

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHẠM HOÀNG DUY

BÀI GIẢNG

Hệ điều hành Windows và Linux/ Unix

PTIT.EDU.VN

HÀ NỘI 2016

Lời nói đầu

Hệ điều hành là một bộ phận cấu thành quan trọng của hệ thống máy tính giúp cho con người có thể khai thác và sử dụng hiệu quả hệ thống máy tính. Hiện nay, Windows và Linux/Unix là các hệ điều hành thông dụng cho máy tính để bàn và máy chủ. Bài giảng này giới thiệu các kiến thức cơ bản và chuyên sâu về các vấn đề quản trị của hai hệ điều hành phổ biến này; cụ thể bao gồm: vấn đề quản trị người dùng; các dịch vụ cơ bản và các dịch vụ mạng; vấn đề bảo trì, cập nhật các bản vá hệ điều hành, sao lưu và khôi phục dự phòng, khắc phục lỗi và giám sát hoạt động của hệ điều hành.

Cấu trúc của bài giảng gồm hai phần và 8 chương. Phần I về hệ điều hành Windows và Phần II về hệ điều hành Linux/Unix. Hai phần này đều gồm 4 chương và có cấu trúc đối xứng với nhau. Cụ thể như sau:

Chương đầu giới thiệu tổng quan về các thành phần cơ bản, kiến trúc của hệ điều hành. Chương này cũng trình bày về quá trình phát triển và các mốc quan trọng của hệ điều hành.

Chương thứ hai đề cập chủ yếu đến vấn đề cài đặt và quản trị các thành phần cơ bản của hệ điều hành cho phép người dùng sử dụng và quản trị máy tính như quản lý trình điều khiển thiết bị, người dùng và quyền truy nhập...

Chương tiếp theo giới thiệu cụ thể về cài đặt và quản trị dịch vụ của hệ điều hành. Các dịch vụ được trình bày bao gồm các dịch vụ mạng, chia sẻ file và thư mục qua mạng, Web và truy nhập từ xa.

Chương cuối cùng trình bày về các vấn đề bảo trì, khắc phục và giám sát hoạt động của các dịch vụ mà người quản trị cài đặt.

Mục lục

CHƯƠNG I. GIỚI THIỆU CÁC HỆ ĐIỀU HÀNH MICROSOFT WINDOWS 11

I.1	Lịch sử phát triển	11
I.2	Kiến trúc của hệ điều hành	13
I.3	Giao diện của Windows.....	14
I.4	Hệ thống file của Windows	16
I.5	Giới thiệu Windows Registry	17

CHƯƠNG II. CÀI ĐẶT VÀ QUẢN TRỊ CÁC THÀNH PHẦN CƠ BẢN CỦA WINDOWS19

II.1	Cài đặt Windows	19
II.2	Trình điều khiển thiết bị	24
II.3	Hệ thống lưu trữ.....	25
II.4	Người dùng và quyền truy nhập	26
II.5	Chính sách nhóm	28
II.6	Các dịch vụ của Windows	30

CHƯƠNG III. QUẢN TRỊ CÁC MÁY CHỦ DỊCH VỤ CỦA WINDOWS SERVER32

III.1	Máy chủ dịch vụ DNS và DHCP	32
III.2	Thư mục động.....	38
III.3	Dịch vụ web.....	43
III.4	Dịch vụ file và in ấn	45
III.5	Dịch vụ truy nhập từ xa	48

CHƯƠNG IV. BẢO TRÌ, KHẮC PHỤC LỖI VÀ GIÁM SÁT HOẠT ĐỘNG CỦA WINDOWS50

IV.1	Cập nhật các bản vá Windows.....	50
IV.2	Sao lưu và khôi phục dự phòng.....	51
IV.3	Khắc phục các sự cố trong Windows.....	53
IV.4	Giám sát hoạt động và kiểm toán Windows	55
IV.5	Giới thiệu các công cụ quản trị Windows từ xa.....	57

