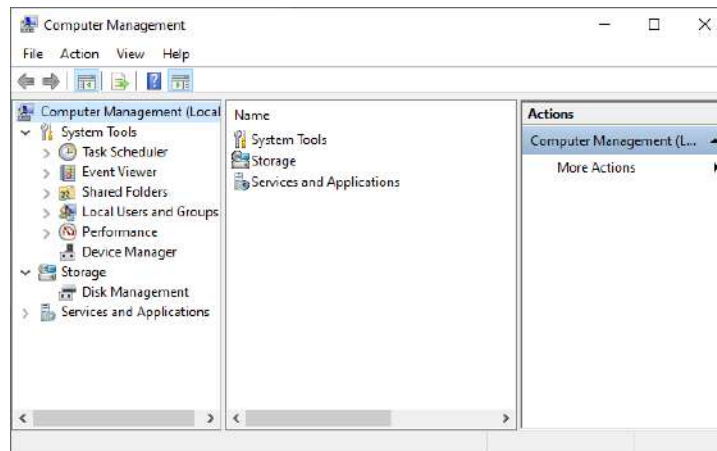
Phân loại tài khoản người dùng và nhóm

Trong quá trình làm việc với máy tính, đặc biệt đối với các máy tính được chia sẻ, người sử dụng có thể vô tình hay cố ý thực hiện các thao tác gây ảnh hưởng đến sự ổn định, độ an toàn và bảo mật của hệ thống. Phân loại người dùng giúp kiểm soát và bảo vệ hệ thống tốt hơn. Mỗi hệ thống có các cách phân loại khác nhau nhưng có thể quy về thành hai loại chính. Loại thứ nhất là người dùng chuẩn (standard user), loại thứ hai là quản trị viên (administrator). Người dùng chuẩn sẽ bị giới hạn một số quyền truy cập như không thể cài đặt phần mềm hay thay đổi các thiết lập hệ thống. Trong khi đó, quản trị viên có toàn quyền kiểm soát hệ thống.

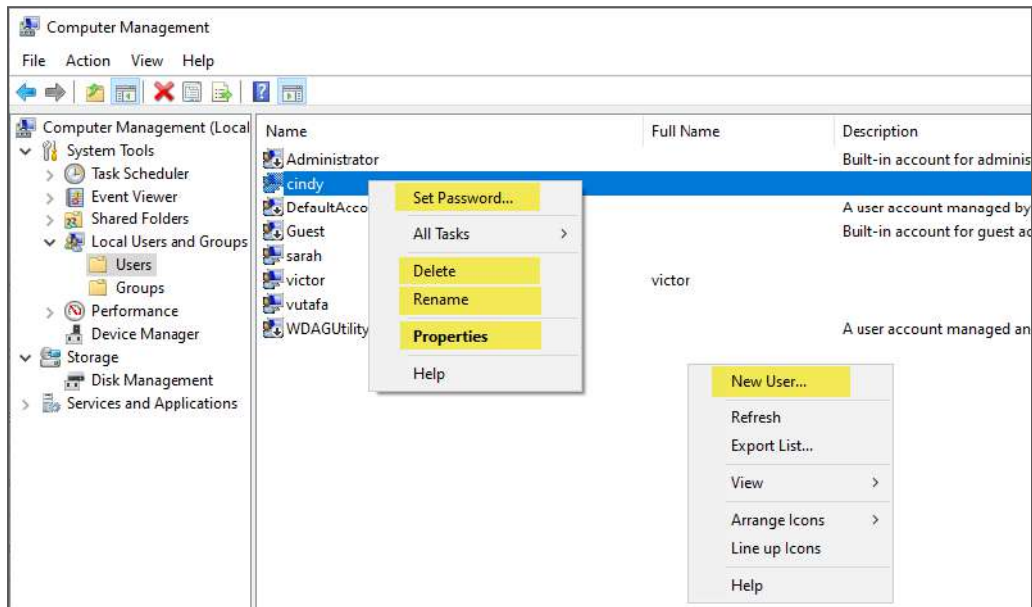
Ngoài phân loại từng người dùng, chúng ta còn gom nhóm họ lại để thuận tiện trong quá trình cấu hình. Ví dụ như ta có thể thiết lập nhóm phụ huynh. Những người trong nhóm này sẽ bị giới hạn quyền cài đặt phần mềm. Hay một nhóm khác là trẻ em, chúng ta sẽ bật thêm các chức năng an toàn đối với chúng.

Xem và cấu hình tài khoản trên Windows và Linux

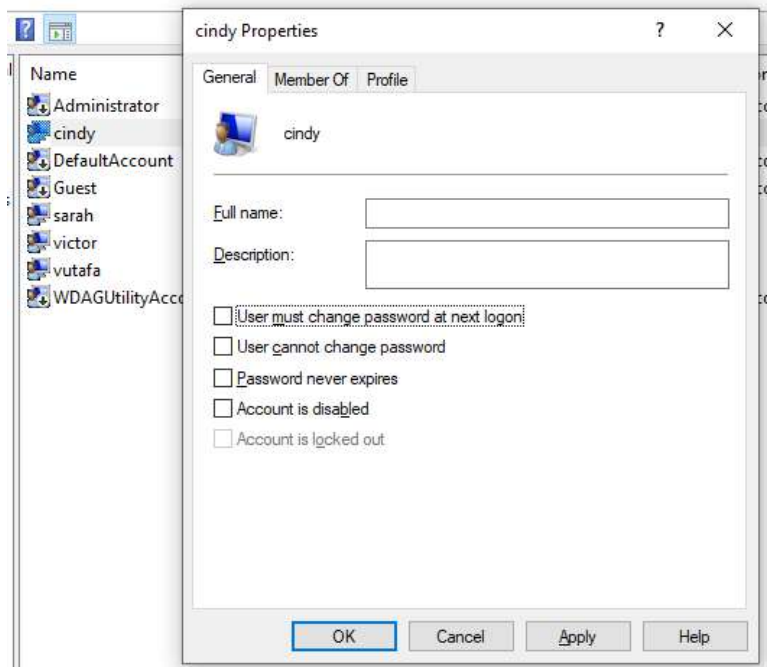
Trên Windows, việc cấu hình người dùng thường thông qua một ứng dụng có tên là Computer Management. Chương trình này quản lý hầu hết các cấu hình quan trọng của hệ thống máy tính.



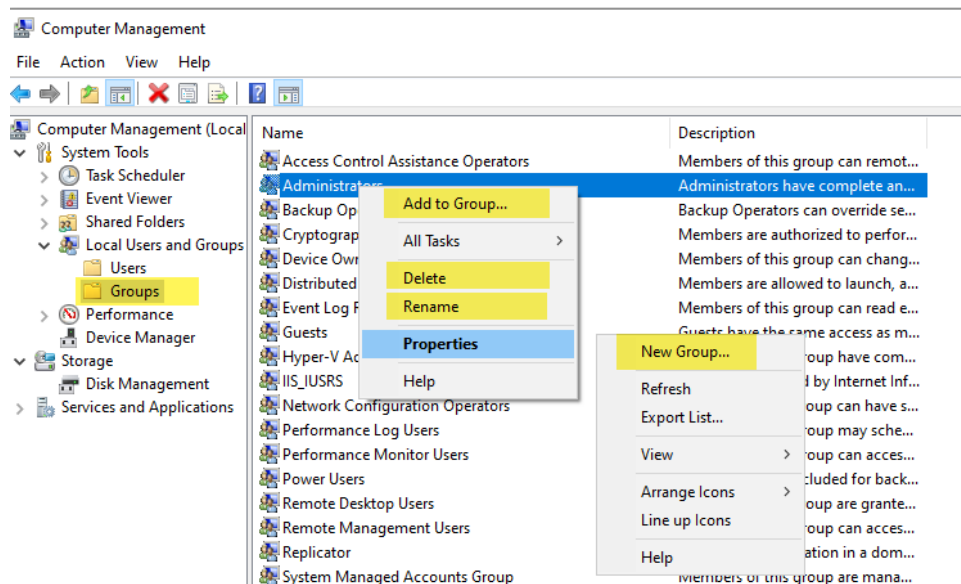
Computer Management bao gồm các công cụ như sau. Bộ lập lịch nhiệm vụ (task scheduler) dùng để thiết lập thời gian thực thi của chương trình hay nhiệm vụ nào đó. Ví dụ, tắt máy tính vào lúc 11h đêm mỗi ngày. Trình xem nhật ký sự kiện (Event Viewer) để xem các tập tin log ghi lại nhật ký của các sự kiện xảy ra trong hệ thống. Phần thư mục chia sẻ (shared folders) giúp các người dùng trong hệ thống có thể chia sẻ tập tin cho nhau. Phần quản lý người dùng và nhóm (local users and groups) là phần quản lý người dùng và nhóm người dùng sử dụng hệ thống. Đối với phần hiệu năng (performance), ta có thể theo dõi quá trình thực thi của các tài nguyên như CPU và RAM. Bộ quản lý thiết bị dùng để quản lý các thiết bị có trong hệ thống như màn hình, loa, v.v. Trong khi đó, bộ quản lý đĩa thì tập trung vào nhiệm vụ quản lý các vùng chứa dữ liệu trong máy tính. Cuối cùng là dịch vụ và ứng dụng để quản lý các chương trình và dịch vụ có sẵn trên hệ thống.



Trong cửa sổ thuộc tính của mỗi tài khoản, ta có thể điều chỉnh việc đăng nhập của tài khoản người dùng như có hay không người dùng phải đổi mật khẩu sau lần đăng nhập tiếp theo, hay người dùng không được thay đổi mật khẩu đã thiết lập, mật khẩu không bị hết hạn. Chúng ta có thể tắt hay dừng một tài khoản nào đó. Mục cuối cùng thể hiện tài khoản đang bị tạm khóa, nguyên nhân có thể vì người dùng nhập sai mật khẩu quá số lần cho phép.



Quản lý các nhóm người dùng trong mục Groups cũng tương tự như quản lý tài khoản người dùng. Nghĩa là ta có thể thêm, xóa, điều chỉnh các nhóm.



Windows PowerShell sử dụng lệnh `Get-LocalUser` để liệt kê danh sách người dùng có trong hệ thống. Kết quả xuất ra với cột `Name` là tên tài khoản, cột `Enabled` mô tả tài khoản có hoạt động hay không và cột `Description` là thông tin thêm mô tả về tài khoản.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> Get-LocalUser

Name                Enabled Description
----                -
Administrator      False  Built-in account for administering the co
cindy               True
DefaultAccount     False  A user account managed by the system.
devan               True
Guest               False  Built-in account for guest access to the
sarah               True
victor              True
```

Lệnh `Get-LocalGroup` dùng để liệt kê nhóm người dùng. Kết quả được thể hiện với hai cột là tên nhóm và mô tả về nhóm đó.

```
PS C:\Users\cindy> Get-LocalGroup

Name                Description
----                -
Access Control Assistance Operators Members of this group can remotely query authorization
Administrators       Administrators have complete and unrestricted access t
Backup Operators     Backup Operators can override security restrictions fo
Cryptographic Operators Members are authorized to perform cryptographic operat
Distributed COM Users Members are allowed to launch, activate and use Distri
Event Log Readers    Members of this group can read event logs from local m
Guests               Guests have the same access as members of the Users gr
Hyper-V Administrators Members of this group have complete and unrestricted a
IIS_IUSRS            Built-in group used by Internet Information Services.
Network Configuration Operators Members in this group can have some administrative pri
Performance Log Users Members of this group may schedule logging of performa
Performance Monitor Users Members of this group can access performance counter o
Power Users          Power Users are included for backwards compatibility a
Remote Desktop Users Members in this group are granted the right to logon m
Remote Management Users Members of this group can access WMI resources over ma
Replicator           Supports file replication in a domain
System Managed Accounts Group Members of this group are managed by the system.
Users                Users are prevented from making accidental or intentio
```

Lệnh `Get-LocalGroupMember` dùng để liệt kê nhóm người dùng. Kết quả được thể hiện với hai cột là tên nhóm và mô tả về nhóm đó.

2. Quản lý mật khẩu

Cách thức quản lý mật khẩu

Theo mặc định, Windows NT 4.0, Windows 2000, Windows XP và Windows Server 2003 không lưu trữ mật khẩu người dùng ở dạng bản rõ. Thay vào đó, mật khẩu được lưu trữ bằng hai cách biểu diễn mật khẩu khác nhau, thường được gọi là "hàm băm". Đầu tiên, hàm băm của LAN Manager (LM), kém an toàn hơn nhiều so với thứ hai, hàm băm NTLM. Lý do lưu trữ cả hai bản đại diện là để tương thích ngược với các ứng dụng và hệ điều hành cũ hơn như Windows 98.

Về mặt kỹ thuật, hàm băm LM không phải là một hàm băm. Nó được thực hiện bằng cách chuyển đổi tất cả các ký tự chữ thường trong mật khẩu thành chữ hoa, đặt mật khẩu bằng NULL ký tự cho đến khi nó dài chính xác 14 ký tự, chia mật khẩu thành hai đoạn 7 ký tự, sử dụng từng đoạn riêng biệt làm khóa DES để mã hóa một chuỗi cụ thể, nối hai văn bản mật mã thành một chuỗi 128 bit và lưu trữ kết quả.

Do thuật toán được sử dụng để tạo ra băm LM, nên băm rất dễ bị phá vỡ. Hàm băm NTLM còn được gọi là mã băm Unicode vì nó hỗ trợ bộ ký tự Unicode đầy đủ. Hàm băm NTLM được tính toán bằng cách lấy mật khẩu văn bản và tạo mã băm MD4 của nó. Hàm băm MD4 là những gì thực sự được lưu trữ trong cơ sở dữ liệu Active Directory hoặc cơ sở dữ liệu SAM cục bộ. Hàm băm NTLM có khả năng chống lại các cuộc tấn công vét cạn hơn nhiều so với hàm băm LM.

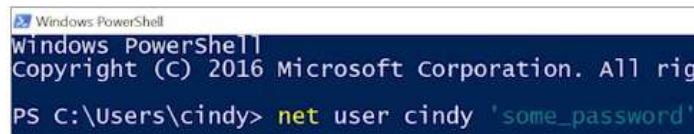
Cập nhật mật khẩu

Để thay đổi mật khẩu của người dùng trên PowerShell, ta sử dụng lệnh `net`. Cú pháp lệnh `net` cho phép gõ tường minh mật khẩu trên câu lệnh. Tuy nhiên, việc này gây rủi ro bảo mật nếu có người khác xung quanh. Do đó, lệnh `net` sử dụng dấu hoa thị (dấu `*`) để người dùng gõ mật khẩu ở chế độ không thể hiện trên màn hình. Ngoài ra, chức năng yêu cầu người dùng phải đổi mật khẩu sau khi đăng nhập được thể hiện qua tham số `/logonpasswordchg:yes`

```
net user user_name new_password  
net user user_name *
```

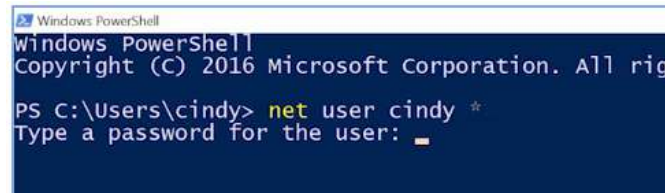


```
net user user_name /logonpasswordchg:yes
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> net user cindy 'some_password'
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> net user cindy *
Type a password for the user: 
```

Cách đặt mật khẩu an toàn

Người dùng thường có nhiều tài khoản máy tính khác nhau. Để dễ nhớ mật khẩu, họ thường sử dụng các mật khẩu giống nhau hoặc gần giống nhau. Thậm chí, họ sẽ chọn một mật khẩu rất đơn giản và dễ nhớ, chẳng hạn như ngày sinh của họ, tên cha mẹ hay người thân. Những mật khẩu ngắn và đơn giản tương đối dễ dàng để những kẻ tấn công xác định. Một số phương pháp phổ biến mà kẻ tấn công sử dụng để phát hiện ra mật khẩu như:

- Đoán: kẻ tấn công cố gắng đăng nhập bằng tài khoản của người dùng bằng cách đoán liên tục các từ và cụm từ có khả năng xảy ra như tên, địa chỉ, ngày sinh người thân của họ.
- Tấn công từ điển: kẻ tấn công sử dụng một tập tin chứa các từ và thử các cách khác nhau để ghép các từ đó thành mật khẩu.
- Tấn công vét cạn: kẻ tấn công sử dụng một chương trình tự động tạo ra các giá trị băm hoặc mã hóa cho tất cả các mật khẩu có thể có và so sánh chúng với các giá trị trong tập tin mật khẩu.

Mỗi phương pháp tấn công này có thể bị làm chậm đáng kể hoặc thậm chí bị đánh bại thông qua việc sử dụng mật khẩu mạnh. Mật khẩu mạnh là mật khẩu bao gồm các ký tự từ ít nhất ba trong số năm nhóm sau đây: ký tự chữ cái viết thường, ký tự chữ cái viết hoa, số, ký tự biểu tượng, ký tự Unicode.

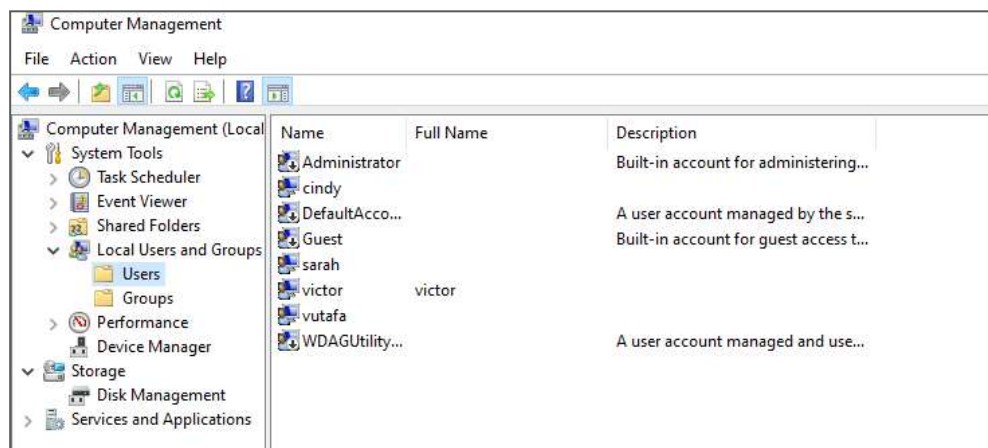
Tuy nhiên, mật khẩu cũng cần phải dễ dàng ghi nhớ bởi người dùng vì việc quên mật khẩu có thể gây nhiều phiền toái. Để có thể đặt mật khẩu dễ nhớ, chúng ta có thể đặt một câu có ý nghĩa với các ký tự thuộc ít nhất 3 trong số 5 nhóm trên và độ dài trên 14 ký tự. Mật khẩu càng dài thì càng khó phá.

Người dùng cũng nên thay đổi mật khẩu thường xuyên. Mặc dù mật khẩu dài và mạnh khó phá hơn nhiều so với mật khẩu ngắn và đơn giản, chúng vẫn có thể bị bẻ khóa. Kẻ tấn công có đủ thời gian và khả năng tính toán theo ý mình cuối cùng có thể phá vỡ bất kỳ mật khẩu nào. Nói chung, mật khẩu nên được thay đổi trong vòng 42 ngày và mật khẩu cũ không bao giờ được sử dụng lại.

3. Quản lý tài khoản người dùng

Thêm và xóa người dùng trên Windows

Trong Windows, ta có thể quản lý các tài khoản người dùng trong mục Users của phần Local Users and Groups (Computer Management). Các tài khoản có thể được thêm, xóa, điều chỉnh, thiết lập mật khẩu nếu chúng ta đang đăng nhập với quyền quản trị hệ thống.

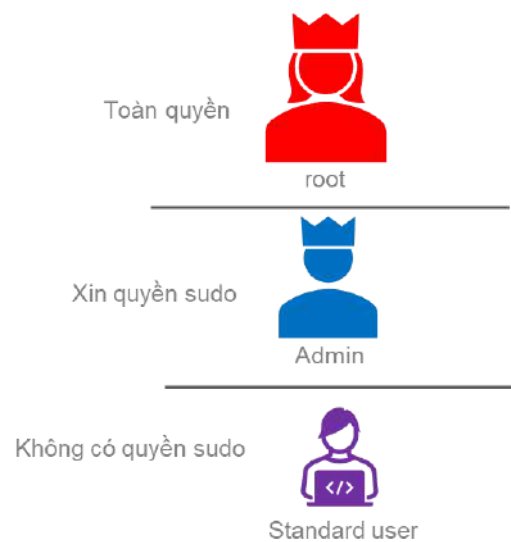


Thêm hay xóa người dùng trong PowerShell cũng được thực hiện qua lệnh net nhưng thêm các tham số /add và /del tương ứng.

```
net user user_name password /add /logonpasswordchg:yes
net user user_name /del
```

Thêm và xóa người dùng trên Linux

Các hệ điều hành thuộc nhóm Linux có thêm một tài khoản đặc biệt gọi là root, được tạo sẵn khi mới cài đặt Linux. Tài khoản này có toàn quyền đối với hệ thống, là một siêu người dùng (superuser). Điều này tương tự như quản trị viên nhưng trong Linux, tài khoản quản trị viên khi tác động đến hệ thống, phải yêu cầu đặc quyền qua lệnh sudo, viết tắt của từ superuser do hay substitute user do. Thông thường việc yêu cầu này chỉ đòi hỏi nhập mật khẩu mỗi lần cấu hình hệ thống. Việc này nhằm giúp các tài khoản quản trị tránh vô tình thực hiện các hành động nguy hiểm đến hệ thống.



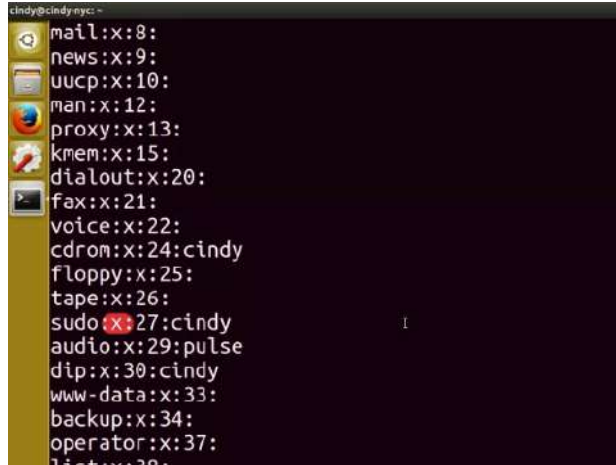
Lệnh sudo có nhiều chức năng, tùy thuộc vào các tham số của lệnh. Về cơ bản, lệnh sudo giúp thực thi các đặc quyền của hệ thống cũng như chuyển đổi qua lại giữa người dùng trong hệ thống.

sudo command

```
cindy@cindy-nyc: ~  
cindy@cindy-nyc:~$ cat /etc/sudoers  
cat: /etc/sudoers: Permission denied  
cindy@cindy-nyc:~$ sudo cat /etc/sudoers
```

Để xem danh sách nhóm người dùng trên Linux, ta chỉ cần đọc tập tin `/etc/group`. Mỗi nhóm được thể hiện bởi tên nhóm, ký tự đại diện mật khẩu, mã group, và danh sách người sử dụng thuộc nhóm.

```
cat /etc/group
```



```
cindy@cindy-nyc:~$ cat /etc/group
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:cindy
floppy:x:25:
tape:x:26:
sudo:x:27:cindy
audio:x:29:pulse
dip:x:30:cindy
www-data:x:33:
backup:x:34:
operator:x:37:
lp:x:38:
```

Trong khi đó, danh sách người dùng được đặt trong tập tin `/etc/passwd`. Tập tin cũng chứa các thông tin về các tiến trình và tài khoản chạy tiến trình đó. Mỗi người dùng gồm có thông tin tên tài khoản, ký tự đại diện mật khẩu, mã định danh người dùng, và một số thông tin khác.

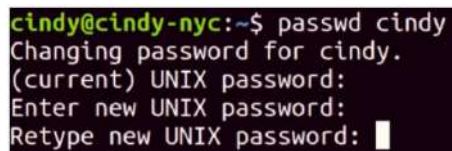
```
cat /etc/passwd
```



```
cindy@cindy-nyc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

Mật khẩu được thay đổi sử dụng lệnh `passwd`. Khi có tham số `-e`, nghĩa là chúng ta muốn mật khẩu hết hạn, người dùng phải đổi mật khẩu sau khi đăng nhập lần kế tiếp.

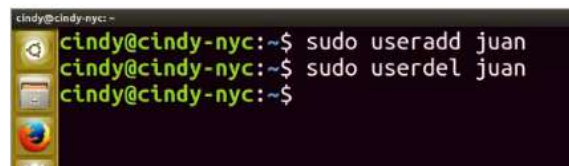
```
passwd user_name  
passwd -e user_name
```



```
cindy@cindy-nyc:~$ passwd cindy  
Changing password for cindy.  
(current) UNIX password:  
Enter new UNIX password:  
Retype new UNIX password: █
```

Để thêm người dùng vào hệ thống, ta sử dụng lệnh `useradd`. Sau khi người dùng được tạo, ta nên sử dụng lệnh cập nhật mật khẩu để thiết lập bảo mật cho tài khoản. Khi muốn xóa người dùng, sử dụng lệnh `userdel`.

```
useradd user_name  
userdel user_name
```

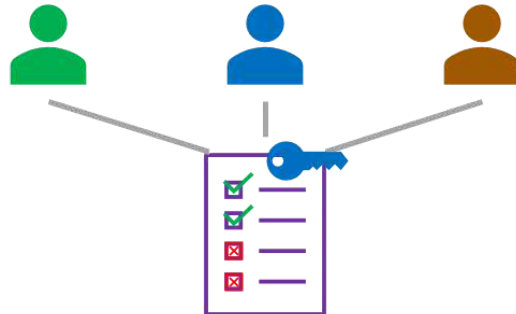


```
cindy@cindy-nyc:~$ sudo useradd juan  
cindy@cindy-nyc:~$ sudo userdel juan  
cindy@cindy-nyc:~$
```

4. Quyền truy cập thư mục và tập tin

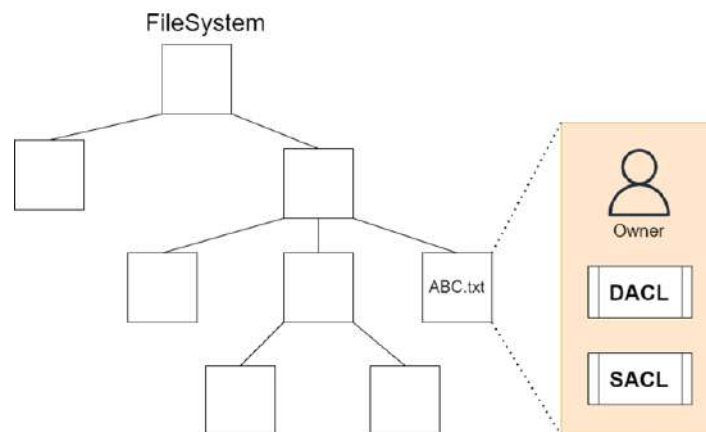
Giới thiệu ACL

Trong các hệ điều hành, một danh sách các quy tắc quy định các quyền truy cập tài nguyên hệ thống đối với người dùng được gọi là ACL (Access Control List). Mỗi quy tắc thường bao gồm một đối tượng và mô tả các quyền truy cập. Ví dụ, một tập tin có cấu hình ACL (Cindy: đọc, viết; Victor: đọc, Sam: đọc, viết, thực thi) nghĩa là Cindy có quyền đọc và viết tập tin này nhưng Victor chỉ có thể đọc tập tin, và Sam có các quyền đọc, viết, thực thi.



(Cindy: đọc, viết; Victor: đọc; Sam: đọc, viết, thực thi)

Đối với tập tin và thư mục, có hai danh sách thể hiện cụ thể các quyền gồm DACL và SACL. Danh sách DACL quy định người nào được truy cập tập tin và các quyền truy cập cụ thể. Trong khi đó, SACL ghi lại lịch sử truy cập tập tin của từng người. Mỗi tập tin hay thư mục đều có một người sở hữu và một hay nhiều DACL.

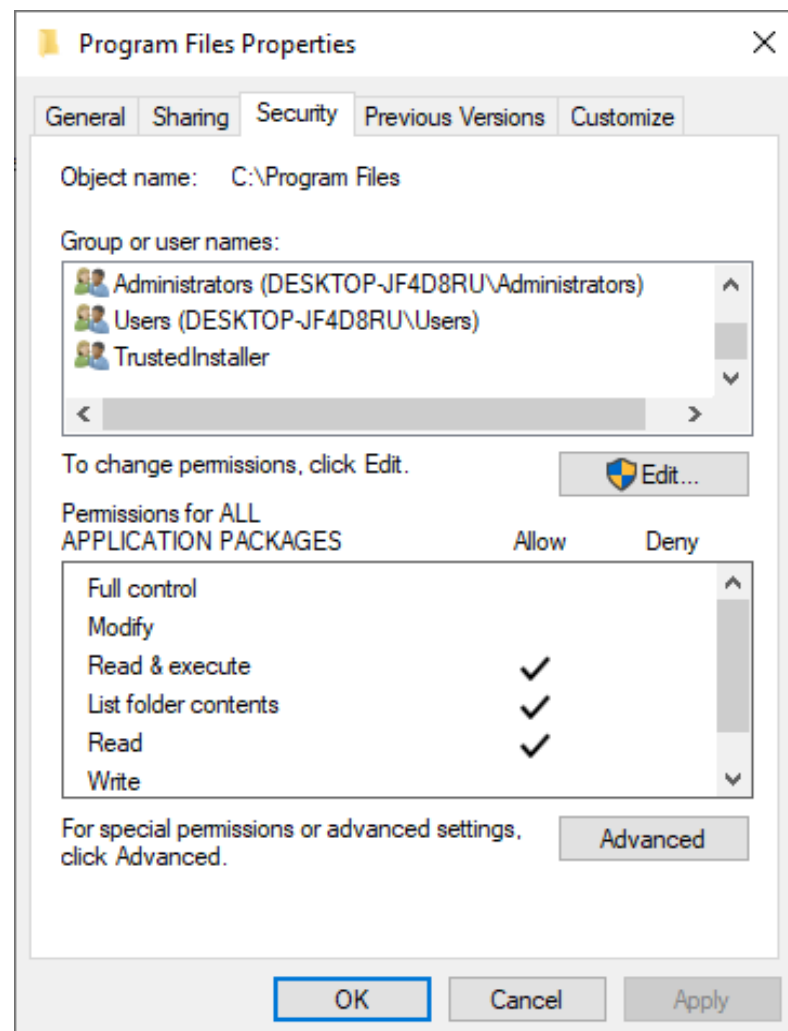


Các quyền khác nhau trên Windows

Mỗi tập tin hay thư mục có một số loại quyền truy cập như quyền đọc, viết, thực thi. Tuy nhiên, mỗi hệ điều hành sẽ có thêm các loại quyền cụ thể hơn. Ví dụ trong hệ điều hành Windows, ta có thêm các quyền như đọc và thực thi,

quyền điều chỉnh, và toàn quyền. Quyền đọc cho phép nhìn thấy tập tin/thư mục và đọc nội dung của chúng. Quyền viết cho phép thay đổi nội dung tập tin; đối với thư mục, quyền viết cho phép tạo thư mục con hay tập tin bên trong. Trong khi đó, quyền thực thi cho phép thực thi nếu tập tin là một chương trình chạy được.

Quyền truy cập trên Windows được thể hiện chi tiết trong cửa sổ Properties của mỗi tập tin/thư mục. Cửa sổ này được bố trí gồm hai phần chính là danh sách người dùng và nhóm, các quyền của từng người dùng/nhóm tương ứng. Chúng ta có thể thay đổi các quyền truy cập ngay trong cửa sổ này.



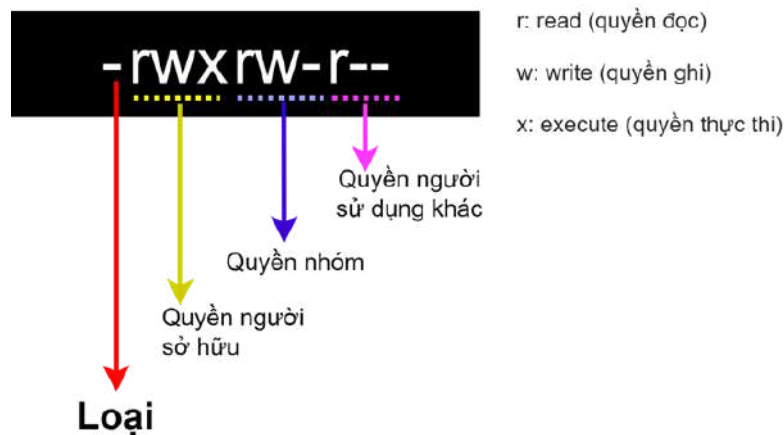
Các quyền khác nhau trên Linux

Khi dùng lệnh `ls -l` trong linux, mỗi dòng kết quả trả về mô tả thông tin về tập tin và thư mục.

```
cindy@cindy-nyc:~$ ls -l ~/my_file
-rwxrw-r-- 1 cindy cool_group 0 Oct  9 17:48 /home/cindy/my_file
```

Trong đó 10 ký tự đầu tiên thể hiện các quyền truy cập. Cụ thể ký tự đầu tiên mô tả loại của đối tượng, nếu là tập tin, ký tự là dấu gạch ngang, nếu là thư mục thì ký tự là chữ d. Bộ 3 ký tự tiếp theo mô tả các quyền của người sở hữu tập tin/thư mục này.

Bộ 3 ký tự thứ hai mô tả quyền của nhóm mà tập tin hay thư mục thuộc về và bộ 3 ký tự cuối cùng là quyền của các người sử dụng khác. Mỗi bộ ba bao gồm 3 ký tự thể hiện có hay không có quyền đọc, viết và thực thi.



Xem và thay đổi các quyền truy cập

Trong Windows PowerShell, để xem và cập nhật các quyền truy cập đối với tập tin/thư mục, ta sử dụng lệnh `icacls`. Lệnh này có nhiều loại tham số và ký hiệu.

icacls file_folder

```
Windows PowerShell
PS C:\Users\vutafa> icacls .\Desktop\
.\Desktop\ NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
            BUILTIN\Administrators:(I)(OI)(CI)(F)
            DESKTOP-JF4D8RU\vutafa:(I)(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\vutafa>
```

Trong Bash, ta sử dụng lệnh `chmod` để cập nhật quyền truy cập đối với tập tin/thư mục. Trong lệnh `chmod`, tham số mode có hai cách để ghi. Một là sử dụng chuỗi ký tự, hai là sử dụng số. Mỗi cách đều có ưu và nhược điểm riêng mà trong quá trình sử dụng chúng ta có thể tự đánh giá được.

chmod mode file_name

```
cindy@cindy-nyc:~$ chmod u+rx my_cool_file
cindy@cindy-nyc:~$ chmod g+rw my_cool_file
cindy@cindy-nyc:~$ chmod o+r my_cool_file
```

Đối với cách sử dụng chuỗi ký tự, mode sẽ gồm 3 thành phần là đối tượng, ký tự thêm hay bỏ bớt và quyền truy cập. Trong thành phần đối tượng, ký tự `u` đại diện cho người sở hữu, `g` cho nhóm và `o` cho người sử dụng khác. Chúng ta có thể cùng lúc mô tả cho nhiều nhóm đối tượng như `ug`, `uo` hay `ugo`. Thành phần thứ hai thể hiện bằng dấu cộng, nghĩa là bổ sung thêm quyền; dấu trừ, nghĩa là bỏ bớt quyền; và bằng, nghĩa là gán từng đó quyền. Thành phần cuối cùng là một chuỗi được cấu thành từ 3 ký tự `r`, `w`, `x` tương ứng với các quyền đọc, viết và thực thi.

```
cindy@cindy-nyc:~$ chmod 754 my_cool_file
```

Khi mô tả mode bằng số, chúng được thể hiện bởi ba con số. Trong một số trường hợp đặc biệt, nó có thể là bốn con số, nhưng chúng ta sẽ bàn trường hợp này sau. Số thứ nhất trong dãy 3 số mô tả quyền của người sở hữu. Trong hình ví dụ là 7. Số thứ hai mô tả quyền của nhóm, trong ví dụ là 5. Và số thứ ba

thể hiện quyền của người dùng khác như số 4 trong hình ví dụ. Mỗi số có giá trị từ 0 đến 7 theo giá trị đếm của dãy 3 bit ứng với thứ tự quy ước của đọc, viết và thực thi. Ví dụ, nếu chúng ta muốn thiết lập quyền đọc và thực thi, không cho phép quyền viết, chuỗi biểu diễn là r-x tương đương với dãy bit 101 trong nhị phân. Ta quy đổi dãy bit 101 thành hệ đếm 10 sẽ được giá trị 5. Như vậy, số 5 sẽ mô tả quyền đọc, thực thi nhưng không viết.

4	2	1
1	0	1
r	w	x

$$r-x \leftrightarrow 101_2 \leftrightarrow 4 + 1 = 5_{10}$$

Lệnh chown và lệnh chgrp giúp chuyển đổi người sở hữu và chuyển đổi nhóm mà tập tin hay thư mục đó thuộc về.

```
cindy@cindy-nyc:~$ sudo chown devan my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool_file
-rwxr-xr-- 1 devan cool_group 0 Oct 9 17:49 my_cool_file
cindy@cindy-nyc:~$ sudo chgrp best_group_ever my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool_file
-rwxr-xr-- 1 devan best_group_ever 0 Oct 9 17:49 my_cool_file
```

Quyền truy cập đặc biệt

Ngoài các quyền cơ bản đã được trình bày, Windows còn định nghĩa thêm các quyền đặc biệt khác ví dụ như quyền xem thuộc tính của tập tin, quyền đọc các thuộc tính mở rộng, v.v...



Linux cũng có một số quyền đặc biệt như SetUID cho phép chạy tập tin như người sở hữu. Để thiết lập SetUID, sử dụng chmod với số 4 được thêm vào trước dãy 3 số như đã đề cập trong phần trước. Nếu biểu diễn dưới dạng chuỗi ký tự là u+s. Trong khi đó, SetGID cho phép chạy tập tin như thành viên của nhóm. SetGID sử dụng giá trị 2. Ngoài ra, chế độ sticky bit cho phép bất kỳ ai cũng có thể viết đến tập tin/thư mục nhưng không thể xóa chúng. Sticky bit sử dụng giá trị 1.

```
cindy@cindy-nyc:~$ sudo chmod u+s my_cool_file
[sudo] password for cindy:
cindy@cindy-nyc:~$ sudo chmod 4755 my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool_file
-rwsr-xr-x 1 devan best_group_ever 0 Oct  9 17:49 my_cool_file
cindy@cindy-nyc:~$ sudo chmod 2755 my_cool_file
cindy@cindy-nyc:~$ ls -l my_cool_file
-rwxr-sr-x 1 devan best_group_ever 0 Oct  9 17:49 my_cool_file
cindy@cindy-nyc:~$ sudo chmod 1755 my_folder/
cindy@cindy-nyc:~$ ls -ld my_folder/
drwxr-xr-t 2 cindy cindy 4096 Oct  5 16:14 my_folder/
cindy@cindy-nyc:~$
```

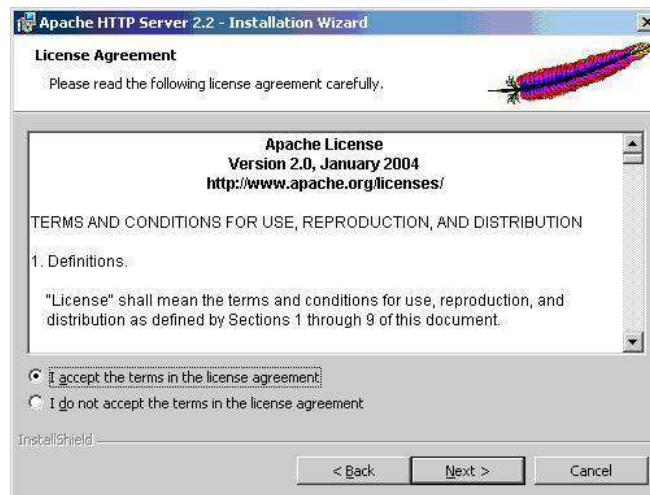
Bài đọc 4: Cài Đặt và Quản Lý Phần Mềm

1. Các gói phần mềm

Các dạng gói phần mềm trên Windows

Khi phát hành phần mềm đến người sử dụng, các nhà phát triển thường đóng gói các tập tin hay tài nguyên cần thiết để chạy một nhiệm vụ nào đó, thành một tập tin duy nhất. Điều này giúp cho quá trình phân phối trở nên thuận tiện hơn. Ngoài ra, việc đóng gói còn tích hợp các công cụ hỗ trợ cài đặt ứng dụng vào máy tính người dùng. Mỗi nhà phát triển cũng có những cách thức đóng gói khác nhau.

Phần mềm trên Windows thường được đóng gói dưới dạng tập tin .exe. Tập tin này chứa các hướng dẫn để máy tính thực thi các nhiệm vụ xác định. Trong Windows cũng có một loại tập tin có đuôi là .msi. Đây là tập tin hướng dẫn trình cài đặt Windows cách thức cài đặt, cập nhật và gỡ bỏ ứng dụng khỏi hệ thống. Nếu đã từng cài đặt các gói phần mềm .msi, chúng ta sẽ thấy các màn hình cài đặt khá tương tự nhau.

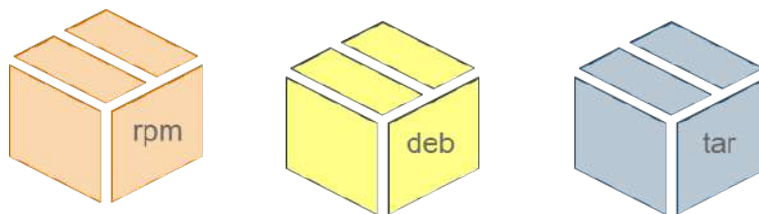


Như vậy, về cơ bản có 2 loại tập tin liên quan đến cài đặt phần mềm trên Windows. Phần mềm đóng gói với đuôi msi thường chỉ cần một số câu lệnh

khởi chạy Windows Installer để thực thi tập tin đó. Tập tin msi sau đó tự quản lý các bản ghi chép và cài đặt phần mềm. Tuy nhiên, các bản đóng gói cần tuân thủ nghiêm ngặt các quy tắc mà một phần mềm được cài đặt. Trong khi đó, bộ cài đặt tùy chỉnh và độc lập cần phải chứa nhiều lệnh để hướng dẫn cụ thể để hệ điều hành biết cách thực hiện. Điểm lợi của cách này là tăng tính linh hoạt của quá trình cài đặt, cập nhật và gỡ bỏ phần mềm.

Các dạng gói phần mềm trên Linux

Trên Linux, mỗi bản phân phối có các cách thức đóng gói phần mềm khác nhau như gói .rpm được sử dụng phổ biến trên Red Hat, Fedora. Gói .deb phổ biến trên Ubuntu, Debian. Gói ebuild của Gentoo, v.v...



Đối với gói .deb, lệnh dpkg được sử dụng để cài đặt, gỡ bỏ, cấu hình phần mềm trên các bản phân phối Linux như Ubuntu. Tham số để chỉ định cài đặt là -i.

```
cindy@cindy-nyc: ~  
cindy@cindy-nyc:~$ sudo dpkg -i atom-amd64.deb  
Selecting previously unselected package atom.  
(Reading database ... 176090 files and directories currently installed.)  
Preparing to unpack atom-amd64.deb ...  
Unpacking atom (1.21.0) ...
```

Để gỡ cài đặt, sử dụng tham số -r.

```
cindy@cindy-nyc:~$ sudo dpkg -r atom
(Reading database ... 183451 files and directories currently installed.)
Removing atom (1.21.0) ...
Processing triggers for gnome-menus (3.13.3-6ubuntu3.1) ...
Processing triggers for desktop-file-utils (0.22-1ubuntu5.1) ...
Processing triggers for bamfdaemon (0.5.3~bzip0+16.04.20160824-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.59ubuntu1) ...
cindy@cindy-nyc:~$
```

Tham số -l để liệt kê tất cả các gói phần mềm Debian đã cài đặt trong máy.

```
cindy@cindy-nyc:~$ dpkg -l | grep atom
ii atom 1.21.0
ditor for the 21st Century.
ii libatomic1:amd64 5.4.0-6ubuntu1~16.04.5
providing __atomic built-in functions
ii libxcb-util1:amd64 0.4.0-0ubuntu3
for X C Binding -- atom, aux and event
```

2. Đóng gói phần mềm với công cụ nén

Thay vì phải tạo ra những gói phần mềm với trình cài đặt, một cách đơn giản hơn là tập hợp các tập tin như mã nguồn, tập tin lỗi, v.v... và gói chúng lại thành một tập tin duy nhất. Quá trình này gọi là lưu trữ gói phần mềm (package archive /ar.kai/). Thông thường quá trình gói cũng sẽ nén tập tin lại với kích thước nhỏ hơn. Trên Windows, một số loại gói phổ biến như zip, rar, và tar. Còn trên Linux, các loại gói phổ biến là tar, tgz, gz, zip.

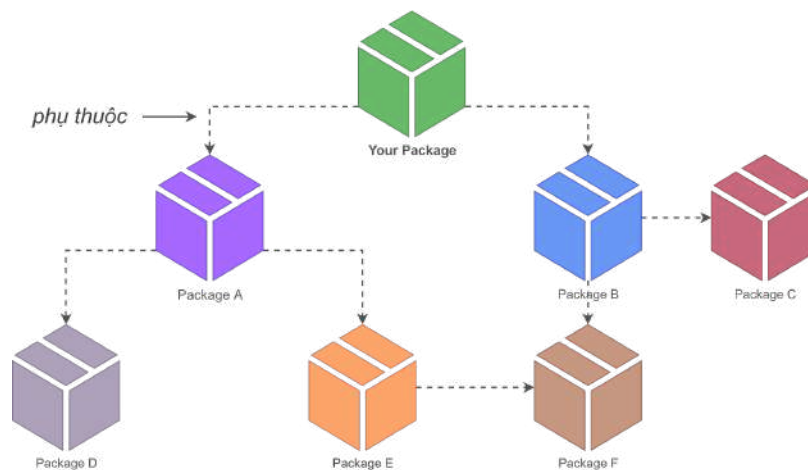
Để đóng gói và mở gói lưu trữ phần mềm, ta có rất nhiều công cụ từ miễn phí đến có phí. Trong số đó, 7zip là một phần mềm miễn phí đang được sử dụng phổ biến. Bên cạnh đó, bản thân PowerShell hay Bash cũng tích hợp sẵn các công cụ để thực hiện việc này. Ví dụ, lệnh Compress-Archive trong Powershell hay lệnh tar trong Bash.