CHƯƠNG V. GIỚI THIỆU CÁC HỆ ĐIỀU HÀNH LINUX/UNIX.....61

V.1	Lịch sử phát triển	61
V.2	Kiến trúc của hệ điều hành	62
V.3	Giao diện của Linux/Unix	63
V.4	Hệ thống file của Linux/Unix	66
V.5	Các phiên bản chính của Linux/Unix	68

CHƯƠNG VI. CÀI ĐẶT VÀ QUẢN TRỊ CÁC THÀNH PHẦN CƠ BẢN CỦA LINUX/UNIX.....	70
VI.1 Cài đặt Linux/Unix	70
VI.2 Quản trị các trình điều khiển thiết bị	76
VI.3 Hệ thống lưu trữ.....	77
VI.4 Người dùng và quyền truy nhập	80
VI.5 Các dịch vụ của Linux/Unix	83
CHƯƠNG VII. QUẢN TRỊ CÁC MÁY CHỦ DỊCH VỤ CỦA LINUX/UNIX SERVER	87
VII.1 Dịch vụ DNS và DHCP	87
VII.2 Dịch vụ web.....	91
VII.3 Dịch vụ thư điện tử.....	94
VII.4 Dịch vụ file và in ấn	98
VII.5 Dịch vụ truy nhập từ xa	100
CHƯƠNG VIII. BẢO TRÌ, KHẮC PHỤC LỖI VÀ GIÁM SÁT HOẠT ĐỘNG CỦA LINUX/UNIX	102
VIII.1 Cập nhật các bản vá	102
VIII.2 Sao lưu và khôi phục dự phòng	104
VIII.3 Khắc phục các sự cố	106
VIII.4 Giám sát hoạt động và kiểm toán	107
VIII.5 Giới thiệu các công cụ quản trị từ xa.....	113
VIII.6 Lập trình Shell	114

Danh mục các hình vẽ

Hình I-1. Giao diện dòng lệnh của MS-DOS	11
Hình I-2. Giao diện menu và đồ họa Windows 3.1	12
Hình I-3. Kiến trúc cơ bản của hệ điều hành Windows	13
Hình I-4. Giao diện GUI Windows	15
Hình I-5. Danh mục đăng ký trong Windows	18
Hình II-1. Lựa chọn chức năng cài đặt.....	22
Hình II-2. Các lựa chọn phiên bản cài đặt.....	23
Hình II-3. Màn hình khái quát cho quản trị máy chủ	24
Hình II-4. Trình quản lý thiết bị Device Manage và hộp thoại thuộc tính thiết bị.....	25
Hình II-5. Giao tiếp chuyển đổi kiểu và dạng ổ đĩa.	26
Hình II-6. Giao diện quản trị người dùng và nhóm cục bộ	28
Hình II-7. Giao diện quản trị chính sách nhóm.....	29
Hình II-8. Giao diện gán chính sách cho việc đăng nhập/xuất.....	30
Hình II-9. Giao diện quản trị dịch vụ và thuộc tính của dịch vụ.....	30
Hình III-1. Cấu trúc cây tên miền.....	32
Hình III-2. Cách phân rã địa chỉ DNS.....	33
Hình III-3. Giao diện chọn chức năng DNS.....	34
Hình III-4. Cửa sổ nhập bản ghi SOA.....	35
Hình III-5. Cài đặt dịch vụ DHCP.....	37
Hình III-6. Định nghĩa dải địa chỉ cho cấp phát động DHCP	37
Hình III-7. Đơn vị tổ chức của thư mục động	40
Hình III-8. Tạo tài khoản máy tính trong miền	41
Hình III-9. Giao diện quản trị người dùng thư mục động	42
Hình III-10. Cài đặt dịch vụ thư mục động	42
Hình III-11. Cài đặt máy chủ IIS	43
Hình III-12. Các tham số cài đặt trang chủ Web.....	44
Hình III-13. Quyền với thư mục chia sẻ (bên trái) và NTFS (bên phải).	45
Hình III-14. Giao diện quản trị giới hạn lưu trữ.....	46
Hình III-15. Chia sẻ máy in.....	47