Compress-Archive -Path source dest

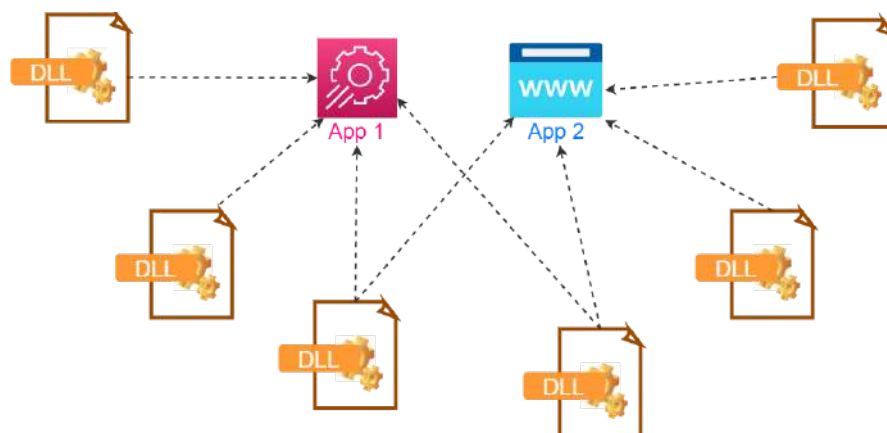
```
PS C:\Users\cindy> Compress-Archive -Path C:\Users\cindy\Desktop\CoolFiles\ ~\Desktop\CoolArchive.zip
```


3. Phụ thuộc gói phần mềm

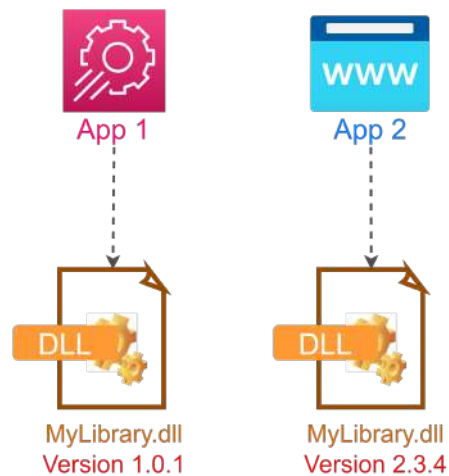
Trong quá trình sản xuất phần mềm, các nhà phát triển thường tận dụng các gói phần mềm khác để giúp rút ngắn thời gian phát triển do không cần viết lại mã nguồn cho các chức năng đã có. Bên cạnh đó, khi nhiều gói phần mềm được sử dụng chung giữa các phần mềm thì hệ điều hành sẽ tiết kiệm tài nguyên hơn, vì chỉ cần tải lên một lần. Từ đó ra đời khái niệm phụ thuộc gói phần mềm, package dependency.



Thư viện liên kết động DLL là những gói chương trình trên Windows có thể được sử dụng bởi các chương trình khác. Trình cài đặt Windows cũng quản lý các gói tin phụ thuộc này để đảm bảo các chương trình có thể sử dụng.



Trong Windows, mỗi thư viện DLL có thể có nhiều phiên bản khác nhau. Điều này có thể xảy ra vấn đề, một số ứng dụng chỉ tương thích phiên bản DLL này mà không tương thích bản DLL khác. Microsoft đã giải quyết vấn đề này bằng công nghệ Side-by-Side assembly, viết tắt là SxS. Cốt lõi bên dưới công nghệ này nằm ở chỗ Windows chứa nhiều phiên bản khác nhau của một DLL và tải phiên bản phù hợp với ứng dụng đang thực hiện.



Trên Linux, các gói phụ thuộc có thể là các gói phần mềm khác hoặc có thể là một thứ gì đó giống như các thư viện được chia sẻ. Thư viện chia sẻ trên Linux tương tự như DLL trên Windows. Các trình quản lý gói giúp việc cài đặt và gỡ bỏ phần mềm dễ dàng hơn, bao gồm cả việc cài đặt các gói phụ thuộc.

4. Quản lý gói phần mềm

Đối với việc cài đặt các gói phần mềm theo cách trước đây, chúng ta phải tải gói phần mềm và sử dụng bộ cài đặt của hệ điều hành để thực hiện. Tuy nhiên, cách này có thể gặp một số bất lợi như một số phần mềm phải cài gói phụ thuộc trước khi cài gói mong muốn hay việc cập nhật phải thực hiện gỡ bỏ ứng dụng trước đó, hay không tự động cập nhật khi có phiên bản mới, thậm chí người dùng có thể cài 2 phiên bản khác nhau của cùng một phần mềm, v.v... Đương nhiên, điều này còn lệ thuộc vào cách các phần mềm hỗ trợ người dùng

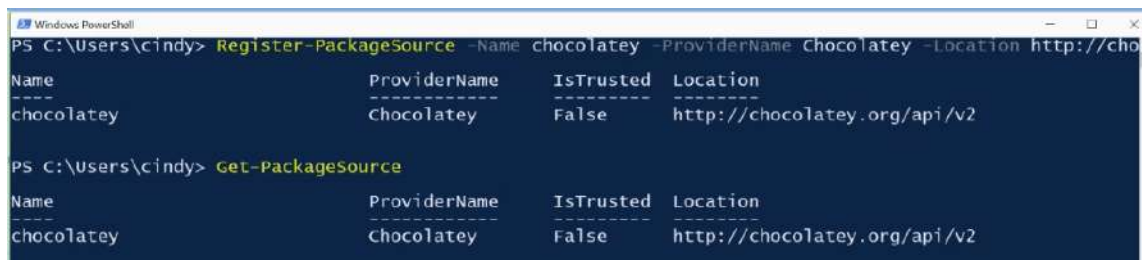
đến mức nào. Một giải pháp được đề xuất là sử dụng bộ quản lý gói phần mềm, package manager. Công cụ này giúp tổ chức, cài đặt, cập nhật, cấu hình và gỡ bỏ phần mềm và gói phụ thuộc một cách chặt chẽ.

Từ đầu năm 2020, Microsoft phát hành bộ quản lý gói phần mềm được gọi là winget. Trước đó, mọi người thường sử dụng các bộ quản lý từ các nhà phát triển khác, nổi tiếng trong đó có Chocolatey, Scoop, AppGet. Trên Linux, bộ quản lý gói phần mềm APT đơn giản hóa quá trình quản lý phần mềm dựa trên Debian như hệ điều hành Ubuntu. Bộ quản lý phần mềm này tự động hóa việc truy cập, cấu hình và cài đặt các gói phần mềm, từ các tập tin được biên dịch trước hoặc bằng cách biên dịch mã nguồn.

Kho chứa gói phần mềm là các máy chủ được tổ chức để lưu trữ các phần mềm trên Internet. Tùy thuộc vào kho chứa nhưng nhìn chung các kho chứa này sẽ thường xuyên cập nhật bản mới của các gói phần mềm, kiểm tra các gói phụ thuộc, bổ sung các gói mới, v.v... Bộ quản lý gói phần mềm trên máy tính người dùng thường liên kết đến các kho chứa này để tải và cài đặt các gói cần thiết.

Chocolatey là một kho chứa các gói phần mềm trên Windows để người dùng có thể tải và sử dụng. Đây là kho phần mềm được phát triển bởi bên thứ ba. Trước khi truy cập kho này, chúng ta cần đăng ký với lệnh Register-PackageSource. Sau khi đăng ký, ta có thể kiểm tra lại bằng lệnh Get-PackageSource.

```
Register-PackageSource -Name chocolatey -ProviderName  
Chocolatey -Location http://chocolatey.org/api/v2
```



```
Windows PowerShell
PS C:\Users\cindy> Register-PackageSource -Name chocolatey -ProviderName Chocolatey -Location http://chocolatey.org/api/v2

Name      ProviderName  IsTrusted  Location
-----
chocolatey Chocolatey     False      http://chocolatey.org/api/v2

PS C:\Users\cindy> Get-PackageSource

Name      ProviderName  IsTrusted  Location
-----
chocolatey Chocolatey     False      http://chocolatey.org/api/v2
```

Sau khi đã đăng ký kho chứa phần mềm, ta có thể sử dụng lệnh Find-Package để tìm kiếm gói phần mềm và sử dụng lệnh Install-Package để cài. Lệnh Find-Package cũng cho phép xem các gói phụ thuộc của gói phần mềm. Ngoài các cách thức được trình bày ở đây, Find-Package còn có nhiều cách thức thực hiện khác, và đòi hỏi trả cứu thêm tài liệu liên quan.

Find-Package package -IncludeDependencies

```
PS C:\Users\cindy> Find-Package sysinternals -IncludeDependencies
```

Name	Version	Source	Summary
sysinternals	2017.9.12	chocolatey	sysinternals - utilities to help you ma
chocolatey-core.extension	1.3.1	chocolatey	Helper functions extending core choco f

Lệnh Install-Package dùng để cài đặt gói phần mềm. Nếu kho chứa chưa được chỉ định trước đó hoặc muốn thay đổi kho chứa phần mềm, ta cần thêm thuộc tính Source trong lệnh. Sau khi cài đặt, ta có thể sử dụng lệnh Get-Package để kiểm tra và lệnh Uninstall-Package để gỡ bỏ gói phần mềm.

Install-Package -Name package -Source repository

```
Windows PowerShell
PS C:\Users\cindy> Install-Package -Name sysinternals
```

The package(s) come(s) from a package source that is not marked as trusted.
Are you sure you want to install software from 'chocolatey'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y

Name	Version	Source	Summary
sysinternals	2017.9.12	chocolatey	sysinternals - utilities to hel

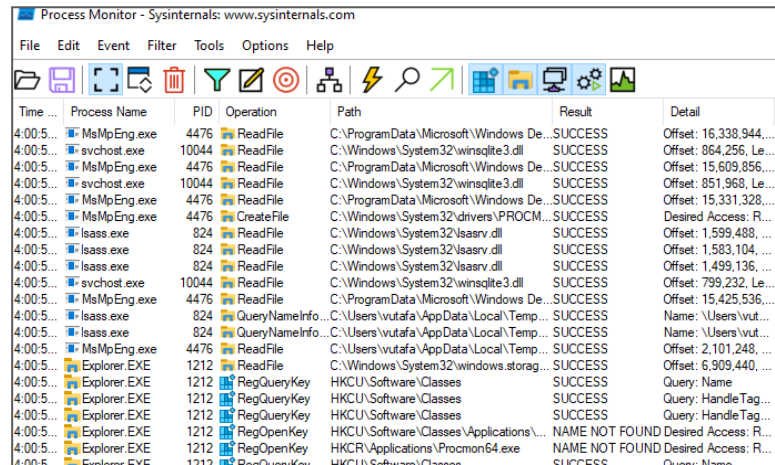
```
PS C:\Users\cindy> Get-Package -name sysinternals
```

Name	Version	Source	ProviderName
sysinternals	2017.9.12	C:\Chocolatey\lib\sysinternal...	Chocolatey

```
PS C:\Users\cindy> Uninstall-Package -Name sysinternals
```

Hầu hết các phần mềm phát hành trên Windows ở dạng mã nguồn đóng, nghĩa là chúng ta không thể thấy mã nguồn của ứng dụng. Do đó, việc theo dõi quá trình cài đặt của các gói phần mềm này thực sự không dễ dàng. Microsoft

phát triển một bộ công cụ gọi là Sysinternals để giúp theo dõi các hoạt động mà gói phần mềm tương tác đến hệ thống như các tập tin đã thực thi, các tiến trình liên quan đến chúng. Đối với gói MSI, do các gói này cần tuân thủ các quy tắc chặt chẽ để bộ cài đặt Windows có thể thực hiện nên chúng ta có thể dùng chương trình Orca để xem quá trình cài đặt, thậm chí có thể tạo và điều chỉnh quá trình này.



Time ...	Process Name	PID	Operation	Path	Result	Detail
4:00:5...	MsMpEng.exe	4476	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 16,338,944,...
4:00:5...	svchost.exe	10044	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 864,256, Le...
4:00:5...	MsMpEng.exe	4476	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,609,856,...
4:00:5...	svchost.exe	10044	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 851,968, Le...
4:00:5...	MsMpEng.exe	4476	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,331,328,...
4:00:5...	MsMpEng.exe	4476	CreateFile	C:\Windows\System32\drivers\PROC...	SUCCESS	Desired Access: R...
4:00:5...	lsass.exe	824	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1,599,488, ...
4:00:5...	lsass.exe	824	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1,583,104, ...
4:00:5...	lsass.exe	824	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1,499,136, ...
4:00:5...	svchost.exe	10044	ReadFile	C:\Windows\System32\winsqlite3.dll	SUCCESS	Offset: 799,232, Le...
4:00:5...	MsMpEng.exe	4476	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 15,425,536,...
4:00:5...	lsass.exe	824	QueryNameInfo...	C:\Users\vtutaf\AppData\Local\Temp...	SUCCESS	Name: \Users\vtut...
4:00:5...	lsass.exe	824	QueryNameInfo...	C:\Users\vtutaf\AppData\Local\Temp...	SUCCESS	Name: \Users\vtut...
4:00:5...	MsMpEng.exe	4476	ReadFile	C:\Users\vtutaf\AppData\Local\Temp...	SUCCESS	Offset: 2,101,248, ...
4:00:5...	Explorer.EXE	1212	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6,909,440, ...
4:00:5...	Explorer.EXE	1212	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
4:00:5...	Explorer.EXE	1212	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
4:00:5...	Explorer.EXE	1212	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
4:00:5...	Explorer.EXE	1212	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
4:00:5...	Explorer.EXE	1212	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
4:00:5...	Explorer.EXE	1212	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name

Trên Ubuntu, thông tin kho chứa được sử dụng bởi bộ quản lý gói phần mềm apt được đặt tại `/etc/apt/sources.list`. Trong tập tin này, chứa các đường dẫn URL và các thông tin về kho chứa của các gói phần mềm. Ngoài ra, trên Linux còn có một kho chứa khác, được gọi là PPA và được quản lý bởi máy chủ Launchpad. Kho chứa này chủ yếu dành cho các nhà phát triển phần mềm mã nguồn mở phân phối sản phẩm của họ. Tuy nhiên, người dùng cũng lưu ý khi sử dụng các gói chưa được kiểm tra bởi các bên có uy tín.

Trước khi cài đặt hay nâng cấp các gói phần mềm trên hệ điều hành Ubuntu, người dùng cần đảm bảo thông tin mới nhất về các gói phần mềm. Điều này được thực hiện qua lệnh `apt update`. Lưu ý, lệnh này không cài đặt hay nâng cấp phần mềm nào cả mà chỉ cập nhật thông tin về các gói phần mềm. Để có thể cài đặt và cập nhật, chúng ta cần thực hiện thêm các lệnh tiếp theo.

apt update

```
cindy@cindy-nyc: ~/Desktop
cindy@cindy-nyc:~/Desktop$ sudo apt update
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:4 http://dl.google.com/linux/chrome/deb stable Release [1,189 B]
Get:5 http://dl.google.com/linux/chrome/deb stable Release.gpg [819 B]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:7 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,388 B]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [364 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
26% [8 Packages store 0 B] [Waiting for headers] [Waiting for headers]
```

Khi đã có thông tin mới nhất về các gói phần mềm, ta có thể dùng lệnh apt upgrade để cập nhật tất các phần mềm đang có trong hệ thống.

apt upgrade

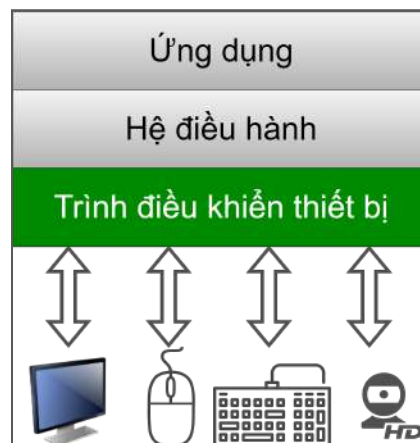
Để cài đặt gói phần mềm với apt, ta dùng lệnh apt install. Lệnh này cũng tự động tải các gói phụ thuộc mà phần mềm yêu cầu và hỏi chúng ta có muốn cài đặt chúng không. Với cách này, chúng ta đỡ tốn công để đi cài đặt từng gói phụ thuộc, thậm chí là các gói phụ thuộc của gói phụ thuộc.

apt install package

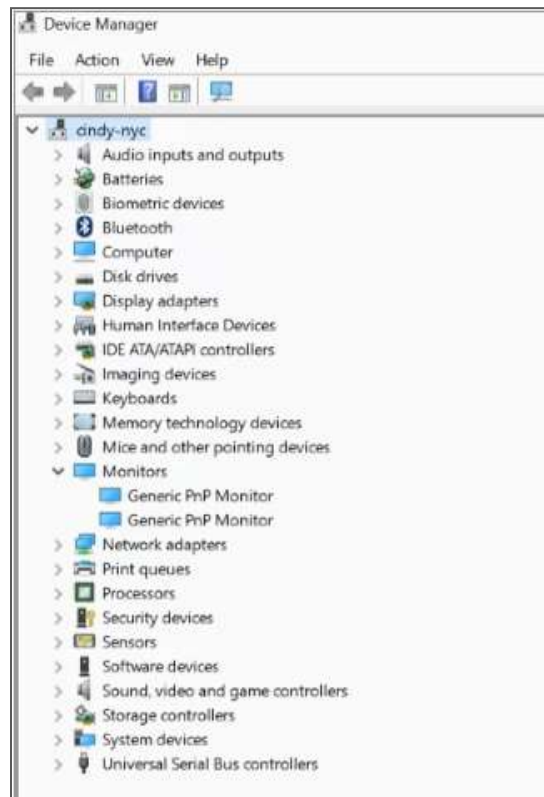
```
cindy@cindy-nyc: ~/Desktop
cindy@cindy-nyc:~/Desktop$ sudo apt install gimp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  gimp-data libamd2.4.1 libbabl-0.1-0 libblas-common libblas3 libcam
  libgfortran3 libgimp2.0 liblapack3 libsdl1.2debian libumfpack5.7.1
Suggested packages:
  gimp-help-en | gimp-help gimp-data-extras python-gobject-2-dbg pyt
The following NEW packages will be installed:
  gimp gimp-data libamd2.4.1 libbabl-0.1-0 libblas-common libblas3 l
  libgegl-0.3-0 libgfortran3 libgimp2.0 liblapack3 libsdl1.2debian l
  python-gtk2
0 upgraded, 18 newly installed, 0 to remove and 16 not upgraded.
Need to get 17.2 MB of archives.
```


5. Quản lý phần mềm thiết bị

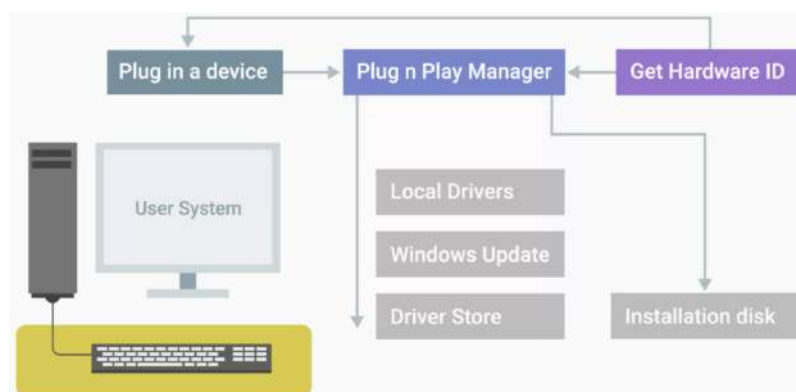
Một phần mềm đặc biệt trong hệ điều hành là trình điều khiển thiết bị (driver). Phần mềm này giúp hệ điều hành có thể giao tiếp với các thiết bị phần cứng để thực hiện các nhiệm vụ của người dùng.



Windows quản lý các driver qua một chương trình được gọi là trình quản lý thiết bị (Device Manager). Những thiết bị nào được nhận ra sẽ được gom vào các mục tương ứng. Những chức năng chính trong trình quản lý thiết bị như liệt kê danh sách các thiết bị, cài đặt thiết bị mới, gỡ bỏ hay cập nhật phiên bản mới của các driver.



Khi có thiết bị mới được cắm vào máy, Windows tự động phát hiện phần cứng mới này, sau đó tìm kiếm và cài đặt phần mềm thích hợp để quản lý nó. Các thiết bị phần cứng thường được nhà sản xuất gán một chuỗi ký tự đặc biệt được gọi là mã phần cứng. Mã này được hệ điều hành sử dụng để tìm kiếm driver phù hợp. Hệ điều hành thường bắt đầu từ những danh sách các thiết bị phổ biến mà nó đang có. Nếu danh sách này không chứa thiết bị phần cứng mới, nó sẽ đến những máy chủ trên Internet để mở rộng tìm kiếm. Chúng ta có thể chỉ định nơi để tìm kiếm driver hoặc chủ động để cài driver cho thiết bị này.



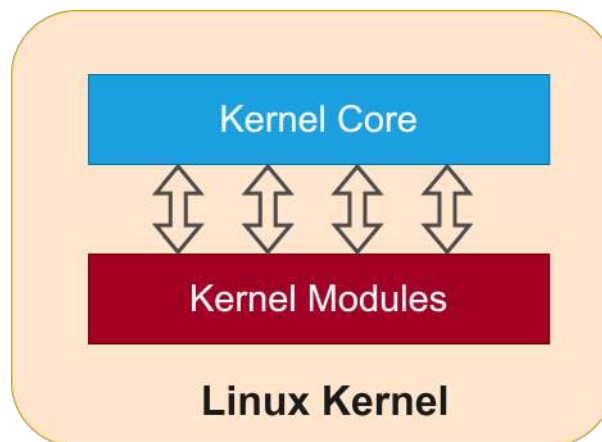
Mỗi thiết bị khi cắm vào máy chạy hệ điều hành Linux đều được xem như là một tập tin. Tập tin này được tạo trong thư mục /dev. Một số thiết bị như chuột, bàn phím có cách thức truyền nhận dữ liệu dưới dạng từng ký tự sẽ được đánh dấu bằng mã c ở đầu chuỗi mô tả quyền truy cập. Nếu thiết bị truyền nhận dữ liệu dưới dạng từng khối dữ liệu như ổ đĩa cứng, ổ USB sẽ được đánh mã b. Ngoài ra, một số loại thiết bị còn quy ước bắt đầu bằng chuỗi nhất định để dễ nhận biết. Ví dụ, các thiết bị lưu trữ như ổ cứng, ổ USB, thẻ nhớ sẽ bắt đầu bằng chuỗi “sd”, sau đó là thứ tự được phát hiện hay kết nối đến hệ thống.

```

crw----- 1 root root    10,  56 Oct 10 11:34 memory_bandwidth
drwxrwxrwt 2 root root    40 Oct 10 11:34 queue
drwxr-xr-x 2 root root    60 Oct 10 11:34 net
crw----- 1 root root    10,  58 Oct 10 11:34 network_latency
crw----- 1 root root    10,  57 Oct 10 11:34 network_throughput
crw-rw-rw- 1 root root     1,   3 Oct 10 11:34 null
crw-r----- 1 root kmem   10, 144 Oct 10 11:34 nvram
crw-r----- 1 root kmem     1,   4 Oct 10 11:34 port
crw----- 1 root root   108,   0 Oct 10 11:34 ppp
crw----- 1 root root    10,   1 Oct 10 11:34 psaux
crw-rw-rw- 1 root tty      5,   2 Oct 10 12:43 ptmx
crw----- 1 root root   246,   0 Oct 10 11:34 ptp0
drwxr-xr-x 2 root root     0 Oct 10 11:34 pts
crw-rw-rw- 1 root root     1,   8 Oct 10 11:34 random
crw-rw-r--+ 1 root netdev  10,  62 Oct 10 11:34 rfkill
lrwxrwxrwx 1 root root     4 Oct 10 11:34 rtc -> rtc0
crw----- 1 root root   250,   0 Oct 10 11:34 rtc0
brw-rw---- 1 root disk     8,   0 Oct 10 11:34 sda
brw-rw---- 1 root disk     8,   1 Oct 10 11:34 sda1
brw-rw---- 1 root disk     8,   2 Oct 10 11:34 sda2
brw-rw---- 1 root disk     8,   3 Oct 10 11:34 sda3
crw-rw---- 1 root disk    21,   0 Oct 10 11:34 sg0

```

Trên Linux, driver của các thiết bị phổ biến thường được xây dựng sẵn trong nhân của hệ điều hành. Nếu thiết bị nào không có, các nhà sản xuất sẽ nhúng vào trong mô đun nhân (kernel module) để có thể tháo lắp vào nhân của hệ điều hành.

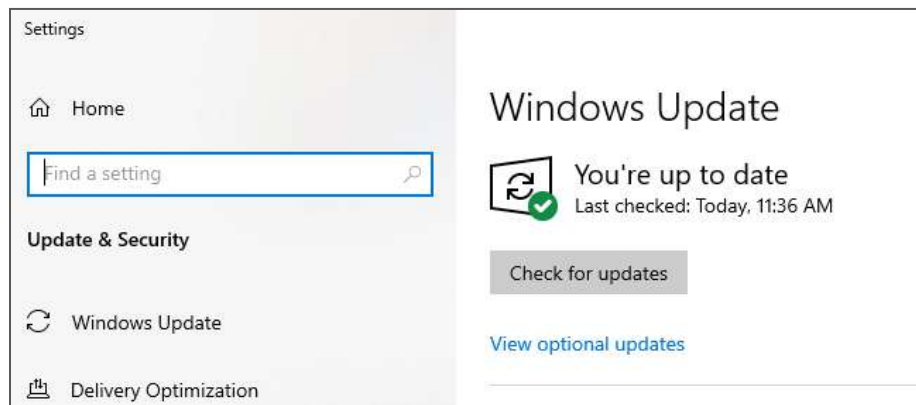


6. Cập nhật hệ điều hành Windows và Linux

Trong quá trình tạo ra hệ điều hành hay phần mềm, các nhà phát triển không tránh khỏi các lỗi có thể xảy ra. Trong số các lỗi thì những lỗi liên quan đến bảo mật thường gây nguy hiểm cho hệ thống người dùng. Do đó, việc phát hiện và sửa chữa những lỗi này vô cùng quan trọng. Những gói phần mềm dùng để khắc phục lỗ hổng bảo mật này được gọi là bản vá bảo mật. Người dùng cần thường xuyên cập nhật phần mềm để tránh bị các hacker khai thác các lỗ hổng này.