Hình III-16. Người dùng và quyền truy nhập máy in.....	48
Hình III-17. Lựa chọn cài đặt VPN(trái) và cấu hình VPN qua kết nối IPv4.	49
Hình IV-1. Cài đặt chương trình cập nhật Windows.....	50
Hình IV-2. Cấu hình thời gian thực hiện sao lưu.	52
Hình IV-3. Chọn dữ liệu sao lưu theo ngày để khôi phục.....	53
Hình IV-4. Lựa chọn sửa lỗi.....	54
Hình IV-5. Chương trình quản lý nhiệm vụ.	55
Hình IV-6. Chương trình xem các sự kiện được lưu lại.....	56
Hình IV-7. Chính sách kiểm toán nâng cao.	57
Hình IV-8. Danh sách các máy chủ được quản trị từ giao diện.	58
Hình IV-9. Thêm máy chủ để quản trị.	58
Hình V-1. Mốc thời gian của các phiên bản UNIX và LINUX.....	62
Hình V-2. Kiến trúc cơ bản LINUX/UNIX.....	63
Hình V-3. Màn hình làm việc Unity.....	65
Hình V-4. Màn hình làm việc GNOME.	66
Hình V-5. Màn hình làm việc KDE.....	66
Hình V-6. Cây thư mục LINUX/UNIX.....	67
Hình VI-1. Giao diện tạo đĩa cài cho ổ USB flash.	71
Hình VI-2. Thiết lập thời gian hệ thống.	72
Hình VI-3. Các lựa chọn phân vùng ổ cứng.....	72
Hình VI-4. Lựa chọn ổ đĩa vật lý để cài đặt.	73
Hình VI-5. Tóm tắt các thông tin về phân vùng ổ đĩa.	73
Hình VI-6. Các gói phần mềm dành cho các dịch vụ máy chủ.....	74
Hình VI-7. Cài đặt trình quản lý khởi động GRUB.	74
Hình VI-8. Màn hình khởi động Ubuntu của người dùng <i>ubuntu</i>	75
Hình VI-9. Các tham số cài đặt cho mạng LAN.	75
Hình VI-10. Tiện ích quản lý thiết bị trong Ubuntu.....	77
Hình VI-11. Sử dụng câu lệnh <i>fdisk</i>	78
Hình VI-12. Nội dung file fstab.	79
Hình VI-13. Nội dung cơ bản của passwd.....	80
Hình VI-14. Giao diện thêm người dùng của Ubuntu.....	81

Hình VI-15. Chương trình giám sát <i>top</i>	85
Hình VI-16. Câu lệnh <i>ps -aux</i>	86
Hình VII-1. Cấu trúc thông tin cấu hình mạng của dịch vụ DHCP	90
Hình VII-2. Nội dung file nhật ký cấp phát DHCP	91
Hình VII-3. Máy chủ Apache hoạt động trên địa chỉ cục bộ.	92
Hình VII-4. Quá trình gửi và nhận thư điện tử.....	94
Hình VII-5. Chọn kiểu dịch vụ cài đặt của Postfix.	96
Hình VII-6. Telnet tới máy chủ dịch vụ không thành công.	96
Hình VII-7. Câu lệnh USER qua telnet tới máy chủ dịch vụ.	97
Hình VII-8. Cấu hình phần mềm thư điện tử Outlook Express.....	97
Hình VII-9. Màn hình kết nối từ xa sử dụng SSH.....	101
Hình VIII-1. Trung tâm phần mềm Ubuntu.	103
Hình VIII-2. Lựa chọn tự động hóa cập nhật.	104
Hình VIII-3. Giao diện đồ họa cho việc sao lưu và khôi phục.....	105
Hình VIII-4. Giao diện màn hình làm việc chính BackupPC.....	106
Hình VIII-5. Các chức năng khắc phục lỗi cơ bản.	107
Hình VIII-6. Nhật ký hệ thống	108
Hình VIII-7. Kết quả của câu lệnh <i>netstat</i>	108
Hình VIII-8. Thống kê vào/ra đĩa.....	109
Hình VIII-9. Danh sách các luật đã thiết lập	110
Hình VIII-10. Thông tin truy nhập vào file chịu giám sát.....	110
Hình VIII-11. Thông tin về việc xác thực người dùng.....	111
Hình VIII-12. Các bộ phận NAGIOS	112
Hình VIII-13. Các bước thực hiện quản trị Puppet.	113