Chúng tôi đã đề cập cách thức cập nhật các gói phần mềm. Mặc dù hệ điều hành cũng là phần mềm, nhưng cách thức cập nhật chúng cần thực hiện theo một cách riêng do đây là phần quan trọng trong hệ thống máy tính của chúng ta.

Hệ điều hành Windows có một chương trình gọi là Windows Update đảm nhiệm việc kiểm tra thường xuyên các bản cập nhật, vá lỗi. Sau đó thông báo đến người dùng để áp dụng bản cập nhật này. Microsoft về sau thiết kế các bản cập nhật dưới dạng tích lũy, nghĩa là gói cập nhật sau sẽ bao gồm các gói cập nhật trước. Điều này giúp cho người dùng không cần phải tải quá nhiều gói cập nhật sau một thời gian dài không sử dụng máy.



Trong hệ điều hành Linux, nhân là thành phần chính hay thành phần lõi của hệ điều hành. Cập nhật hệ điều hành Linux thường liên quan đến cập nhật nhân của chúng. Để kiểm tra phiên bản nhân trên Ubuntu, ta sử dụng lệnh `uname -r`.

Lệnh apt full-upgrade dùng để cập nhật nhân nếu có nhân mới được phát hành. Lưu ý, cần chạy lệnh apt update trước khi cập nhật nhân để kiểm tra thông tin về phiên bản mới nhất.

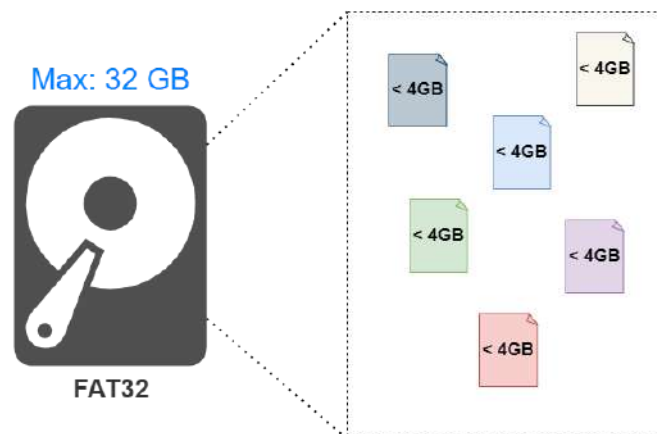
```
cindy@cindy-nyc: ~/Desktop$ uname -r
4.10.0-28-generic
cindy@cindy-nyc:~/Desktop$ sudo apt update
[sudo] password for cindy:
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://dl.google.com/linux/chrome/deb stable Release
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [6
Get:9 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [60
Get:10 http://us.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [
Get:11 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packag
Get:12 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packag
Get:13 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-
Fetched 3,101 kB in 2s (1,366 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
21 packages can be upgraded. Run 'apt list --upgradable' to see them.
cindy@cindy-nyc:~/Desktop$ sudo apt full-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... 10%
```

Bài đọc 5: Hệ Thống Tập Tin

1. Giới thiệu các hệ thống tập tin

Hệ thống tập tin là cách thức và cấu trúc mà hệ điều hành sử dụng để quản lý tập tin được lưu trữ và truy xuất. Mỗi hệ điều hành sử dụng các hệ thống tập tin khác nhau như FAT32, NTFS, exFAT trên Windows, HFS+, APFS trên MacOS, ext*, XFS, JFS trên Linux.

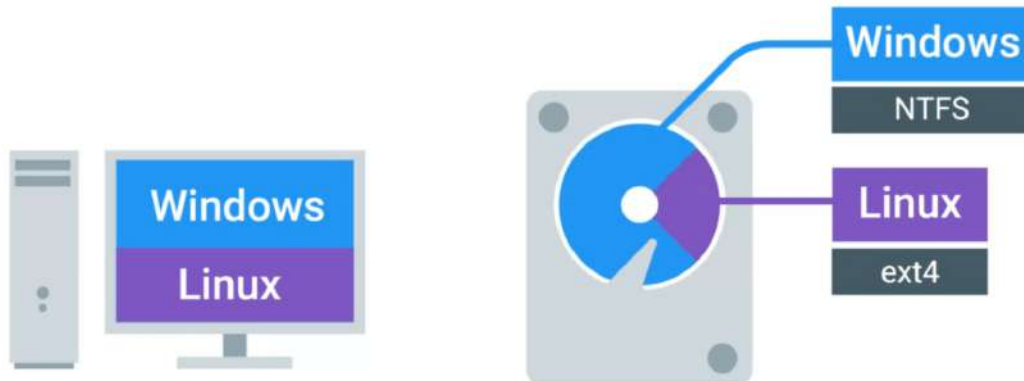
Trong số các hệ thống tập tin thì hệ thống tập tin FAT32 được hỗ trợ bởi hầu hết các hệ điều hành như Windows, Linux, và Mac OS. Tuy nhiên, hệ thống tập tin FAT32 có một số nhược điểm như không hỗ trợ các tập tin lớn hơn 4GB và kích thước của hệ thống tập tin không thể lớn hơn 32GB.



2. Ổ đĩa cứng

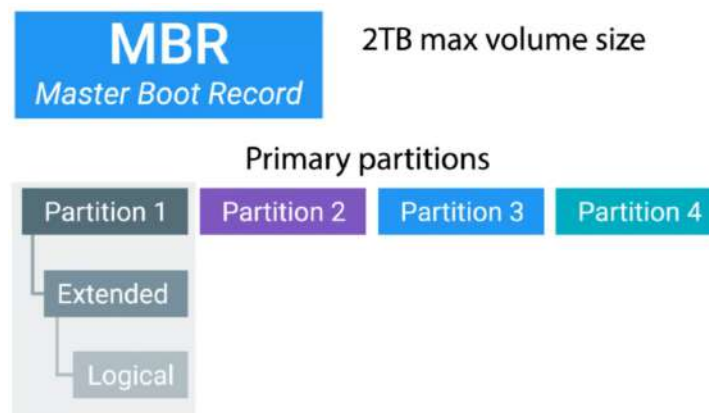
Ổ cứng có thể được chia thành nhiều phân vùng, mỗi phân vùng có thể được quản lý một cách độc lập. Do đó, ta có thể tạo hệ thống tập tin khác nhau cho mỗi phân vùng trên cùng một ổ cứng. Khi phân ổ cứng thành các vùng khác nhau, chúng ta có thể cài đặt nhiều hệ điều hành trên cùng một máy tính. Mỗi hệ điều hành sẽ nằm trên một phân vùng với hệ thống tập tin độc lập nhau. Ví

dự, phân vùng Windows thường sử dụng hệ thống tập tin NTFS. Trong khi đó, phân vùng cài Linux thường sử dụng hệ thống tập tin ext4.

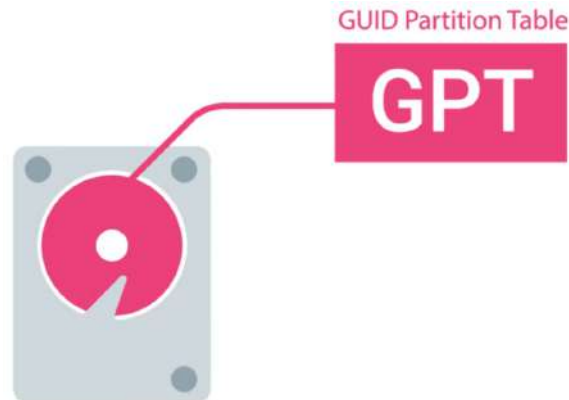


Khi phân vùng được định dạng với một hệ thống tập tin cụ thể, nó được gọi là một volume. Để biết được thông tin về các phân vùng trên đĩa cứng, hệ điều hành cần kiểm tra thông tin trên một bảng được gọi là bảng phân vùng, partition table. Có hai loại bảng được sử dụng phổ biến là MBR và GPT.

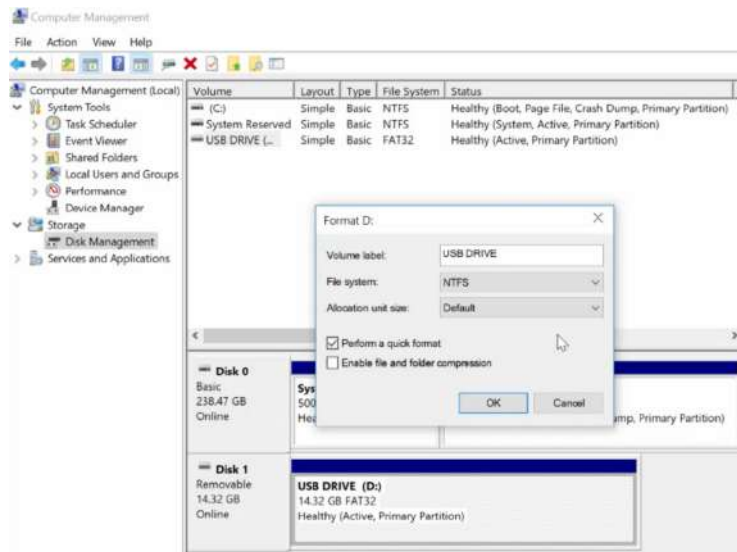
MBR là một bảng phân vùng truyền thống và được sử dụng phổ biến trên các hệ điều hành Windows. Kích thước volume tối đa mà bảng phân vùng này hỗ trợ là 2 TB. Số lượng phân vùng tối đa là 4. Đây được gọi là phân vùng chính (primary partition). Trong trường hợp muốn có thêm phân vùng, ta cần tạo phân vùng mở rộng (extended) trên một phân vùng chính, sau đó tạo ra các phân vùng khác còn được gọi là các phân vùng logic.



GPT là bảng phân vùng mới, ra đời nhằm khắc phục các nhược điểm của MBR như hỗ trợ kích thước volume lớn hơn 2TB rất nhiều và chỉ có một loại partition nên việc quản lý đơn giản hơn. Ngoài ra, GPT không giới hạn số lượng phân vùng được phân chia. Chương trình khởi động máy tính theo chuẩn UEFI chỉ làm việc với bảng phân vùng GPT.

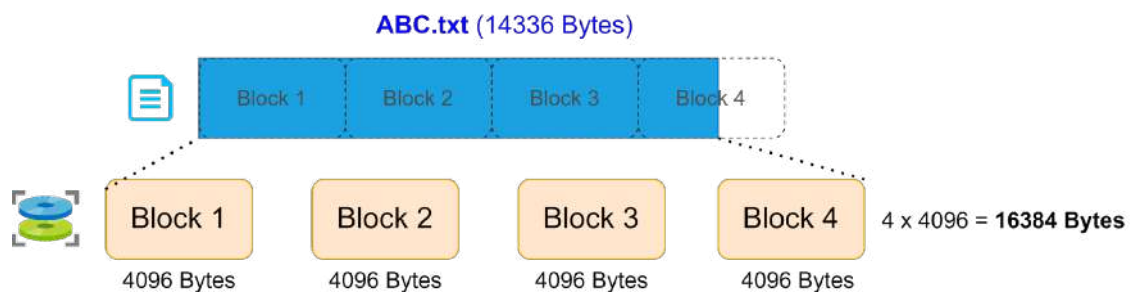


Trên Windows, để phân chia ổ cứng thành các phân vùng và định dạng hệ thống tập tin cho các phân vùng đó, ta sử dụng công cụ Disk Management. Công cụ này được tích hợp sẵn trong hệ điều hành. Trên giao diện sẽ liệt kê các ổ cứng và phân vùng mà hệ điều hành nhận diện được. Các thao tác có thể thực hiện như phân chia ổ cứng, xóa, định dạng lại, v.v...



Trong quá trình phân chia ổ cứng trên Windows, ta cần xác định kích thước đơn vị phân bổ (allocation unit size). Đây là chỉ số mô tả kích thước mỗi khối dữ liệu được ghi vào phân vùng.

Mỗi tập tin sẽ được chia thành các khối có kích thước bằng kích thước phân bổ này để quản lý. Càng ít khối thì hệ thống thực thi càng nhanh. Tuy nhiên, nếu kích thước khối lớn mà lại có nhiều tập tin nhỏ thì sẽ gây lãng phí, vì tập tin có kích thước nhỏ hơn khối cũng sẽ mất dung lượng tương đương với kích thước khối. Ngược lại, nếu kích thước khối nhỏ mà có nhiều tập tin lớn thì sẽ gây chậm do có quá nhiều khối dữ liệu.



Trong giao diện dòng lệnh trên Windows, ta sử dụng công cụ Diskpart để tạo, điều chỉnh và xóa phân vùng. Tùy vào mục đích trên phân vùng ổ đĩa, chúng ta

có các lệnh khác nhau. Một số lệnh phổ biến như list disk dùng để liệt kê các đĩa, select disk để chọn đĩa, clean để xóa dữ liệu, create partition primary để tạo phân vùng, select partition để chọn phân vùng cần thao tác, active để đánh dấu phân vùng được kích hoạt, format để định dạng lại phân vùng. Ngoài các công cụ được hỗ trợ sẵn trên Windows, chúng ta có thể sử dụng các phần mềm được phát triển bởi bên thứ ba với các tiện ích tăng cường.

```
Administrator: Command Prompt - Diskpart
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>Diskpart

Microsoft DiskPart version 10.0.15063.0

Copyright (C) Microsoft Corporation.
On computer: CINDY-NYC

DISKPART> list disk

Disk ###        Status        Size      Free      Dyn  Gpt
-----
Disk 0          Online         238 GB     0 B
Disk 1          Online         14 GB     0 B

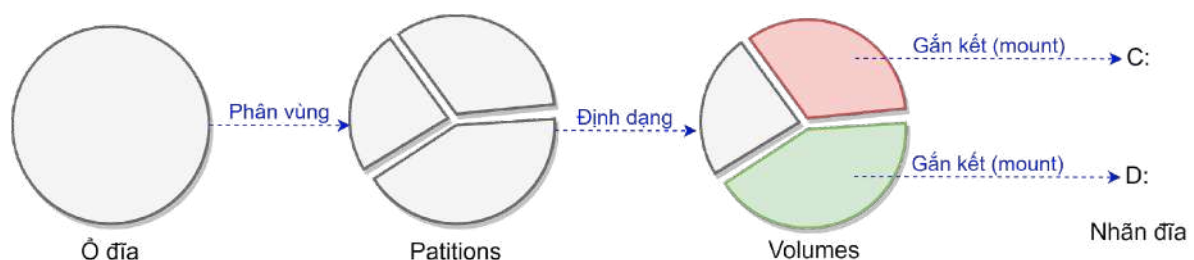
DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.
```

Để có thể sử dụng một hệ thống tập tin, ta cần gắn kết nó vào hệ điều hành. Quá trình này được gọi là mounting và thường được thực hiện tự động bởi Windows. Ví dụ, khi cắm ổ USB đã định dạng vào máy, hệ điều hành lập tức phát hiện và gắn kết nó với một nhãn đĩa. Khi không dùng nữa, ta cần gỡ gắn kết hay unmount ổ đĩa.



Trên Linux cũng có công cụ parted để thực hiện phân vùng và định dạng hệ thống tập tin. Công cụ này hỗ trợ giao diện đồ họa lẫn giao diện dòng lệnh.

```
cindy@cindy-nyc:~$ sudo parted -l
Model: ATA SAMSUNG MZNLN128 (scsi)
Disk /dev/sda: 128GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number   Start    End      Size    File system  Name
  1       1049kB   538MB   537MB   fat32        EFI System Part
  2       538MB   120GB   119GB   ext4
  3       120GB   128GB   8463MB  linux-swap(v1)

Error: /dev/sdb: unrecognised disk label
Model: Kingston DataTraveler 2.0 (scsi)
Disk /dev/sdb: 7803MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
```

Trong giao diện dòng lệnh, lệnh `parted -l` dùng để liệt các ổ đĩa và phân vùng có trong hệ thống. Trong Linux, mỗi thiết bị khi kết nối vào máy tính được xem như một tập tin trong thư mục `/dev`. Các nhãn của thiết bị lưu trữ được bắt đầu bằng từ `sd`, tiếp theo là các ký tự chữ cái như `a`, `b`, `c`, Tương tự, trên mỗi đĩa, nếu có nhiều phân vùng thì các phân vùng được đánh theo số thứ tự 1, 2, 3, v.v... Ví dụ `/dev/sda2` nghĩa là phân vùng thứ 2 của ổ đĩa đầu tiên được nhận diện bởi hệ thống.

Khi thực hiện phân vùng, ta cần chọn ổ đĩa dựa trên tên thiết bị. Một số lệnh sử dụng trong quá trình phân vùng như lệnh `print` để xem thông tin trạng thái ổ đĩa, `mklabel` để thiết lập bảng phân vùng, `mkpart` tạo phân vùng và định dạng hệ thống tập tin, lệnh `quit` để thoát việc tạo phân vùng.

```
cindy@cindy-nyc:~$ sudo parted /dev/sdb
GNU Parted 3.2
Using /dev/sdb
Welcome to GNU Parted! Type 'help' to view a list of commands
(parted) mklabel gpt
(parted) print
Model: Kingston DataTraveler 2.0 (scsi)
Disk /dev/sdb: 7803MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
(parted) mkpart primary ext4 1MiB 5GiB
(parted) print
Model: Kingston DataTraveler 2.0 (scsi)
Disk /dev/sdb: 7803MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
1       1049kB 5369MB 5368MB ext4         primary
(parted) quit
```

Để định dạng lại phân vùng đang có, ta sử dụng lệnh `mkfs`. Lưu ý kiểm tra kỹ thông tin về tên phân vùng trước khi định dạng để tránh bị mất dữ liệu.

Mặc dù các thiết bị như ổ USB thường được gắn kết tự động bởi hệ điều hành mỗi lần cắm vào máy tính, ta vẫn có lệnh để thực hiện thủ công việc gắn kết này. Lệnh `mount` dùng để gắn kết và `umount` để gỡ bỏ gắn kết.

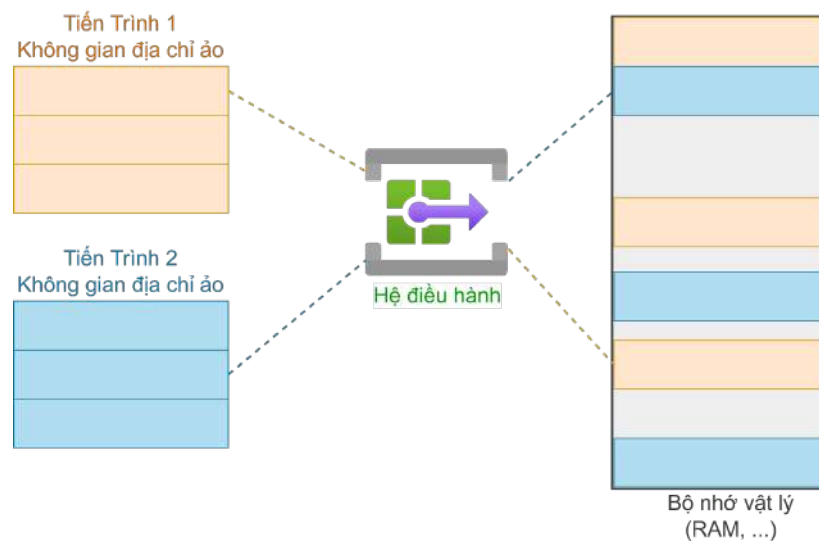
```
cindy@cindy-nyc:~$ sudo mount /dev/sdb1 /my_usb/
cindy@cindy-nyc:~$ cd /my_usb/
cindy@cindy-nyc:/my_usb$
```

Để tránh thực hiện gắn kết thủ công các phân vùng mỗi lần khởi động hệ điều hành, ta thêm các dòng mô tả phân vùng vào tập tin `/etc/fstab`. Cách thức ghi bổ sung tương tự các dòng đang có trong tập tin này. Thông tin về mã phân vùng có thể xem trong kết quả của lệnh `blkid`.

3. Bộ nhớ ảo

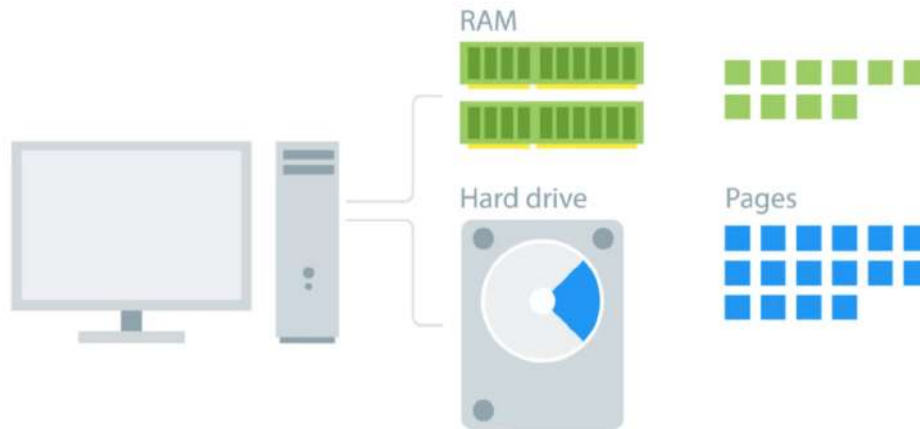
Bộ nhớ ảo và vai trò trong hệ thống

Bộ nhớ ảo là cách thức hệ điều hành cung cấp bộ nhớ vật lý như RAM đến các ứng dụng đang chạy. Hay nói cách khác, các ứng dụng không cần quan tâm dữ liệu được đặt ở đâu trong vùng nhớ vật lý mà chỉ cần biết chúng đang có dữ liệu nào trong không gian địa chỉ ảo được cấp. Khi tương tác, hệ điều hành sẽ ánh xạ địa chỉ ảo này thành các địa chỉ vật lý trên vùng nhớ thực sự.

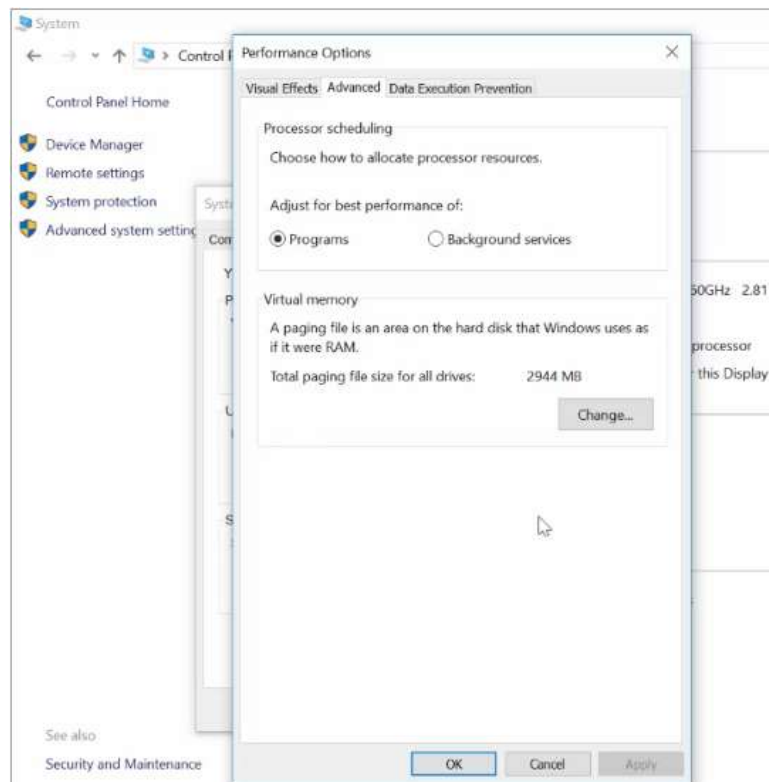


Kỹ thuật phân trang

Mặc dù RAM có tốc độ truy xuất nhanh nhưng dung lượng khá giới hạn. Các ứng dụng có thể không đủ không gian để chạy hoặc có những dữ liệu chưa thực sự cần dùng nhưng lại được để trên RAM sẽ gây lãng phí. Do đó hệ điều hành dựa trên bộ nhớ ảo để lấy một phần của ổ cứng làm bộ nhớ chính và chủ yếu lưu trữ các dữ liệu chưa cần đến. Để quản lý dữ liệu chuyển đổi giữa RAM và vùng nhớ này, người ta phân dữ liệu thành các trang (page).



Các trang trên Windows được chứa trong một tập tin ẩn đặc biệt gọi là `pagefile.sys`. Tập tin này được quản lý tự động bởi hệ điều hành. Chúng ta không nên xóa hay điều chỉnh nó. Ngoài ra, ta cũng có thể cấu hình kích thước vùng ổ cứng để dùng làm bộ nhớ ảo được thể hiện trong cửa sổ Performance Options. Kích thước này được khuyến cáo gấp từ 1.0 lần kích thước RAM trở lên để hệ thống hoạt động tốt.

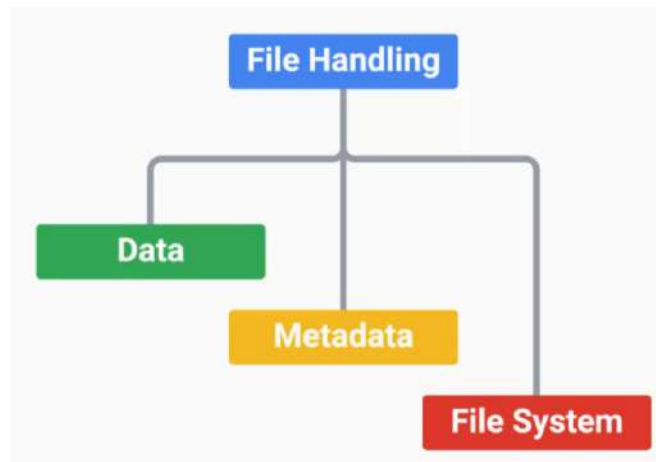


Đối với Linux, khu vực trên ổ cứng được chỉ định làm bộ nhớ ảo được gọi là không gian hoán đổi. Việc định dạng không gian hoán đổi này cũng được thực hiện qua lệnh tạo phân vùng `mkpart` nhưng lúc này chọn hệ thống tập tin là `linux-swap`. Khi đã định dạng phân vùng, ta dùng lệnh `mkswap` để tạo phân vùng này và sau đó chỉ định cho hệ điều hành phân vùng làm không gian hoán đổi bằng lệnh `swapon`.

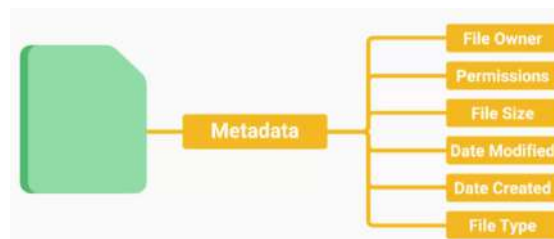
4. Quản lý tập tin

Siêu dữ liệu của tập tin

Bộ quản lý tập tin gồm 3 thành phần chính đó là dữ liệu của tập tin, siêu dữ liệu và hệ thống tập tin.

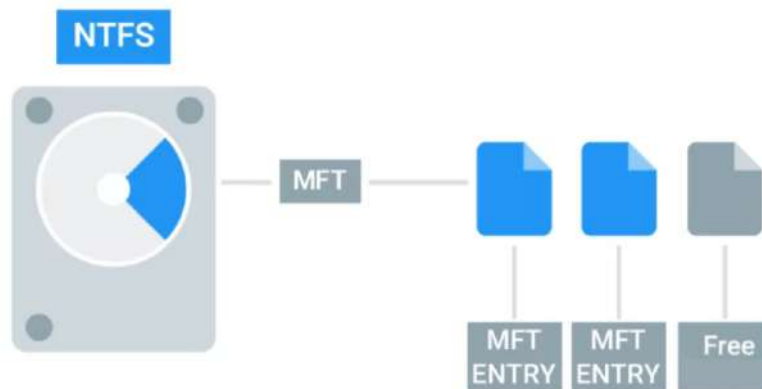


Siêu dữ liệu là loại dữ liệu mô tả thông tin về mỗi loại tập tin như tên, tên mở rộng, loại tập tin, kích thước, ngày giờ cập nhật, v.v. Nhờ đó, chúng ta có thể quản lý về tập tin một cách tốt hơn.

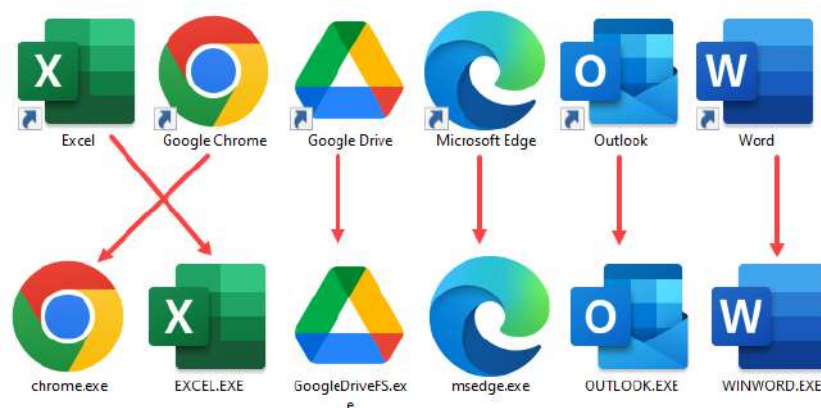


Quản lý tập tin trên hệ thống NTFS

Hệ thống tập tin NTFS sử dụng một bảng tập tin gốc để quản lý tất cả. Mỗi tập tin có ít nhất một phần tử trên MFT mô tả về nó. Khi tập tin bị xóa, các phần tử trên MFT liên quan được đánh dấu là Free (tự do) và có thể được dùng lại cho một tập tin mới.



Một loại tập tin đặc biệt trong Windows là tập tin lối tắt hay shortcut. Tập tin này là tham chiếu đến tập tin khác trong hệ thống. Hay nói một cách đơn giản, ta có thể xem tập tin lối tắt đang chứa một nội dung và nội dung đó là đường dẫn đến tập tin khác.



Bên cạnh tập tin lối tắt, hệ điều hành còn có một dạng khác tương tự. Đó là liên kết tượng trưng nhưng nó không phải là một tập tin. Nó là một phần tử trên bảng MFT và trỏ hay tham chiếu đến một phần tử chứa tên tập tin. Hệ điều hành đối xử với liên kết tượng trưng như thể là tập tin gốc. Tuy nhiên, điểm yếu của liên kết tượng trưng cũng giống như tập tin lối tắt, nghĩa là khi tập tin gốc đổi tên hay di chuyển đến đường dẫn khác thì liên kết tượng trưng sẽ không còn trỏ đúng đến tập tin này được nữa. Để tạo liên kết tượng trưng, ta sử dụng lệnh mklink.

```
mklink symlink_name file
```

```
C:\Users\cindy\Desktop\Links>mklink file_1_symlink file_1.txt  
symbolic link created for file_1_symlink <==> file_1.txt
```

Liên kết cứng cũng là loại liên kết được tạo trong một phân tử ở MFT nhưng nó trỏ trực tiếp đến bản ghi tập tin thay vì tên tập tin như liên kết tượng trưng. Khi chúng ta thay đổi tên tập tin hay di chuyển đến nơi khác thì liên kết cứng vẫn trỏ về tập tin đó, điều này trái ngược với liên kết tượng trưng. Để tạo liên kết cứng, ta vẫn sử dụng lệnh `mklink` nhưng có thêm tham số `/H`.

```
mklink /H symlink_name file
```

```
C:\Users\cindy\Desktop\Links>mklink /H file_1_hardlink file_1.txt  
Hardlink created for file_1_hardlink <==> file_1.txt
```

Quản lý tập tin trên hệ thống Linux

Trên Linux, hệ thống tập tin được tổ chức dưới dạng cấu trúc inode và việc quản lý được thực hiện bằng bảng inode tương tự như bảng MFT trên Windows. Các khái niệm như liên kết tượng trưng và liên kết cứng cũng tương tự. Để tạo liên kết tượng trưng trên Bash, ta sử dụng lệnh `ln`. Nếu có cờ `-s` nghĩa là tạo liên kết tượng trưng và nếu không sẽ tạo liên kết cứng. Chỉ số trên trường thông tin hiển thị bởi lệnh `ls` thể hiện số liên kết cứng trỏ đến tập tin, nếu chỉ số này bằng 0 thì tập tin đã bị xóa khỏi hệ thống.

```
ln -s file symlink_name
```

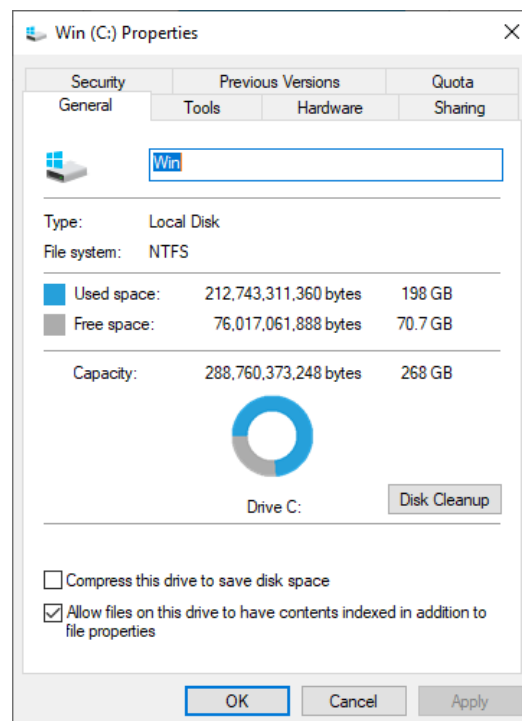
```
ln file hardlink_name
```

```
cindy@cindy-nyc:~/Desktop$ ls -l important_file
-rw-rw-r-- 1 cindy cindy 0 Oct  5 16:40 important_file
cindy@cindy-nyc:~/Desktop$ ln -s important_file important_file_softlink
cindy@cindy-nyc:~/Desktop$ ln important_file important_file_hardlink
cindy@cindy-nyc:~/Desktop$ ls
important_file  important_file_hardlink  important_file_softlink
cindy@cindy-nyc:~/Desktop$ ls -l important_file
-rw-rw-r-- 2 cindy cindy 0 Oct  5 16:40 important_file
```

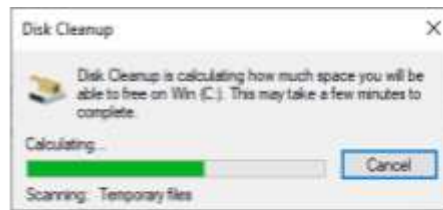
5. Quản lý ổ đĩa

Tỷ lệ sử dụng và dọn dẹp ổ đĩa

Windows hỗ trợ một số tiện ích để xem trạng thái của các ổ đĩa như không gian đã sử dụng, không gian còn trống.

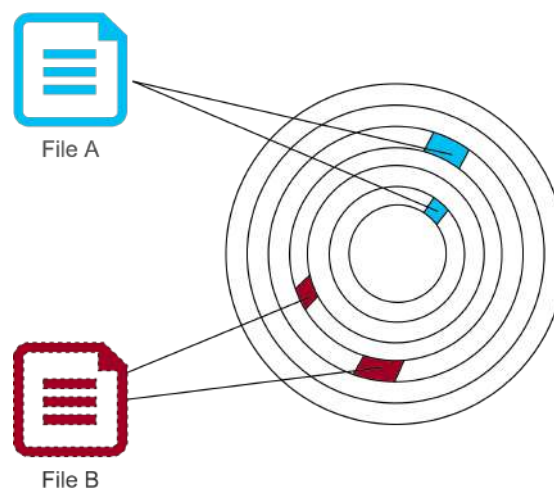


Chức năng Disk Cleanup dùng để kiểm tra và dọn dẹp các tập tin không cần thiết trên ổ đĩa.



Chống phân mảnh ổ đĩa

Qua thời gian sử dụng, ổ cứng, cụ thể là ổ đĩa HDD, có thể bị hiện tượng phân mảnh. Nghĩa là tập tin bố trí thành những khối ở những nơi cách xa nhau. Điều này làm cho thời gian đọc dữ liệu lâu do cần phải di chuyển đầu đọc nhiều. Chống phân mảnh là cách thức hệ điều hành tổ chức lại các khu vực phân bố của một tập tin. Windows lập lịch để tự động chạy nhiệm vụ này. Tuy nhiên, chúng ta có thể chủ động chống phân mảnh bằng chương trình Disk Defragmenter. Đối với ổ cứng dạng thể rắn, SSD, mặc dù không dùng các đĩa xoay nhưng quá trình tối ưu ổ cứng được gọi là trim, cũng được thường xuyên thực hiện để làm cho quá trình đọc, ghi dữ liệu trở nên tốt hơn.



Trên Linux, ta có thể sử dụng lệnh `du` để kiểm tra dung lượng của từng thư mục và lệnh `df` để kiểm tra không gian còn trống trong máy. Kết quả sẽ liệt kê chi tiết từng thiết bị được gắn kết vào máy tính.

`du -h`

`df -h`

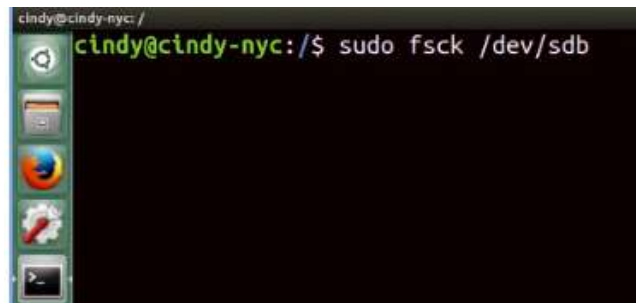
```
cindy@cindy-nyc:/$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            3.9G   0    3.9G   0% /dev
tmpfs           787M   9.4M  777M   2% /run
/dev/sda2       109G   5.5G   99G    6% /
tmpfs           3.9G  308K   3.9G   1% /dev/shm
tmpfs           5.0M   4.0K   5.0M   1% /run/lock
tmpfs           3.9G   0    3.9G   0% /sys/fs/cgroup
/dev/sda1       511M   3.4M  508M   1% /boot/efi
tmpfs           787M   76K   787M   1% /run/user/1000
```

6. Sửa chữa hệ thống tập tin

Hư hỏng dữ liệu (data corruption) là hiện tượng dữ liệu bị hư do vấn đề xảy ra trong hệ thống hay do thao tác của người dùng. Ví dụ, dữ liệu chưa được ghi xong lên ổ USB nhưng đã bị gỡ ra đột ngột. Hệ thống tập tin NTFS sử dụng các tập tin log để lưu lịch sử thay đổi tập tin và tìm cách để phục hồi lại khi có sự cố. Windows hỗ trợ công cụ, được gọi là `chkdsk`, để kiểm tra ổ cứng và phục hồi những vấn đề liên quan đến hư hỏng dữ liệu. Tham số `/f` dùng để sửa các lỗi trên đĩa, trong khi đó `/r` xác định các vùng hư hỏng nghiêm trọng và cố gắng để phục hồi dữ liệu này.

```
C:\Windows\system32>chkdsk /F D:  
The type of the file system is NTFS.  
Volume label is my-thumb-drive.  
  
Stage 1: Examining basic file system structure ...  
    256 file records processed.  
File verification completed.  
    0 large file records processed.  
    0 bad file records processed.  
  
Stage 2: Examining file name linkage ...  
    280 index entries processed.  
Index verification completed.  
    0 unindexed files scanned.  
    0 unindexed files recovered to lost and found.  
  
Stage 3: Examining security descriptors ...  
Security descriptor verification completed.  
    12 data files processed.
```

Trên Linux, để phát hiện và sửa chữa hệ thống tập tin ta có thể sử dụng lệnh fsck.



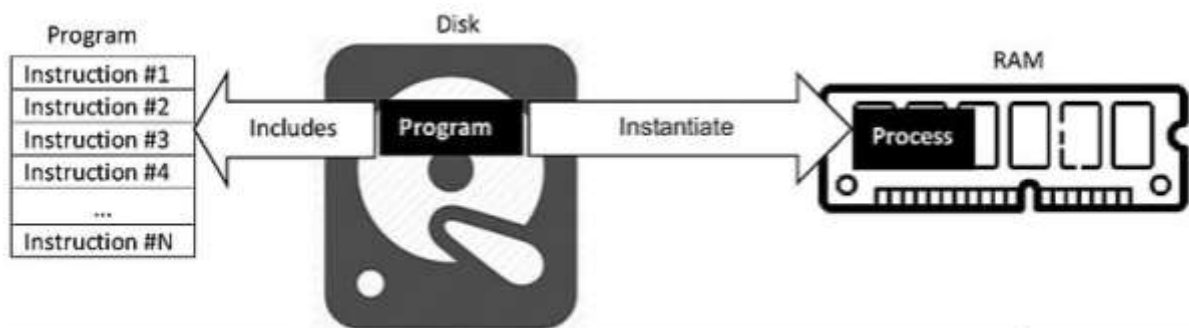
```
cindy@cindy-nyc: /  
cindy@cindy-nyc:/$ sudo fsck /dev/sdb
```

Bài đọc 6: Quản Lý Tiến Trình

1. Vòng đời của tiến trình

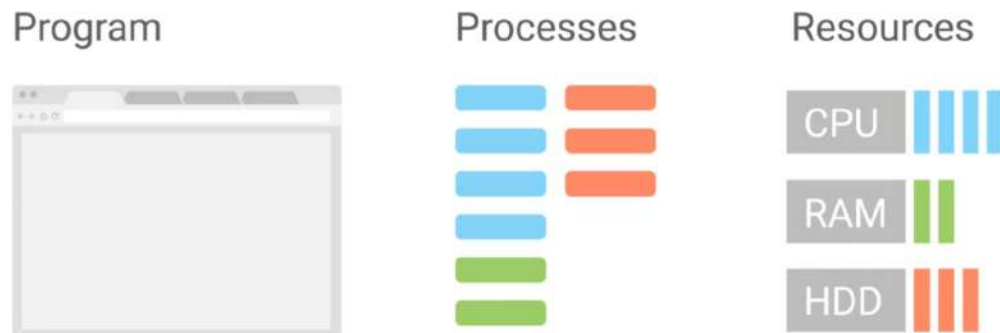
Tiến trình

Tiến trình (process) là một chương trình đang ở trạng thái thực thi, trong khi đó chương trình là một ứng dụng, một đoạn mã trên vùng nhớ mà chúng ta chưa chạy. Chúng ta có thể tạo ra nhiều tiến trình của một chương trình. Ví dụ, khi mở nhiều lần chương trình notepad trên Windows, mỗi một cửa sổ chúng ta nhìn thấy là một tiến trình của một chương trình duy nhất là Notepad.

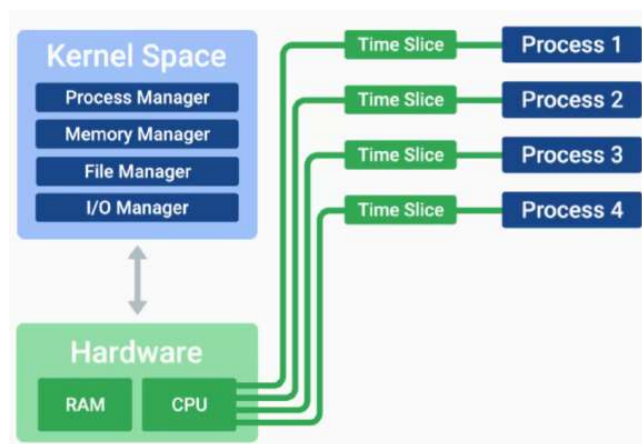


Nguồn: wikimedia

Trình duyệt web như Google Chrome khi thực thi sẽ tạo nhiều tiến trình ứng với mỗi thẻ được mở.



Trong quá trình thực thi, mỗi tiến trình đều cần tài nguyên như RAM, CPU, v.v. Tuy nhiên tài nguyên trong máy tính là hữu hạn, ví dụ, chỉ có 1 CPU trong khi đó có đến 10 tiến trình đều muốn dùng, thì việc quản lý và chia sẻ tài nguyên giữa các tiến trình trở nên quan trọng. Việc luân chuyển tài nguyên sẽ giúp trải nghiệm của người dùng hệ thống trở nên tốt hơn. Một công cụ giúp hệ điều hành có thể làm được điều đó là lát cắt thời gian (time slice). Đó là khoảng thời gian đủ ngắn để HĐH ngắt một tiến trình (tức là đòi lại tài nguyên) và xem xét việc có nên cấp tiếp hay cấp cho một tiến trình khác hay không. Các quyết định này được thực hiện bởi bộ lập lịch (scheduler).



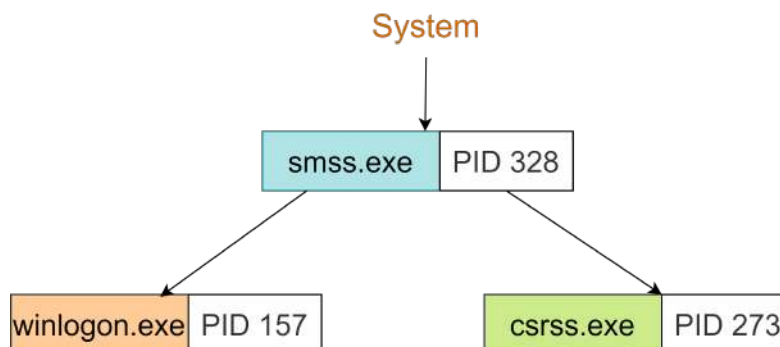
Mỗi tiến trình được gán một mã định danh (Process ID, PID) để phân biệt với các tiến trình khác đang chạy trong hệ thống. Mã này cũng được sử dụng như một tham số cho các lệnh mà chúng ta sẽ đề cập trong các phần tiếp theo.

Name	PID	Status
chrome.exe	1928	Running
chrome.exe	17852	Running
chrome.exe	16568	Running
chrome.exe	5288	Running
chrome.exe	16944	Running
chrome.exe	10004	Running
chrome.exe	11808	Running
chrome.exe	4240	Running
chrome.exe	2808	Running
chrome.exe	17208	Running
chrome.exe	17272	Running
chrome.exe	9448	Running
chrome.exe	11624	Running
chrome.exe	1728	Running
chrome.exe	10840	Running
chrome.exe	6632	Running

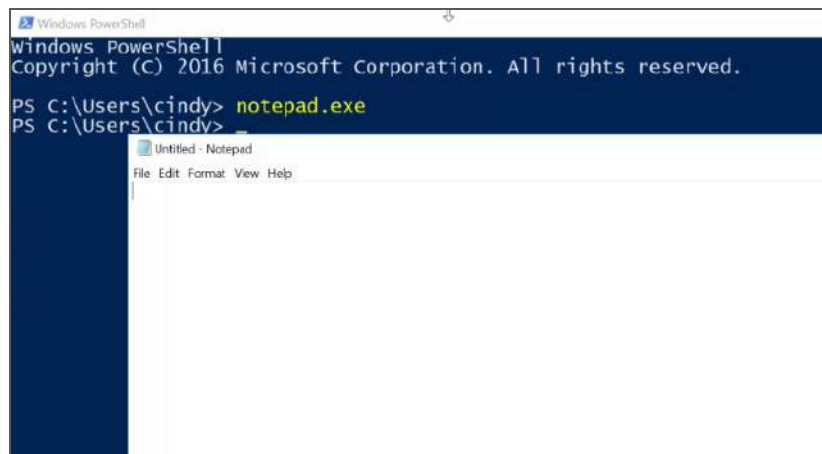
Ngoài các tiến trình mà chúng ta chủ động thực thi một chương trình cụ thể, hệ thống còn có các loại tiến trình khác chạy ngầm bên dưới. Người dùng thông thường sẽ không thấy và không tương tác trực tiếp với các tiến trình này nhưng chúng lại cần thiết để hệ thống làm việc một cách chặt chẽ. Một số tiến trình chạy ngầm như tiến trình lập lịch, quản lý mạng, ghi nhật ký sự kiện, v.v... Các hacker cũng lợi dụng loại tiến trình này để thực thi các tiến trình chạy ngầm gây hại cho hệ thống và người dùng.