Danh mục các bảng

Bảng I-1. Tương quan các hệ thống file Windows.....	16
Bảng II-1. Cấu hình tối thiểu.....	21
Bảng II-2. Khả năng quản lý phần cứng và ảo hóa.	21
Bảng II-3. Các tính năng của Server 2008 và 2012.....	22

PTIT.EDU.VN

Các từ viết tắt

ACL – Access Control List: Danh sách kiểm soát truy nhập.

AD – Active Directory: Thư mục động

DHCP – Dynamic Host Configuration Protocol: Giao thức cấu hình máy tính động

DNS – Domai Name Service: Dịch vụ tên miền

FAT – File Allocation Table: Bảng cấp phát file

GUI – Graphic User Interface: Giao diện người dùng đồ họa

IDE – Integrated Drive Electronics: Ổ đĩa điện tử tích hợp

NTFS - New Technology File System: hệ thống file công nghệ mới.

RAID – Redundant Array of Independent Disks : Chuỗi dự phòng các ổ đĩa độc lập

SATA – Serial AT Attachment: Kết nối AT(Advanced Technology) nối tiếp

SCSI – Small Computer System Interface: Giao tiếp hệ thống máy tính nhỏ

UEFI – Unified Extensible Firmware Interface: Giao tiếp firmware mở rộng hợp nhất

Phần I – Quản trị hệ điều hành Microsoft Windows

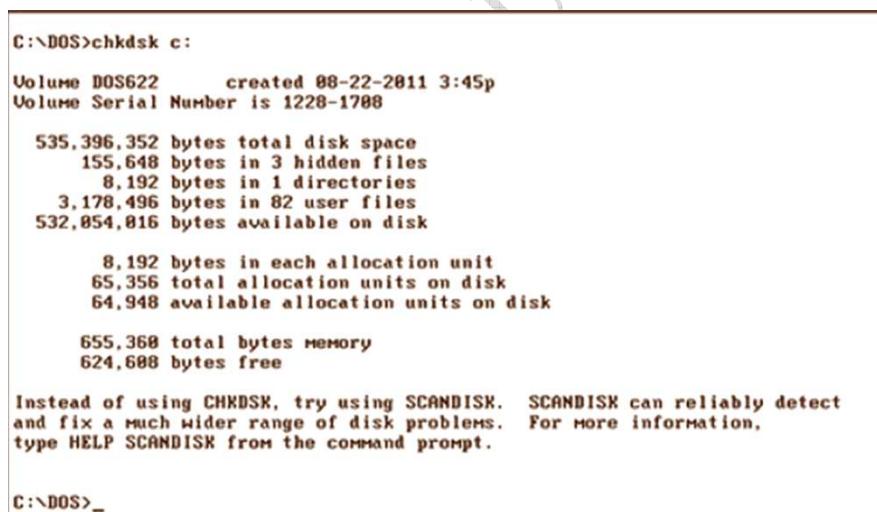
Phần 1 bắt đầu bằng việc giới thiệu về các mốc phát triển quan trọng của hệ điều hành Microsoft Windows từ chỗ là phiên bản dùng cho máy tính cá nhân cho đến phiên bản sử dụng cho máy chủ. Kiến trúc cơ bản của hệ điều hành Windows cũng được trình bày trong phần này. Chương tiếp theo trình bày về vấn đề về việc cài đặt hệ điều hành Windows và tập trung chủ yếu vào môi trường máy trạm và máy chủ. Chương này cũng giới thiệu cách thức cơ bản để quản trị hệ điều hành Windows như hệ thống lưu trữ, các thiết bị, quyền truy nhập máy tính cục bộ. Hai chương còn lại trong phần này tập trung vào việc triển khai và quản lý các dịch vụ cần thiết mà hệ điều hành máy chủ Windows hỗ trợ như thư mục động, các dịch vụ mạng Internet, cũng như việc đảm bảo an toàn cho việc vận hành thông qua các công cụ giám sát, bảo trì và khắc phục lỗi.