Tạo và kết thúc tiến trình

Khi Windows khởi động, một tiến trình được xem gần như đầu tiên thực hiện là Session Manager Subsystem. Tiến trình này thiết lập một số cấu hình khởi tạo cho hệ điều hành. Sau đó nó sẽ khởi động tiến trình đăng nhập cùng với tiến trình Client/Server Runtime Subsystem để thực thi giao diện đồ họa và giao diện dòng lệnh.

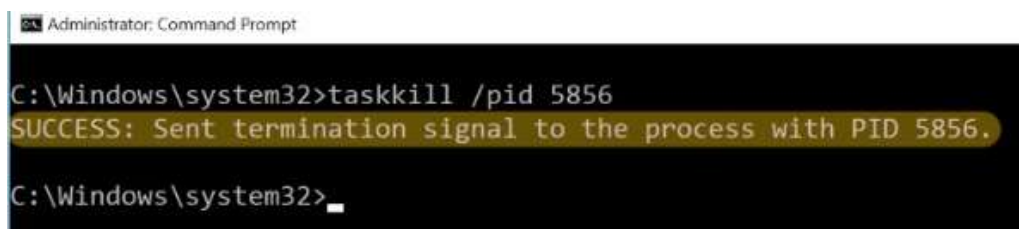


Mỗi tiến trình trên Windows khi được tạo mới, chúng sẽ được tạo bởi một tiến trình cha. Tiến trình con thừa kế một số tính chất từ tiến trình cha nhưng sau đó hoạt động độc lập với tiến trình cha. Ví dụ, nếu bắt đầu notepad.exe từ PowerShell thì tiến trình cha sẽ là PowerShell và tiến trình con là notepad. Khi tiến trình notepad chạy, nó sẽ độc lập với tiến trình PowerShell. Việc đóng PowerShell sẽ không ảnh hưởng đến tiến trình notepad đang chạy.

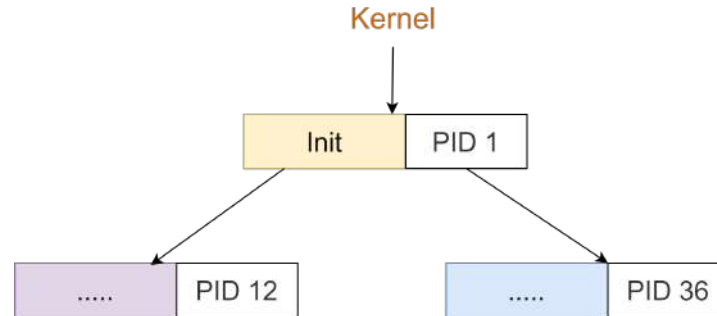


Trong giao diện dòng lệnh, ta có thể sử dụng lệnh taskkill để hủy tiến trình đang chạy. Cú pháp là taskkill /pid process_id. Có thể thấy, để hủy tiến trình ta cần biết mã của tiến trình thay vì tên của chương trình đang chạy. Trong các phần sau, chúng tôi sẽ trình bày nơi để có thể xem mã tiến trình này.

taskkill /pid process_id



Đối với Linux, tiến trình đầu tiên được thực thi là tiến trình init. Tiếp theo, tiến trình init sẽ khởi tạo các tiến trình khác thực thi trong hệ điều hành.



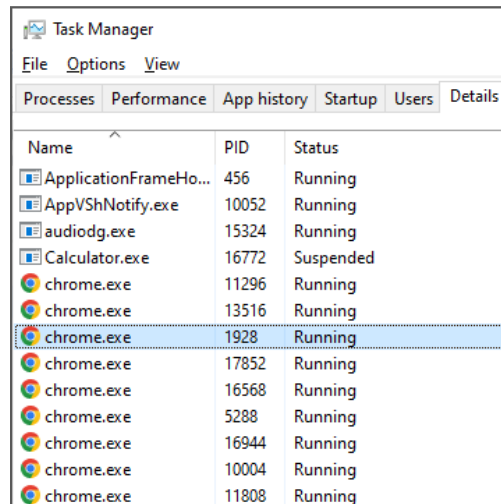
Để hủy tiến trình lên Linux, chúng ta sử dụng lệnh kill cùng với mã của tiến trình. Nếu không có cờ nào bật lên nghĩa là dừng tiến trình nhưng cho thời gian để tiến trình dọn dẹp và giải phóng tài nguyên một cách an toàn. Tuy nhiên, nếu lệnh kill có thêm cờ -KILL thì tiến trình được yêu cầu dừng ngay lập tức, tức là không cho thời gian để dọn dẹp. Nếu thay thế bằng cờ -TSTP nghĩa là ta muốn tạm dừng tiến trình và cờ -CONT là tiếp tục thực hiện tiến trình đó.

2. Quản lý tiến trình

Quản lý tiến trình trên Windows

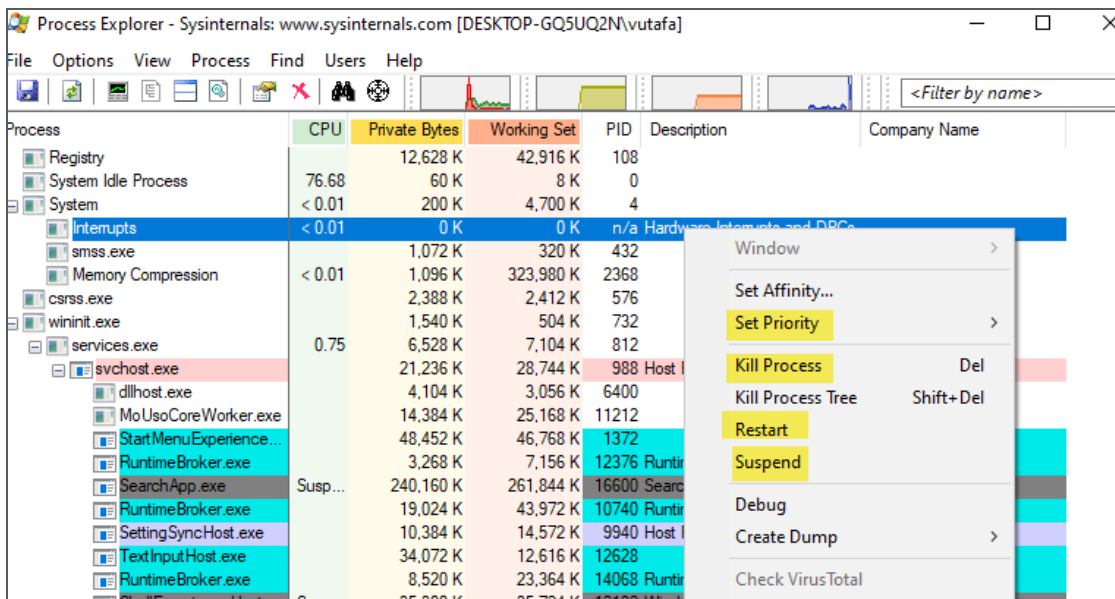
Chương trình Task Manager (taskmgr.exe) quản lý các chương trình, tiến trình đang thực hiện trên máy cùng với các thông tin như tài nguyên CPU, bộ nhớ đã sử dụng. Ngoài ra chúng ta có thể tạo hay hủy tiến trình, xem mã tiến trình trên cửa sổ.

Task Manager						
File Options View						
Processes Performance App history Startup Users Details Services						
Name	Status	17% CPU	42% Memory	1% Disk	0% Network	2% GPU
Microsoft Windows Search Filte...		0%	1.1 MB	0 MB/s	0 Mbps	0%
> Start		0%	19.1 MB	0 MB/s	0 Mbps	0%
> Search		0%	0 MB	0 MB/s	0 Mbps	0%
> Microsoft Text Input Application		0%	3.9 MB	0 MB/s	0 Mbps	0%
> Runtime Broker		0%	1.5 MB	0 MB/s	0 Mbps	0%
> Google Chrome (13)		1.6%	962.1 MB	0 MB/s	0 Mbps	0%



Name	PID	Status
ApplicationFrameHo...	456	Running
AppVShNotify.exe	10052	Running
audiodg.exe	15324	Running
Calculator.exe	16772	Suspended
chrome.exe	11296	Running
chrome.exe	13516	Running
chrome.exe	1928	Running
chrome.exe	17852	Running
chrome.exe	16568	Running
chrome.exe	5288	Running
chrome.exe	16944	Running
chrome.exe	10004	Running
chrome.exe	11808	Running

Microsoft còn phát triển một công cụ có tên là Process Explorer để bổ sung thêm các tính năng tăng cường trong quản lý tiến trình. Công cụ này không được tích hợp sẵn mà cần tải từ trang của Microsoft. Một số tính năng bổ sung như điều chỉnh độ ưu tiên, tạm dừng hay khởi động lại tiến trình, xem danh sách các tiến trình con, v.v... Lưu ý, khi khởi động lại tiến trình nào đó thì tiến trình cha của tiến trình này sẽ là tiến trình process explorer, chính là chương trình chúng ta đang tương tác đến.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12,628 K	42,916 K	108		
System Idle Process	76.68	60 K	8 K	0		
System	< 0.01	200 K	4,700 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,072 K	320 K	432		
Memory Compression	< 0.01	1,096 K	323,980 K	2368		
csrss.exe		2,388 K	2,412 K	576		
wininit.exe		1,540 K	504 K	732		
services.exe	0.75	6,528 K	7,104 K	812		
svchost.exe		21,236 K	28,744 K	988	Host Process for Windows Services	
dllhost.exe		4,104 K	3,056 K	6400		
MoUsoCoreWorker.exe		14,384 K	25,168 K	11212		
Start Menu Experience Host.exe		48,452 K	46,768 K	1372		
RuntimeBroker.exe		3,268 K	7,156 K	12376	Runtime Broker	
SearchApp.exe	Susp...	240,160 K	261,844 K	16600	Search App	
RuntimeBroker.exe		19,024 K	43,972 K	10740	Runtime Broker	
SettingSyncHost.exe		10,384 K	14,572 K	9940	Host Process for Settings Sync	
TextInputHost.exe		34,072 K	12,616 K	12628	Text Input Host	
RuntimeBroker.exe		8,520 K	23,364 K	14068	Runtime Broker	

Đối với giao diện dòng lệnh, ta có thể sử dụng lệnh tasklist hoặc lệnh Get-Process để liệt kê tất cả các tiến trình đang chạy trong hệ thống cùng với các thông tin liên quan như mã tiến trình, tài nguyên sử dụng.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vutafa> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
475	27	16192	12808	0.58	456	6	ApplicationFrameHost
152	8	1580	488		10052	0	AppVShNotify
284	12	7360	13120	0.66	6516	0	audiodg
596	30	42132	808	0.77	16772	6	Calculator
375	19	115416	176296	6.28	692	6	chrome
262	18	105524	73536	30.20	1728	6	chrome
758	50	264016	155708	346.86	1928	6	chrome
243	16	24404	8268	0.47	2808	6	chrome

Quản lý tiến trình trên Linux

Trên Linux, lệnh ps được sử dụng để liệt kê các tiến trình đang chạy trong hệ thống. Kết quả trả về bao gồm mã tiến trình trong cột PID, trạng thái tiến trình, thời gian CPU thực thi, lệnh dùng để chạy tiến trình.

```
cindy@cindy-nyc: ~$ ps -x
```

PID	TTY	STAT	TIME	COMMAND
1245	?	Ss	0:00	/lib/systemd/systemd --user
1248	?	S	0:00	(sd-pam)
1295	?	Sl	0:00	/usr/bin/gnome-keyring-daemon --daemonize
1299	?	Ss	0:00	/sbin/upstart --user
1420	?	S	0:00	upstart-udev-bridge --daemon --user
1442	?	Ss	0:01	dbus-daemon --fork --session --address=un
1468	?	Ss	0:00	/usr/lib/x86_64-linux-gnu/hud/window-stac
1545	?	Ssl	0:02	/usr/lib/x86_64-linux-gnu/bamf/bamfdaemon
1548	?	S	0:00	upstart-dbus-bridge --daemon --system --u
1549	?	S	0:00	upstart-file-bridge --daemon --user
1553	?	S	0:00	upstart-dbus-bridge --daemon --session --
1566	?	Ssl	0:20	/usr/bin/ibus-daemon --daemonize --xim --
1576	?	Sl	0:00	/usr/lib/gvfs/gvfsd
1582	?	Sl	0:00	/usr/lib/gvfs/gvfsd-fuse /run/user/1000/g
1586	?	Sl	0:00	/usr/lib/ibus/ibus-dconf

Tương tự như các thiết bị được cắm vào máy tính, Linux đối xử mọi thứ như tập tin kể cả với tiến trình. Các tiến trình là các tập tin nằm trong thư mục /proc. Do đó để liệt kê các tiến trình, ta có thể sử dụng lệnh ls. Để xem thông tin hay trạng thái chi tiết của tiến trình, ta sử dụng lệnh cat.

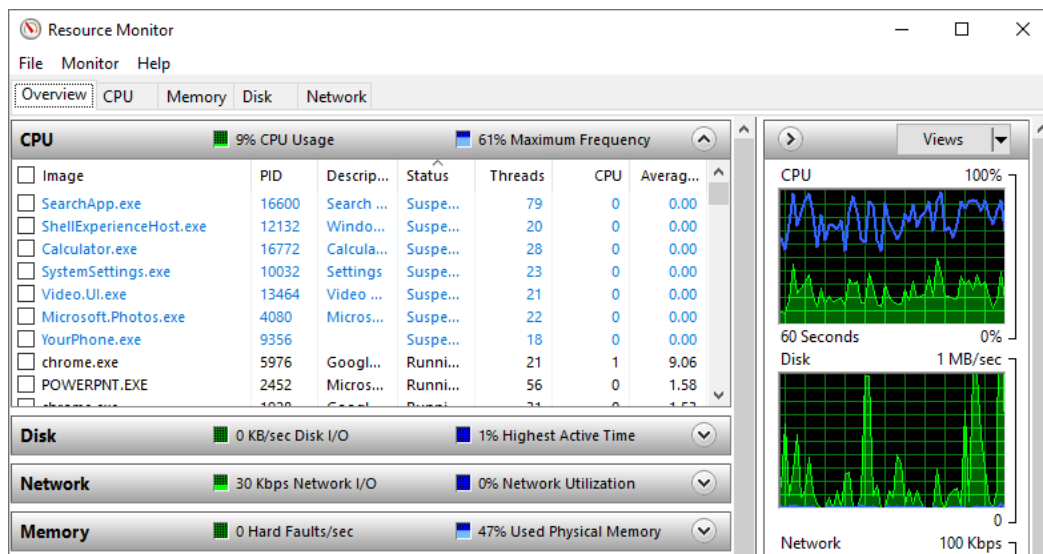
```
cindy@cindy-nyc:~$ ls -l /proc
total 0
dr-xr-xr-x  9 root      root      0 Oct 10 11:34 1
dr-xr-xr-x  9 root      root      0 Oct 10 11:34 10
dr-xr-xr-x  9 root      root      0 Oct 10 11:34 100
dr-xr-xr-x  9 root      root      0 Oct 10 11:34 101
dr-xr-xr-x  9 cindy     cindy    0 Oct 10 15:10 10116
dr-xr-xr-x  9 cindy     cindy    0 Oct 10 15:10 10123
dr-xr-xr-x  9 cindy     cindy    0 Oct 10 15:15 10168
dr-xr-xr-x  9 root      root      0 Oct 10 11:34 102
```

Trong quá trình một tiến trình thực thi, chúng ta có thể giao tiếp với chúng qua hình thức gửi tín hiệu. Ví dụ, khi nhấn tổ hợp phím Ctrl + C trong giao diện dòng lệnh, ta muốn gửi một tín hiệu SIGINT để yêu cầu dừng thực thi tiến trình. Điều này giúp dừng tiến trình chạy lâu hoặc không cần thiết. Tín hiệu SIGTERM để dừng tiến trình nhưng cho thời gian dọn dẹp, SIGKILL dừng ngay lập tức, SIGTSTP tạm dừng tiến trình và SIGCONT để phục hồi trạng thái chạy.

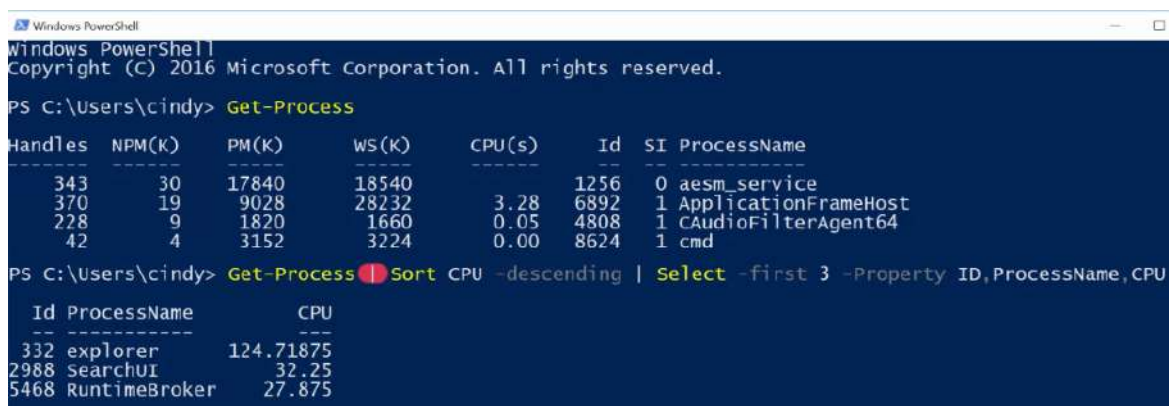
3. Quản lý tài nguyên hệ thống

Theo dõi tài nguyên hệ thống trên Windows

Có nhiều công cụ trong Windows để có thể theo dõi tài nguyên của hệ thống. Một số công cụ chúng ta đã điểm qua như Task Manager, hay Process Explorer. Một công cụ chuyên biệt hơn là Resource Monitoring và đã được tích hợp sẵn. Chương trình cho phép xem dung lượng CPU, mức tiêu thụ bộ nhớ, đọc/xuất của đĩa, truyền/nhận dữ liệu qua mạng. Đây là những tài nguyên ảnh hưởng nhiều đến tốc độ của các tiến trình thực thi trong máy tính.



Lệnh `Get-Process` trong PowerShell cũng thể hiện thông tin tài nguyên đang được sử dụng bởi các tiến trình. Kết quả của lệnh này có thể được xử chuỗi qua toán tử pipe để lọc các kết quả mà chúng ta mong muốn. Ví dụ, lệnh `Get-Process | Sort CPU -descending | Select -first 3 -Property ID, ProcessName, CPU`. Lệnh này lấy kết quả từ `Get-Process` và sắp xếp chúng giảm dần theo cột CPU, sau đó chọn ra 3 tiến trình đầu tiên trong danh sách để trả về. Thông tin trình bày trên màn hình chỉ cần 3 cột là ID, nên tiến trình và mức CPU tiêu thụ.



```

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> Get-Process

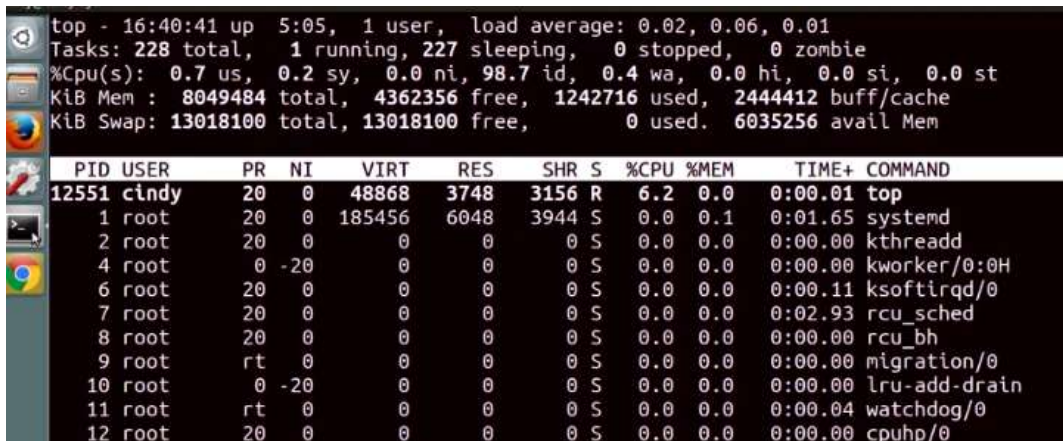
Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI  ProcessName
-----
343      30      17840  18540  3.28    1256  0  aesm_service
370      19      9028   28232  0.05    6892  1  ApplicationFrameHost
228      9       1820   1660   0.00    4808  1  CAudioFilterAgent64
42       4       3152   3224   0.00    8624  1  cmd

PS C:\Users\cindy> Get-Process | Sort CPU -descending | Select -first 3 -Property ID, ProcessName, CPU

Id ProcessName  CPU
--
332 explorer    124.71875
2988 SearchUI    32.25
5468 RuntimeBroker 27.875
  
```

Theo dõi tài nguyên hệ thống trên Linux

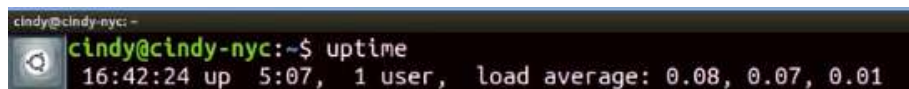
Lệnh top trên Linux thể hiện danh sách các tiến trình sử dụng nhiều tài nguyên nhất trên máy tính. Danh sách này cập nhật liên tục theo trạng thái hiện tại của hệ thống.



```
top - 16:40:41 up 5:05, 1 user, load average: 0.02, 0.06, 0.01
Tasks: 228 total, 1 running, 227 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.7 us, 0.2 sy, 0.0 ni, 98.7 id, 0.4 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 8049484 total, 4362356 free, 1242716 used, 2444412 buff/cache
KiB Swap: 13018100 total, 13018100 free, 0 used. 6035256 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12551	cindy	20	0	48868	3748	3156	R	6.2	0.0	0:00.01	top
1	root	20	0	185456	6048	3944	S	0.0	0.1	0:01.65	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
4	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
6	root	20	0	0	0	0	S	0.0	0.0	0:00.11	ksoftirqd/0
7	root	20	0	0	0	0	S	0.0	0.0	0:02.93	rcu_sched
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
10	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	lru-add-drain
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.04	watchdog/0
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0

Ngoài lệnh top, ta có thể sử dụng lệnh uptime để thể hiện thông tin tài nguyên được sử dụng bởi mỗi người dùng như số lượng người dùng, tổng thời gian chạy, mức CPU tiêu thụ trung bình.



```
cindy@cindy-nyc: ~$ uptime
16:42:24 up 5:07, 1 user, load average: 0.08, 0.07, 0.01
```

Trong một số tình huống ta cần biết tiến trình nào đang làm việc trên tập tin nào. Lệnh lsof trả về danh sách các tập tin đang mở và tiến trình đang sử dụng chúng.

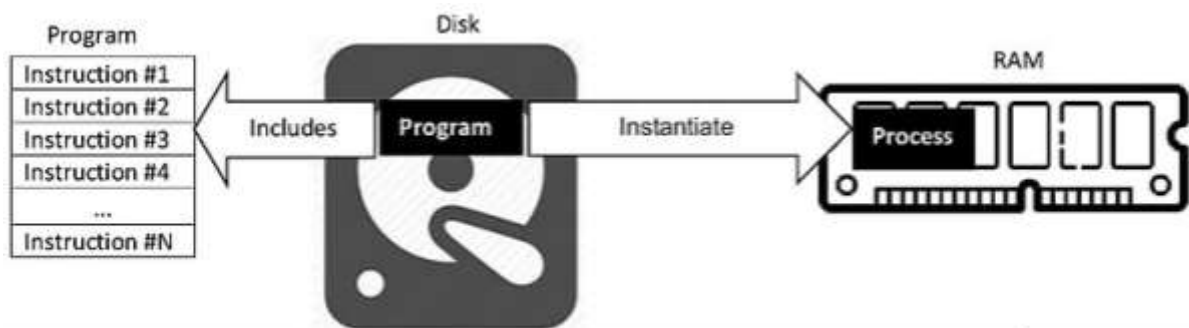
```
cindy@cindy-nyc: ~
ls -lsof 12573 cindy mem REG 8,2 456632 1315474 /lib/x86_64-linux-
e.so.3.13.2
ls -lsof 12573 cindy mem REG 8,2 1868984 1315345 /lib/x86_64-linux-
.23.so
ls -lsof 12573 cindy mem REG 8,2 130224 1315503 /lib/x86_64-linux-
linux.so.1
ls -lsof 12573 cindy mem REG 8,2 162632 1315317 /lib/x86_64-linux-
3.so
ls -lsof 12573 cindy 0u CHR 136,1 0t0 4 /dev/pts/1
ls -lsof 12573 cindy 1u CHR 136,1 0t0 4 /dev/pts/1
ls -lsof 12573 cindy 2u CHR 136,1 0t0 4 /dev/pts/1
ls -lsof 12573 cindy 3r DIR 0,4 0 1 /proc
ls -lsof 12573 cindy 4r DIR 0,4 0 206420 /proc/12573/fd
ls -lsof 12573 cindy 5w FIFO 0,10 0t0 206425 pipe
ls -lsof 12573 cindy 6r FIFO 0,10 0t0 206426 pipe
ls -lsof 12574 cindy cwd DIR 8,2 4096 3014658 /home/cindy
ls -lsof 12574 cindy rtd DIR 8,2 4096 2 /
ls -lsof 12574 cindy txt REG 8,2 163224 4719351 /usr/bin/ls
ls -lsof 12574 cindy mem REG 8,2 10219008 4726010 /usr/lib/locale/lc
```

Bài đọc 7: Quản Lý Tiến Trình

1. Vòng đời của tiến trình

Tiến trình

Tiến trình (process) là một chương trình đang ở trạng thái thực thi, trong khi đó chương trình là một ứng dụng, một đoạn mã trên vùng nhớ mà chúng ta chưa chạy. Chúng ta có thể tạo ra nhiều tiến trình của một chương trình. Ví dụ, khi mở nhiều lần chương trình notepad trên Windows, mỗi một cửa sổ chúng ta nhìn thấy là một tiến trình của một chương trình duy nhất là Notepad.

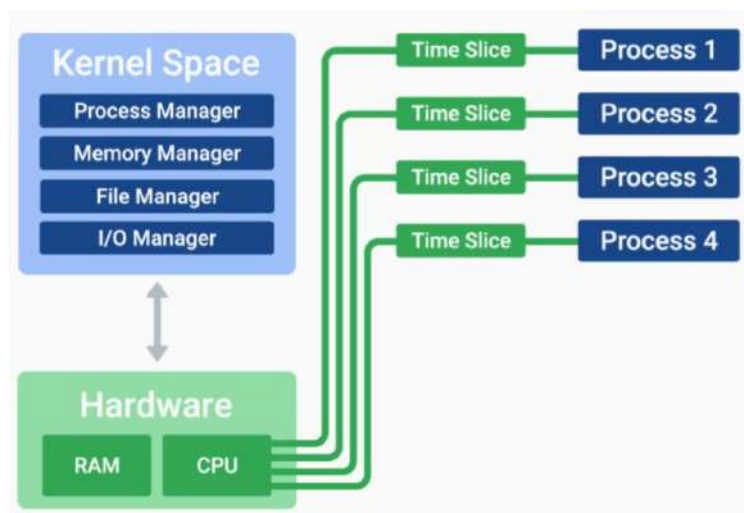


Nguồn: wikipedia

















Trình duyệt web như Google Chrome khi thực thi sẽ tạo nhiều tiến trình ứng với mỗi thẻ được mở.



Trong quá trình thực thi, mỗi tiến trình đều cần tài nguyên như RAM, CPU, v.v. Tuy nhiên tài nguyên trong máy tính là hữu hạn, ví dụ, chỉ có 1 CPU trong khi đó có đến 10 tiến trình đều muốn dùng, thì việc quản lý và chia sẻ tài nguyên giữa các tiến trình trở nên quan trọng. Việc luân chuyển tài nguyên sẽ giúp trải nghiệm của người dùng hệ thống trở nên tốt hơn. Một công cụ giúp hệ điều hành có thể làm được điều đó là lát cắt thời gian (time slice). Đó là khoảng thời gian đủ ngắn để HĐH ngắt một tiến trình (tức là đòi lại tài nguyên) và xem xét việc có nên cấp tiếp hay cấp cho một tiến trình khác hay không. Các quyết định này được thực hiện bởi bộ lập lịch (scheduler).



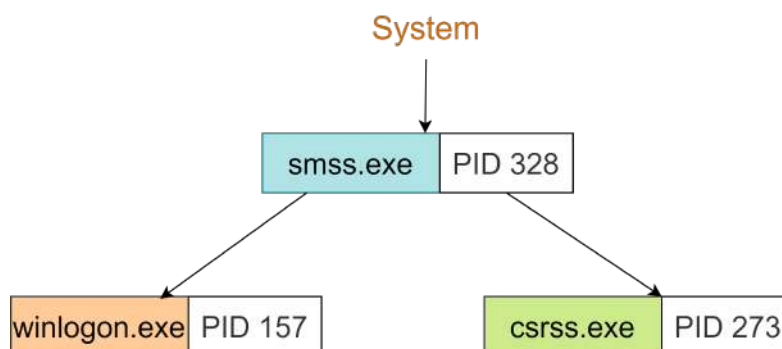
Mỗi tiến trình được gán một mã định danh (Process ID, PID) để phân biệt với các tiến trình khác đang chạy trong hệ thống. Mã này cũng được sử dụng như một tham số cho các lệnh mà chúng ta sẽ đề cập trong các phần tiếp theo.

Name	PID	Status
 chrome.exe	1928	Running
 chrome.exe	17852	Running
 chrome.exe	16568	Running
 chrome.exe	5288	Running
 chrome.exe	16944	Running
 chrome.exe	10004	Running
 chrome.exe	11808	Running
 chrome.exe	4240	Running
 chrome.exe	2808	Running
 chrome.exe	17208	Running
 chrome.exe	17272	Running
 chrome.exe	9448	Running
 chrome.exe	11624	Running
 chrome.exe	1728	Running
 chrome.exe	10840	Running
 chrome.exe	6632	Running

Ngoài các tiến trình mà chúng ta chủ động thực thi một chương trình cụ thể, hệ thống còn có các loại tiến trình khác chạy ngầm bên dưới. Người dùng thông thường sẽ không thấy và không tương tác trực tiếp với các tiến trình này nhưng chúng lại cần thiết để hệ thống làm việc một cách chặt chẽ. Một số tiến trình chạy ngầm như tiến trình lập lịch, quản lý mạng, ghi nhật ký sự kiện, v.v... Các hacker cũng lợi dụng loại tiến trình này để thực thi các tiến trình chạy ngầm gây hại cho hệ thống và người dùng.

Tạo và kết thúc tiến trình

Khi Windows khởi động, một tiến trình được xem gần như đầu tiên thực hiện là Session Manager Subsystem. Tiến trình này thiết lập một số cấu hình khởi tạo cho hệ điều hành. Sau đó nó sẽ khởi động tiến trình đăng nhập cùng với tiến trình Client/Server Runtime Subsystem để thực thi giao diện đồ họa và giao diện dòng lệnh.

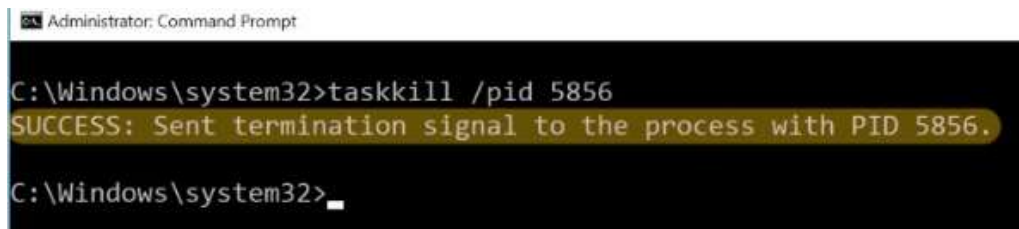


Mỗi tiến trình trên Windows khi được tạo mới, chúng sẽ được tạo bởi một tiến trình cha. Tiến trình con thừa kế một số tính chất từ tiến trình cha nhưng sau đó hoạt động độc lập với tiến trình cha. Ví dụ, nếu bắt đầu notepad.exe từ PowerShell thì tiến trình cha sẽ là PowerShell và tiến trình con là notepad. Khi tiến trình notepad chạy, nó sẽ độc lập với tiến trình PowerShell. Việc đóng PowerShell sẽ không ảnh hưởng đến tiến trình notepad đang chạy.

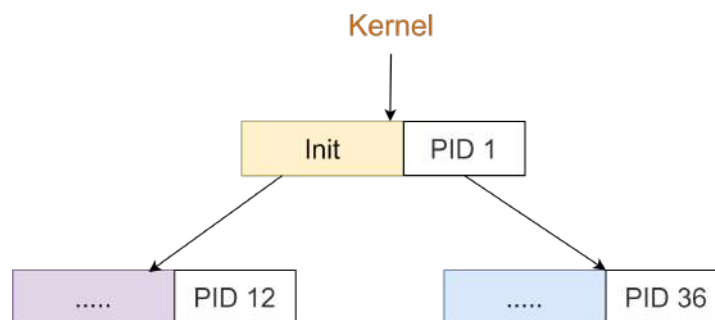


Trong giao diện dòng lệnh, ta có thể sử dụng lệnh `taskkill` để hủy tiến trình đang chạy. Cú pháp là `taskkill /pid process_id`. Có thể thấy, để hủy tiến trình ta cần biết mã của tiến trình thay vì tên của chương trình đang chạy. Trong các phần sau, chúng tôi sẽ trình bày nơi để có thể xem mã tiến trình này.

`taskkill /pid process_id`



Đối với Linux, tiến trình đầu tiên được thực thi là tiến trình `init`. Tiếp theo, tiến trình `init` sẽ khởi tạo các tiến trình khác thực thi trong hệ điều hành.

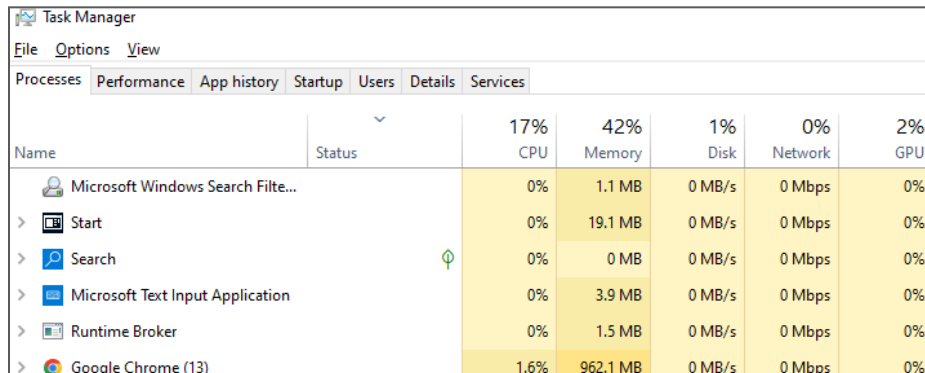


Để hủy tiến trình lên Linux, chúng ta sử dụng lệnh kill cùng với mã của tiến trình. Nếu không có cờ nào bật lên nghĩa là dừng tiến trình nhưng cho thời gian để tiến trình dọn dẹp và giải phóng tài nguyên một cách an toàn. Tuy nhiên, nếu lệnh kill có thêm cờ -KILL thì tiến trình được yêu cầu dừng ngay lập tức, tức là không cho thời gian để dọn dẹp. Nếu thay thế bằng cờ -TSTP nghĩa là ta muốn tạm dừng tiến trình và cờ -CONT là tiếp tục thực hiện tiến trình đó.

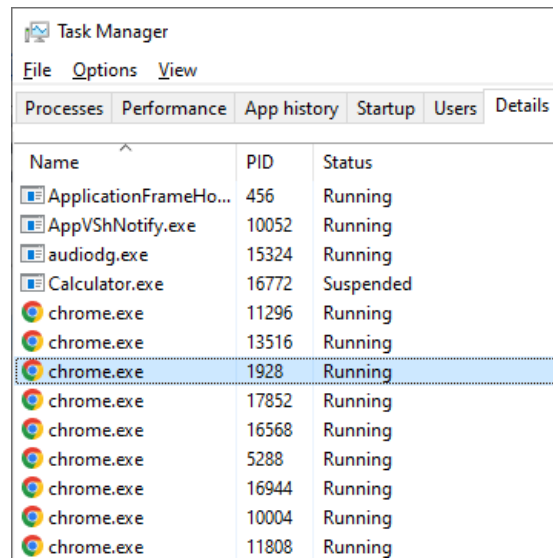
2. Quản lý tiến trình

Quản lý tiến trình trên Windows

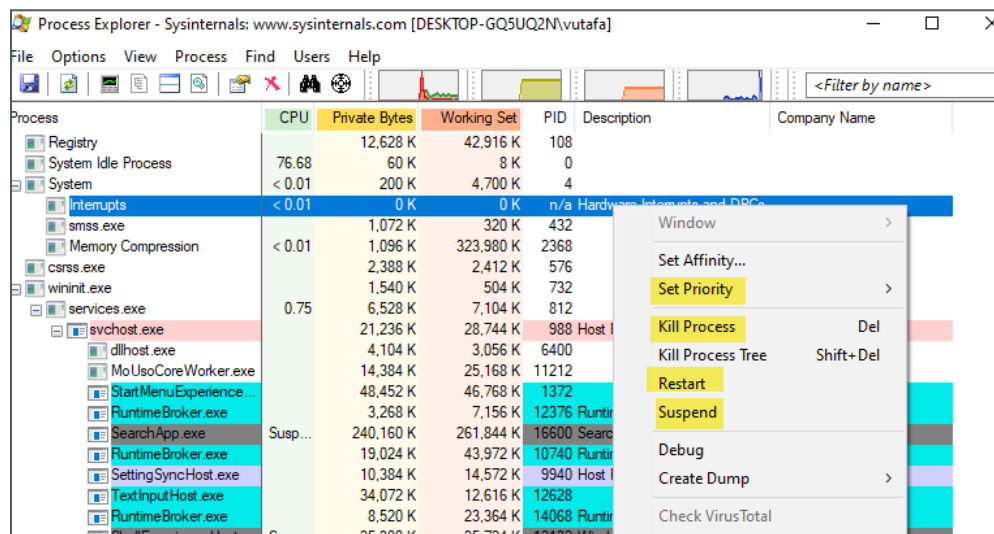
Chương trình Task Manager (taskmgr.exe) quản lý các chương trình, tiến trình đang thực hiện trên máy cùng với các thông tin như tài nguyên CPU, bộ nhớ đã sử dụng. Ngoài ra chúng ta có thể tạo hay hủy tiến trình, xem mã tiến trình trên cửa sổ.



Name	Status	17% CPU	42% Memory	1% Disk	0% Network	2% GPU
Microsoft Windows Search Filte...		0%	1.1 MB	0 MB/s	0 Mbps	0%
> Start		0%	19.1 MB	0 MB/s	0 Mbps	0%
> Search		0%	0 MB	0 MB/s	0 Mbps	0%
> Microsoft Text Input Application		0%	3.9 MB	0 MB/s	0 Mbps	0%
> Runtime Broker		0%	1.5 MB	0 MB/s	0 Mbps	0%
> Google Chrome (13)		1.6%	962.1 MB	0 MB/s	0 Mbps	0%



Microsoft còn phát triển một công cụ có tên là Process Explorer để bổ sung thêm các tính năng tăng cường trong quản lý tiến trình. Công cụ này không được tích hợp sẵn mà cần tải từ trang của Microsoft. Một số tính năng bổ sung như điều chỉnh độ ưu tiên, tạm dừng hay khởi động lại tiến trình, xem danh sách các tiến trình con, v.v... Lưu ý, khi khởi động lại tiến trình nào đó thì tiến trình cha của tiến trình này sẽ là tiến trình process explorer, chính là chương trình chúng ta đang tương tác đến.



Đối với giao diện dòng lệnh, ta có thể sử dụng lệnh `tasklist` hoặc lệnh `Get-Process` để liệt kê tất cả các tiến trình đang chạy trong hệ thống cùng với các thông tin liên quan như mã tiến trình, tài nguyên sử dụng.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vutafa> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
475	27	16192	12808	0.58	456	6	ApplicationFrameHost
152	8	1580	488		10052	0	AppVShNotify
204	12	7360	13120	0.66	6516	0	audiodg
596	30	42132	808	0.77	16772	6	Calculator
375	19	115416	176296	6.28	692	6	chrome
262	18	105524	73536	30.20	1728	6	chrome
758	50	264016	155708	346.86	1928	6	chrome
243	16	24404	8268	0.47	2808	6	chrome

Quản lý tiến trình trên Linux

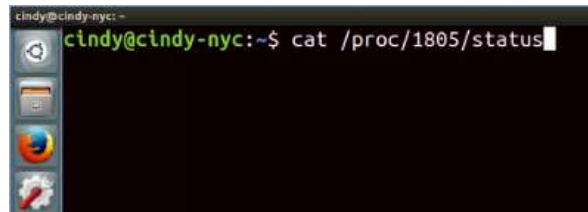
Trên Linux, lệnh `ps` được sử dụng để liệt kê các tiến trình đang chạy trong hệ thống. Kết quả trả về bao gồm mã tiến trình trong cột PID, trạng thái tiến trình, thời gian CPU thực thi, lệnh dùng để chạy tiến trình.

```
cindy@cindy-nyc:~$ ps -x
```

PID	TTY	STAT	TIME	COMMAND
1245	?	Ss	0:00	/lib/systemd/systemd --user
1248	?	S	0:00	(sd-pam)
1295	?	Sl	0:00	/usr/bin/gnome-keyring-daemon --daemonize
1299	?	Ss	0:00	/sbin/upstart --user
1420	?	S	0:00	upstart-udev-bridge --daemon --user
1442	?	Ss	0:01	dbus-daemon --fork --session --address=un
1468	?	Ss	0:00	/usr/lib/x86_64-linux-gnu/hud/window-stac
1545	?	Ssl	0:02	/usr/lib/x86_64-linux-gnu/bamf/bamfdaemon
1548	?	S	0:00	upstart-dbus-bridge --daemon --system --u
1549	?	S	0:00	upstart-file-bridge --daemon --user
1553	?	S	0:00	upstart-dbus-bridge --daemon --session --
1566	?	Ssl	0:20	/usr/bin/ibus-daemon --daemonize --xim --
1576	?	Sl	0:00	/usr/lib/gvfs/gvfsd
1582	?	Sl	0:00	/usr/lib/gvfs/gvfsd-fuse /run/user/1000/g
1586	?	Sl	0:00	/usr/lib/ibus/ibus-dconf

Tương tự như các thiết bị được cắm vào máy tính, Linux đối xử mọi thứ như tập tin kể cả với tiến trình. Các tiến trình là các tập tin nằm trong thư mục /proc. Do đó để liệt kê các tiến trình, ta có thể sử dụng lệnh ls. Để xem thông tin hay trạng thái chi tiết của tiến trình, ta sử dụng lệnh cat.

```
cindy@cindy-nyc:~$ ls -l /proc
total 0
dr-xr-xr-x 9 root      root      0 Oct 10 11:34 1
dr-xr-xr-x 9 root      root      0 Oct 10 11:34 10
dr-xr-xr-x 9 root      root      0 Oct 10 11:34 100
dr-xr-xr-x 9 root      root      0 Oct 10 11:34 101
dr-xr-xr-x 9 cindy     cindy     0 Oct 10 15:10 10116
dr-xr-xr-x 9 cindy     cindy     0 Oct 10 15:10 10123
dr-xr-xr-x 9 cindy     cindy     0 Oct 10 15:15 10168
dr-xr-xr-x 9 root      root      0 Oct 10 11:34 102
```



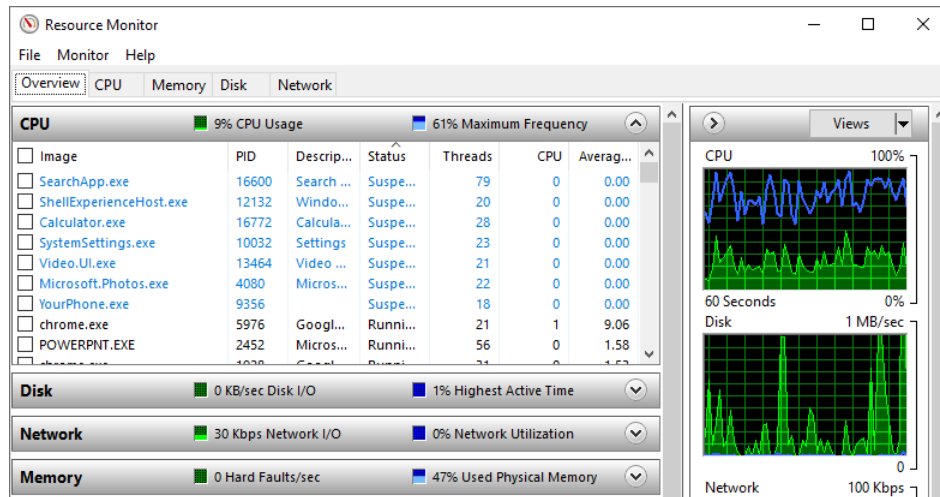
```
cindy@cindy-nyc:~$ cat /proc/1805/status
```

Trong quá trình một tiến trình thực thi, chúng ta có thể giao tiếp với chúng qua hình thức gửi tín hiệu. Ví dụ, khi nhấn tổ hợp phím Ctrl + C trong giao diện dòng lệnh, ta muốn gửi một tín hiệu SIGINT để yêu cầu dừng thực thi tiến trình. Điều này giúp dừng tiến trình chạy lâu hoặc không cần thiết. Tín hiệu SIGTERM để dừng tiến trình nhưng cho thời gian dọn dẹp, SIGKILL dừng ngay lập tức, SIGTSTP tạm dừng tiến trình và SIGCONT để phục hồi trạng thái chạy.

3. Quản lý tài nguyên hệ thống

Theo dõi tài nguyên hệ thống trên Windows

Có nhiều công cụ trong Windows để có thể theo dõi tài nguyên của hệ thống. Một số công cụ chúng ta đã điểm qua như Task Manager, hay Process Explorer. Một công cụ chuyên biệt hơn là Resource Monitoring và đã được tích hợp sẵn. Chương trình cho phép xem dung lượng CPU, mức tiêu thụ bộ nhớ, đọc/xuất của đĩa, truyền/nhận dữ liệu qua mạng. Đây là những tài nguyên ảnh hưởng nhiều đến tốc độ của các tiến trình thực thi trong máy tính.



Lệnh `Get-Process` trong PowerShell cũng thể hiện thông tin tài nguyên đang được sử dụng bởi các tiến trình. Kết quả của lệnh này có thể được xử chuỗi qua toán tử pipe để lọc các kết quả mà chúng ta mong muốn. Ví dụ, lệnh `Get-Process | Sort CPU -descending | Select -first 3 -Property ID, ProcessName, CPU`. Lệnh này lấy kết quả từ `Get-Process` và sắp xếp chúng giảm dần theo cột CPU, sau đó chọn ra 3 tiến trình đầu tiên trong danh sách để trả về. Thông tin trình bày trên màn hình chỉ cần 3 cột là ID, tên tiến trình và mức CPU tiêu thụ.