Chương I. GIỚI THIỆU CÁC HỆ ĐIỀU HÀNH MICROSOFT WINDOWS

Chương này giới thiệu quá trình phát triển của hệ điều hành Microsoft Windows và tập trung vào các tính năng đặc trưng, nổi bật của hệ điều hành này. Ngoài ra, chương này trình bày kiến trúc khái quát của hệ điều hành và các khái niệm căn bản của môi trường Windows.

I.1 Lịch sử phát triển

Hệ điều hành Windows ban đầu không sử dụng giao diện đồ họa như hiện nay mà có nguồn gốc từ hệ thống dựa trên ký tự và giao diện đồ họa đơn giản. Phiên bản đầu tiên của hệ điều hành Microsoft là MS-DOS (Disk Operating System – Hệ thống điều khiển đĩa) ra đời vào năm 1981. Tại thời điểm đó, chức năng chủ yếu của hệ điều hành là nạp các chương trình và quản lý các ổ đĩa. MS-DOS không tích hợp giao diện người dùng đồ họa (GUI^{*}) và hoạt động qua các câu lệnh như trong Hình I-1. Hệ điều hành này đã rất phổ biến từ năm 1981 đến 1999.



```
C:\>chkdsk c:
Volume DOS622 created 08-22-2011 3:45p
Volume Serial Number is 1228-1708

535,396,352 bytes total disk space
 155,648 bytes in 3 hidden files
    8,192 bytes in 1 directories
 3,178,496 bytes in 82 user files
532,854,816 bytes available on disk

    8,192 bytes in each allocation unit
  65,356 total allocation units on disk
  64,948 available allocation units on disk

  655,368 total bytes memory
  624,688 bytes free

Instead of using CHKDSK, try using SCANDISK. SCANDISK can reliably detect
and fix a much wider range of disk problems. For more information,
type HELP SCANDISK from the command prompt.

C:\>_
```

Hình I-1. Giao diện dòng lệnh của MS-DOS.

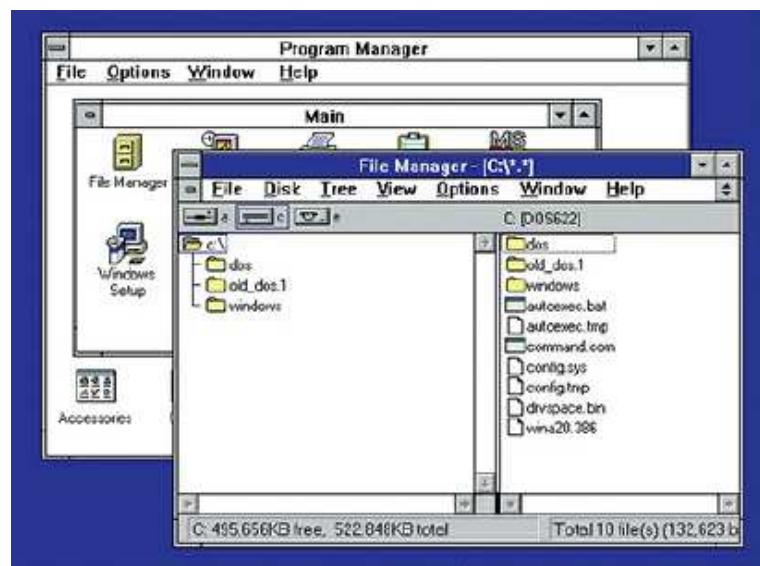
Cấu hình máy tính tiêu biểu cho hệ điều hành này là bộ xử lý tốc độ cỡ khoảng 10-40Mhz, bộ nhớ chính 1MB, màn hình độ phân giải 640x480 điểm ảnh, ổ đĩa mềm dung lượng 1,44MB, và ổ cứng dung lượng cỡ 100MB.