```

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> Get-Process

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
343 30 17840 18540 3.28 1256 0 aasm_service
370 19 9028 28232 0.05 6892 1 ApplicationFrameHost
228 9 1820 1660 0.00 4808 1 CAudioFilterAgent64
42 4 3152 3224 0.00 8624 1 cmd

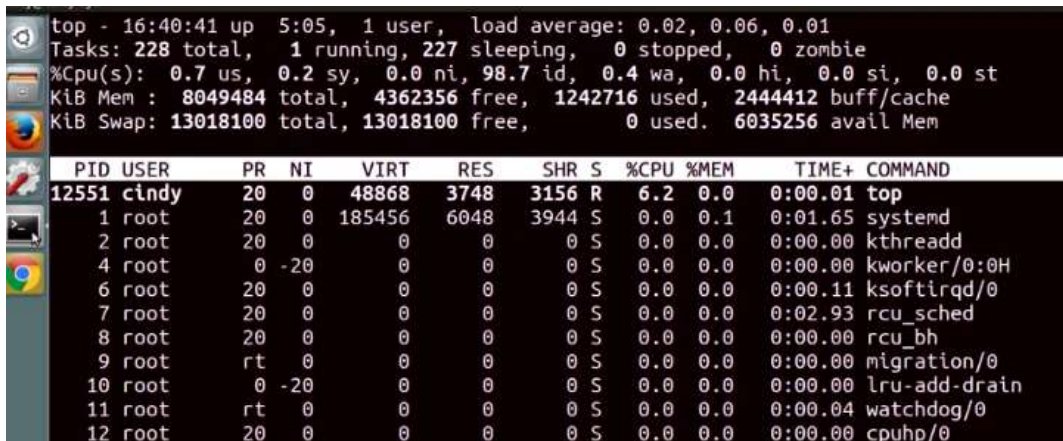
PS C:\Users\cindy> Get-Process | Sort CPU -descending | Select -first 3 -Property ID, ProcessName, CPU

Id ProcessName CPU
---
332 explorer 124.71875
2988 SearchUI 32.25
5468 RuntimeBroker 27.875

```

Theo dõi tài nguyên hệ thống trên Linux

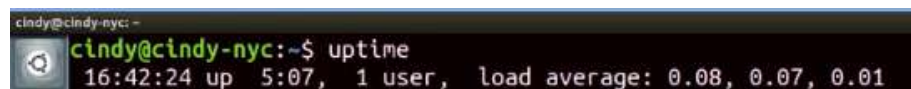
Lệnh top trên Linux thể hiện danh sách các tiến trình sử dụng nhiều tài nguyên nhất trên máy tính. Danh sách này cập nhật liên tục theo trạng thái hiện tại của hệ thống.



```
top - 16:40:41 up 5:05, 1 user, load average: 0.02, 0.06, 0.01
Tasks: 228 total, 1 running, 227 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.7 us, 0.2 sy, 0.0 ni, 98.7 id, 0.4 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 8049484 total, 4362356 free, 1242716 used, 2444412 buff/cache
KiB Swap: 13018100 total, 13018100 free, 0 used. 6035256 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12551	cindy	20	0	48868	3748	3156	R	6.2	0.0	0:00.01	top
1	root	20	0	185456	6048	3944	S	0.0	0.1	0:01.65	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
4	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
6	root	20	0	0	0	0	S	0.0	0.0	0:00.11	ksoftirqd/0
7	root	20	0	0	0	0	S	0.0	0.0	0:02.93	rcu_sched
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
10	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	lru-add-drain
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.04	watchdog/0
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0

Ngoài lệnh top, ta có thể sử dụng lệnh uptime để thể hiện thông tin tài nguyên được sử dụng bởi mỗi người dùng như số lượng người dùng, tổng thời gian chạy, mức CPU tiêu thụ trung bình.



```
cindy@cindy-nyc: ~$ uptime
16:42:24 up 5:07, 1 user, load average: 0.08, 0.07, 0.01
```

Trong một số tình huống ta cần biết tiến trình nào đang làm việc trên tập tin nào. Lệnh lsof trả về danh sách các tập tin đang mở và tiến trình đang sử dụng chúng.



```
cindy@cindy-nyc: ~$ lsof
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	FILE
lsof	12573	cindy	mem	REG		8,2	/lib/x86_64-linux...
e-so.3.13.2	12573	cindy	mem	REG		8,2	/lib/x86_64-linux...
lsof	12573	cindy	mem	REG		8,2	/lib/x86_64-linux...
lsof	12573	cindy	mem	REG		8,2	/lib/x86_64-linux...
lsof	12573	cindy	0u	CHR		136,1	/dev/pts/1
lsof	12573	cindy	1u	CHR		136,1	/dev/pts/1
lsof	12573	cindy	2u	CHR		136,1	/dev/pts/1
lsof	12573	cindy	3r	DIR		0,4	/proc
lsof	12573	cindy	4r	DIR		0,4	/proc/12573/fd
lsof	12573	cindy	5w	FIFO		0,10	/proc/12573/p1pe
lsof	12573	cindy	6r	FIFO		0,10	/proc/12573/p1pe
lsof	12574	cindy	cwd	DIR		8,2	/home/cindy
lsof	12574	cindy	rtd	DIR		8,2	/
lsof	12574	cindy	txt	REG		8,2	/usr/bin/lsof
lsof	12574	cindy	mem	REG		8,2	/usr/lib/locale/L...

Phần 2

HƯỚNG DẪN

TRẢ LỜI CÂU HỎI

Điều hướng hệ thống

1. Sử dụng máy Linux, bạn có cây thư mục sau:

Nếu đường dẫn hiện tại của bạn là /home/cindy/Pictures/Canada và bạn muốn chuyển sang thư mục Alaska, bạn có thể sử dụng lệnh nào sau đây? Đánh dấu vào tất cả những gì phù hợp.

- A. `cd ~/Pictures/Alaska`
- B. `cd ../Alaska`
- C. `cd /Pictures/Alaska`
- D. `cd /home/cindy/Pictures/Alaska`

Đáp án: A, B, D

2. Trong Bash, bạn có thể sử dụng lệnh nào sau đây để xem một danh sách dạng dài của tất cả các tệp trong thư mục /home? Đánh dấu vào tất cả các câu phù hợp.

- A. `list -a /home`
- B. `ls -la /home`
- C. `ls -l -a /home`
- D. `ls -la ~`

Đáp án: B, C

3. Trong Bash, bạn có thể sử dụng lệnh nào sau đây để xóa thư mục có tên: “Miscellaneous Directory”?

- A. `rm Miscellaneous Directory`
- B. `rm -r Miscellaneous Directory`
- C. `rm Miscellaneous\ Directory`
- D. `rm -r Miscellaneous\ Directory`

Đáp án: D

4. Trong Bash, bạn có thể sử dụng lệnh nào sau đây để xem nội dung của tài liệu. Đánh dấu vào tất cả những gì phù hợp.

- A. open
- B. cat
- C. less
- D. dog

Đáp án: B, C

5. Trong máy Linux, bạn có các tập tin sau: apple.txt, banana.jpg, chocolate.txt, cam.txt

Để tìm từ "fruit" trong các tập tin văn bản trên có thể dùng lệnh gì? Đánh dấu vào tất cả những câu phù hợp.

- A. grep fruit apple.txt chocolate.txt orange.txt
- B. grep fruit *.txt
- C. find fruit apple.txt chocolate.txt
- D. find fruit apple.txt chocolate.txt orange.txt

Đáp án: A, B

6. Trong máy Linux, bạn có một tập tin có tên "styles_of_fish.txt" và bạn muốn nối từ "trout" vào nội dung tập tin. Bạn có thể sử dụng lệnh nào sau đây?

- A. echo trout < types_of_fish.txt
- B. echo trout > types_of_fish.txt
- C. echo trout >> types_of_fish.txt
- D. echo trout 2> types_of_fish.txt

Đáp án: C

7. Trong máy Linux, bạn muốn duyệt qua qua một thư mục có tên

/home/ben/Documents và tìm kiếm từ "important" trong tên các tập tin có trong thư mục này. Bạn có thể sử dụng lệnh nào sau đây?

- A. `ls /home/ben/Documents | grep important`
- B. `ls /home/ben/Documents >> grep important`
- C. `ls /home/ben/Documents < grep important`
- D. `ls /home/ben/Documents > grep important`

Đáp án: A

Quyền truy cập hệ thống

1. Các quyền tập tin cơ bản trên linux là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Đọc (read)
- B. Viết (write)
- C. Điều chỉnh (modify)
- D. Thực thi (execute)

Đáp án: A, B, D

2. Bạn được cung cấp kết quả đầu ra của lệnh `ls -l` trong Linux như sau:

```
ls -l books_file
```

```
dr-x-wxr-- 1 phelan cool_group 0 Aug 20 11:10 books_file
```

Trả lời câu hỏi sau: Ký tự đầu tiên của kết quả mô tả điều gì?

- A. Người sở hữu tập tin là một người dùng lớp D
- B. Người sở hữu tập tin có quyền xóa
- C. `books_file` là một thư mục
- D. `books_file` là một thiết bị đĩa

Đáp án: C

3. Bạn được cung cấp kết quả đầu ra của lệnh `ls -l` trong Linux như sau:

```
ls -l books_file
```

```
dr-x-wxr-- 1 phelan cool_group 0 Aug 20 11:10 books_file
```

Trả lời câu hỏi sau: Bộ ba bit cuối cùng (r--) trong quyền và thuộc tính tập tin đề cập đến ai?

- A. Người sở hữu
- B. Tất cả người sử dụng khác
- C. Nhóm mà tập tin thuộc về
- D. Tập tin thông thường

Đáp án: B

4. Bạn được cung cấp kết quả đầu ra của lệnh `ls -l` trong Linux như sau:

```
ls -l books_file
```

```
dr-x-wxr-- 1 phelan cool_group 0 Aug 20 11:10 books_file
```

Trả lời câu hỏi sau: Bộ ba bit thứ hai (-wx) cung cấp cho bạn những quyền nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Đọc (read)
- B. Viết (write)
- C. Thực thi (execute)
- D. Nhóm mà tập tin thuộc về

Đáp án: B

5. Nếu tôi muốn thay đổi quyền của một tập tin có tên `honey_bears`, tôi có thể sử dụng lệnh nào để cấp quyền ghi cho chủ sở hữu của tập tin này mà không thay đổi các quyền khác? Chủ sở hữu hiện chỉ có quyền truy cập đọc vào tập tin này. Đánh dấu vào tất cả các câu phù hợp.

- A. `chmod u+w honey_bears`
- B. `chmod o+w honey_bears`
- C. `chmod 644 honey_bears`
- D. `chmod 400 honey_bears`

Đáp án: A

Quản lý phần mềm và gói phần mềm

1. Sự khác biệt giữa tập tin EXE và tập tin MSI là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Tập tin MSI là một tập tin thực thi có thể cung cấp cho bạn toàn quyền kiểm soát đối với cách cài đặt ứng dụng của bạn.
- B. Tập tin EXE là một tập tin thực thi có thể chứa tập tin MSI như tài nguyên của nó.
- C. Tập tin MSI được trình cài đặt Windows sử dụng để kiểm soát cách ứng dụng cài đặt.

Đáp án: B, C

2. Khi nào bạn muốn sử dụng tập tin MSI để hướng dẫn cài đặt một chương trình, thay vì EXE?

- A. Khi bạn muốn hoàn tất, kiểm soát tùy chỉnh cách ứng dụng được cài đặt.
- B. Khi bạn muốn trình cài đặt Windows thực hiện việc ghi sổ và thiết lập cho ứng dụng của mình, với đánh đổi là tuân theo các quy tắc mà trình cài đặt yêu cầu.
- C. Khi bạn muốn có thể cài đặt ứng dụng của mình trên Linux cũng như Windows.

Đáp án: B

3. Nếu bạn đang thực hiện cài đặt từ dòng lệnh trong Windows, thì phương pháp tốt nhất để kiểm tra các tùy chọn mà gói cài đặt cung cấp là gì? Đánh dấu

vào tất cả các câu phù hợp.

- A. Sử dụng các cờ /?, /h hoặc /help khi chạy gói để xem chúng có cung cấp bất kỳ thông tin hữu ích nào không.
- B. Tham khảo tài liệu của ứng dụng để xem họ cung cấp những tùy chọn nào.
- C. Quyết định rằng bạn không muốn cài đặt ứng dụng từ dòng lệnh và sử dụng GUI để thay thế.

Đáp án: A, B

4. Sự khác biệt giữa apt và dpkg là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. dpkg được sử dụng như một lệnh cho gói phần mềm Debian độc lập
- B. apt được sử dụng như một trình quản lý gói
- C. apt cài đặt các gói phụ thuộc
- D. dpkg cài đặt các gói phụ thuộc

Đáp án: A, B, C

5. Đuôi mở rộng tập tin nào sau đây được coi là tập tin lưu trữ trong Windows?

Đánh dấu vào tất cả các câu phù hợp.

- A. .tar
- B. .exe
- C. .zip
- D. .rar

Đáp án: A, C, D

6. Lệnh PowerShell nào mà bạn có thể sử dụng để giải nén và nén các kho lưu trữ?

- A. 7Zip
- B. tar
- C. Compress-Archive

Đáp án: C

7. Mục đích của DLL trong Windows là gì?

- A. Để chia sẻ một gói mã nguồn hữu ích giữa các chương trình
- B. Để chiếm dung lượng trên ổ cứng của bạn
- C. Hướng dẫn cài đặt gói thông qua Windows Installer

Đáp án: A

8. Hầu hết các thư viện dùng chung trong Windows được quản lý bằng cách nào sau đây?

- A. Hợp nhất Side-by-Side (SxS)
- B. Phụ thuộc trái và phải (LRAs)
- C. Thư viện liên kết động (DLL)

Đáp án: A

9. Tập lệnh chính xác cần sử dụng để tìm một gói phần mềm trong các nguồn gói có sẵn từ dòng lệnh PowerShell là gì?

- A. Register-PackageSource
- B. Get-PackageSource
- C. Find-Package

Đáp án: C

10. Lệnh PowerShell nào sau đây sẽ cài đặt gói "awesomesoftware" từ kho phần mềm Chocolatey?

- A. Install-Package -Name awesomesoftware -Source chocolatey
- B. Install-Package -Name chocolatey -Source awesomesoftware
- C. Install-Package -Name awesomesoftware -Source MicrosoftWindows

Đáp án: A

11. Trước khi cài đặt phần mềm, bạn nên chạy lệnh nào sau đây để tải phiên bản cập nhật của phần mềm?

- A. apt install
- B. apt update
- C. apt remove
- D. apt search

Đáp án: B

12. Công cụ nào sau đây cho phép bạn tạo hoặc chỉnh sửa tệp MSI?

- A. Process monitor
- B. Orca
- C. Setup.exe

Đáp án: B

13. Thông tin nào sau đây là thông tin mà Windows sẽ sử dụng để tìm kiếm trình điều khiển (driver) phù hợp cho phần cứng mới được kết nối với máy tính Windows?

- A. Mã cắm và chạy (PnP code)
- B. Mã phần cứng (Hardware ID)
- C. Số định danh điều khiển (Drive Identification Number)

Đáp án: B

14. Trên Linux, trong thư mục /dev, các thiết bị bắt đầu bằng sd có thể được liên kết với loại thiết bị nào? Đánh dấu vào tất cả các câu phù hợp.

- A. Speaker (loa)

- B. Hard drive (ổ cứng)
- C. USB drive (ổ USB)
- D. Memory stick (thẻ nhớ)

Đáp án: B, C, D

15. Điều nào sau đây mô tả đúng về "Bản vá bảo mật?"

- A. Một mảnh phần mềm nhằm khắc phục lỗ hổng bảo mật
- B. Một mảnh vải dùng để vá một sợi cáp bị đứt
- C. Một phiên bản hệ điều hành hoàn toàn mới, an toàn hơn

Đáp án: A

Hệ thống tập tin

1. Đặc điểm nào sau đây là đặc điểm của hệ thống tập tin FAT32? Đánh dấu vào tất cả các câu phù hợp.

- A. Nó không hỗ trợ các tập tin lớn hơn 4GB.
- B. Nó đọc và ghi tương thích với hệ điều hành Windows, Mac và Linux.
- C. Kích thước hệ thống tập tin của nó không được lớn hơn 32GB.
- D. Nó hỗ trợ các tập tin có kích thước lên đến 8GB

Đáp án: A, B, C

2. Sự khác biệt giữa bảng phân vùng GPT và MBR là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. MBR chỉ cho phép kích thước phân vùng từ 2TB trở xuống
- B. MBR là tiêu chuẩn mới cho các bảng phân vùng
- C. GPT không có giới hạn về số lượng phân vùng có thể tạo
- D. GPT cho phép bạn có kích thước âm lượng từ 2TB trở lên

Đáp án: A, C, D

3. Trước khi bạn có thể lưu trữ tập tin trên ổ cứng, bạn phải thực hiện thao tác nào sau đây? Đánh dấu vào tất cả các câu phù hợp.

- A. Không cần làm gì; ổ cứng có thể được sử dụng để lưu trữ các tập tin tùy ý
- B. Định dạng một hệ thống tập tin
- C. Phân vùng đĩa cứng
- D. Gắn kết hệ thống tập tin

Đáp án: B, C, D

4. Bạn muốn định dạng một phân vùng bằng NTFS và biết rằng dữ liệu bạn sẽ lưu trữ chủ yếu bao gồm nhiều tập tin nhỏ. Để sử dụng ít không gian nhất có thể, bạn nên chọn kích thước đơn vị phân bổ (Allocation Unit Size) lớn hơn hay nhỏ hơn trong quá trình định dạng?

- A. Kích thước đơn vị phân bổ lớn hơn
- B. Kích thước đơn vị phân bổ nhỏ hơn

Đáp án: B

5. Trong Linux, thiết bị có tên /dev/sdb2 nói đến điều gì?

- A. Ổ đĩa cứng đầu tiên được phát hiện trên hệ thống
- B. Phân vùng thứ hai của đĩa cứng thứ hai được phát hiện trên hệ thống
- C. Ổ cứng B thứ hai
- D. Phân vùng thứ nhất của ổ đĩa cứng thứ hai được phát hiện trên hệ thống

Đáp án: B

6. Đúng hay sai: Nếu bạn muốn tiết kiệm dung lượng trên máy tính Windows, việc xóa tệp pagefile.sys là một ý tưởng hay.

- A. Đúng

B. Sai

Đáp án: B

7. Lệnh nào sau đây trong Windows sẽ tạo một liên kết tượng trưng (symbolic link) có tên “cauliflower” tới tệp có tên “broccoli.txt”?

- A. `mklink cauliflower broccoli.txt`
- B. `mklink broccoli.txt cauliflower`
- C. `mklink /H cauliflower broccoli.txt`

Đáp án: A

8. Đúng hay sai: Trong các phiên bản Windows hiện đại, bạn cần phải chạy định kỳ chương trình chống phân mảnh ổ đĩa (disk defragmentation) một cách thủ công để giữ cho ổ đĩa ở trạng thái tốt.

- A. Đúng
- B. Sai

Đáp án: B

9. Trong Linux, sự khác biệt giữa các lệnh `df` và `du` là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. `df` được sử dụng để xác định dung lượng trống trên toàn bộ máy
- B. `du` được sử dụng để xác định lượng sử dụng đĩa trên một thư mục cụ thể
- C. `df` được sử dụng để xóa các tập tin trong một thư mục
- D. `du` được sử dụng để phục hồi các tập tin trong một thư mục

Đáp án: A, B

10. Trong Linux, sự khác biệt giữa liên kết cứng và liên kết mềm là gì? Đánh dấu vào tất cả các câu phù hợp.

- A. Một liên kết mềm trỏ đến một tên tập tin
- B. Một liên kết cứng trỏ đến một inode
- C. Một liên kết cứng trỏ đến một tên tập tin
- D. Bạn có thể xem số lượng liên kết cứng của một tập tin bằng lệnh `ls -l`

Đáp án: A, B, D

11. Mặc dù NTFS phần lớn là một hệ thống tập tin tự phục hồi, bạn có thể chạy công cụ nào sau đây để xác định và sửa chữa những vị trí bị hỏng nghiêm trọng trên ổ C?

- A. `chkdsk /r c:`
- B. `chkdsk c:`
- C. `fsck c:`

Đáp án: A

12. Nếu bạn muốn tự động gắn kết một hệ thống tập tin khi khởi động máy tính, bạn phải sửa đổi tập tin nào?

- A. `/etc/fstab`
- B. `/dev/sda`
- C. `/etc/sudoers`
- D. `/etc/group`

Đáp án: A

Quản lý tiến trình

1. Đúng hay sai: Các tiến trình Windows có thể hoạt động độc lập với tiến trình cha của chúng.

- A. Đúng
- B. Sai

Đáp án: A

2. Công cụ nào sau đây có thể giúp bạn thu thập thông tin về các tiến trình đang chạy trên hệ điều hành Windows?

- A. Task Manager
- B. Công cụ tasklist từ giao diện dòng lệnh cmd
- C. Lệnh Get-Process trong PowerShell
- D. Tất cả câu trên

Đáp án: D

3. Nếu bạn khởi động lại một tiến trình bằng tiện ích Process Explorer, thì tiến trình cha mới của tiến trình đó sẽ là gì?

- A. cmd.exe
- B. Process Explorer
- C. windows.exe
- D. momanddad.exe

Đáp án: B

4. Lệnh PowerShell nào sau đây cho bạn biết tiến trình nào trên hệ thống đang sử dụng nhiều tài nguyên CPU nhất?

- A. `Get-Process | Sort CPU -descending | Select -first 1 -Property ID,ProcessName,CPU`
- B. `Get-Process | Sort RAM -descending | Select -first 1 -Property ID,ProcessName,CPU`
- C. `cpu_usage.exe | top -1`

Đáp án: A

5. Nếu bạn có một máy tính chậm, một số thủ phạm có thể gây ra điều này là

gì? Chọn tất cả những câu phù hợp.

- A. Việc sử dụng CPU quá cao
- B. Nhiều hoạt động nhập/xuất
- C. Việc sử dụng RAM quá cao
- D. Quá nhiều tiến trình đang chạy

Đáp án: A, B, C, D

6. Trong Linux, bạn có thể sử dụng lệnh nào để kết thúc tiến trình với PID 342 một cách an toàn?

- A. kill 342
- B. kill -KILL 342
- C. kill -TSTP 342
- D. kill -CONT 342

Đáp án: A

7. Trong Linux, bạn có thể sử dụng lệnh nào để kết thúc tiến trình với PID 342 ngay lập tức?

- A. kill 342
- B. kill -KILL 342
- C. kill -TSTP 342
- D. kill -CONT 342

Đáp án: B

8. Trong Linux, bạn có thể sử dụng lệnh nào để tạm dừng một tiến trình có PID là 342?

- A. kill 342

- B. kill -KILL 342
- C. kill -TSTP 342
- D. kill -CONT 342

Đáp án: C

Triển khai hệ điều hành trong thực tế

1. Phần nào của gói PuTTY cho phép bạn thực hiện truyền tập tin bằng giao thức SCP?

- A. pscp.exe
- B. psftp.exe
- C. pageant.exe

Đáp án: A

2. Nếu bạn đang điều tra các sự cố đăng nhập trên máy tính Windows, thì phần nào trong Event Viewer là nơi hợp lý để bạn bắt đầu xem xét?

- A. System
- B. Application and Services
- C. Security

Đáp án: C

3. Bạn có thể tìm thấy thông tin về lỗi khởi động trong tập tin log nào? Đánh dấu vào tất cả các câu phù hợp.

- A. /var/log/syslog
- B. /var/log/auth.log
- C. /var/log/kern.log
- D. /var/log/mail.log

Đáp án: A, C

4. Bạn có thể tìm thấy thông tin về lỗi xác thực trong tập tin log nào?

- A. `/var/log/syslog`
- B. `/var/log/auth.log`
- C. `/var/log/kern.log`
- D. `/var/log/mail.log`

Đáp án: B

5. Để một kết nối ssh hoạt động, điều nào sau đây cần đúng? Đánh dấu vào tất cả các câu phù hợp.

- A. SSH được cài đặt trên máy khách
- B. Máy chủ SSH đang chạy trên máy mà bạn muốn kết nối
- C. VPN cần được cấu hình
- D. Bạn cần xác định một tên miền để thực hiện SSH vào

Đáp án: A, B, D