Tuy có nhiều công ty cung cấp giao diện đồ họa như Apple, Xerox, hay IBM song Windows đã thành công hơn tất cả sản phẩm của công ty khác thể hiện qua số lượng các bản được bán ra ngoài thị trường. Việc phổ biến này không có nghĩa là Windows ưu việt hơn các sản phẩm khác mà đơn giản là mọi người sẽ hay bắt gặp sản phẩm này hơn.

* GUI - Graphic User Interface: Giao diện người dùng đồ họa

Phiên bản khiến cho Windows trở nên phổ biến là Windows 3.1 xuất hiện vào giữa những năm 1990 và thiết lập nền móng cho các phiên bản Windows khác đến tận ngày nay. Hệ thống Windows 3.1 bao gồm các menu lựa chọn, các cửa sổ có thể thay đổi kích thước và hệ thống chạy chương trình gọi là quản lý chương trình – Program Manager. Chương trình đặc biệt này cho phép nhóm các chương trình lại và dùng biểu tượng đại diện cho chương trình. Rất nhiều các khái niệm của Windows 3.1 đã được sử dụng cho đến các hệ điều hành ngày nay. Windows 3.1 và hệ thống tương tự vẫn dựa trên DOS để hoạt động.

Cùng thời điểm với Windows 3.1, Microsoft tung ra hệ điều hành khác gọi là Windows NT với nghĩa là hệ thống Windows công nghệ mới. Windows NT được thiết kế lại và là hệ điều hành mạng, chạy trên nền 32 bit song sử dụng GUI như Windows 3.1. Hệ điều hành mới mạnh hơn và sử dụng các nhân và phần nạp khởi động riêng chứ không dựa trên DOS. Windows NT hướng tới môi trường làm việc cộng tác và tính toán hiệu năng cao. Các hệ thống Windows sau này vẫn dựa trên kiến trúc của Windows NT.



Hình I-2. Giao diện menu và đồ họa Windows 3.1

Vào năm đầu của thế kỷ 21, Microsoft đưa ra Windows 2000 hướng tới môi trường máy chủ và máy trạm nhằm thay thế cho sản phẩm Windows NT trước đó. Một trong những tính năng quan trọng đó là thư mục động (*Active Directory*) dựa trên các chuẩn công nghiệp về tên miền, giao thức truy nhập thư mục và xác thực để kết nối và chia sẻ dữ liệu giữa các máy tính với nhau. Dịch vụ đầu cuối (*Terminal Service*) cho phép kết nối từ xa được tích hợp và mở rộng cho tất cả các phiên bản dùng cho máy chủ.

Vào năm 2001, Microsoft kết hợp các dòng sản phẩm Windows NT/2000 (dành cho đối tượng công ty và doanh nghiệp) và Windows 95/98/Me (người quản trị thông thường) tạo nên Windows XP. Kể từ phiên bản này các sản phẩm của Microsoft cần phải qua thủ tục kích hoạt để được sử dụng hợp lệ. Đây có lẽ là một trong những phiên bản Windows tốt nhất và là hệ thống chạy lâu nhất (gần 13 năm tính từ lúc ra đời) cho dù ban đầu hệ thống có nhiều vấn đề về tính an toàn và hiệu năng. Windows Vista và Windows 7 được Microsoft đưa ra nhằm thay

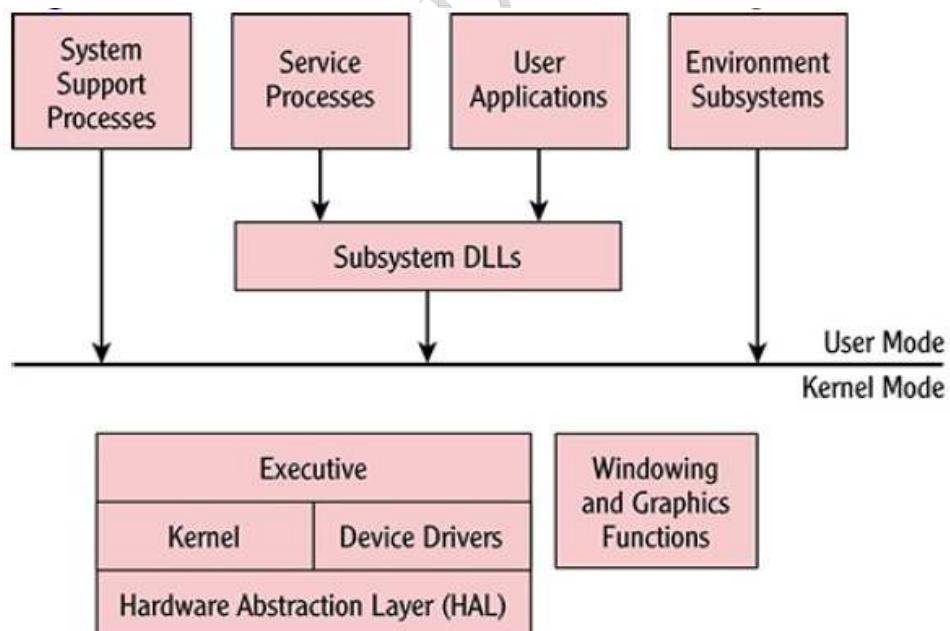
thể cho bản Windows XP song không được người dùng chấp nhận rộng rãi như bản Windows XP.

Windows 8 và đặc biệt là Windows 10 thể hiện sự thay đổi mạnh mẽ về việc sử dụng các thiết bị tính toán cá nhân mà máy tính PC là một đại diện. Mục tiêu của hệ điều hành mới là hợp nhất các nền tảng Windows cho các thiết bị di động như điện thoại, máy tính bảng. Như vậy, các ứng dụng có thể được tải về và chạy trên tất cả các thiết bị Windows.

Với sản phẩm dành cho môi trường chuyên nghiệp, Windows Server 2003 đưa ra các khái niệm về chức năng máy chủ như Web, file, ứng dụng hay cơ sở dữ liệu và công cụ hỗ trợ cài đặt các chức năng một cách thuận tiện. Phiên bản nâng cấp Server 2003 R2 hỗ trợ tính toán 64 bit và các công cụ quản lý tập trung, các chức năng ảo hóa. Các phiên sau gồm có Server 2008, 2012 tăng cường khả năng kết nối mạng, các hệ thống file phân tán, các tính năng bảo mật, ảo hóa và hướng tới tính toán đám mây (*cloud computing*).

I.2 Kiến trúc của hệ điều hành

Kiến trúc của hệ điều hành Windows hiện thời dựa trên kiến trúc Windows NT. Về cơ bản, kiến trúc này (như trong hình dưới đây) được chia thành hai lớp tương ứng với hai chế độ hoạt động: chế độ nhân và chế độ người dùng. Chế độ nhân dành cho nhân của hệ điều hành và các chương trình mức thấp khác hoạt động. Chế độ người dùng dành cho các ứng dụng như Word, Excel và các hệ thống con hoạt động.



Hình I-3. Kiến trúc cơ bản của hệ điều hành Windows

Về kỹ thuật, các thao tác ở chế độ nhân được thực thi ở cấp độ thấp nhất hay chế độ đặc quyền. Các thao tác ở chế độ người dùng được thực thi ở cấp độ cao nhất hay chế độ không đặc quyền. Nói cách khác, các chế độ này hạn chế các tài nguyên máy tính mà chương trình được phép sử dụng.

Các khái niệm cơ bản của chế độ người quản trị như sau:

- *Chương trình hỗ trợ hệ thống (System Support Processes)*: chứa các chương trình thực hiện các chức năng hệ thống như đăng nhập, quản lý phiên làm việc.
- *Các chương trình dịch vụ (Service Processes)*: cung cấp dịch vụ của hệ điều hành như quản lý máy in, tác vụ. Chúng cũng có thể là các dịch vụ như cơ sở dữ liệu hay cung cấp chức năng cho chương trình khác.
- *Ứng dụng người dùng (User Applications)*: Các chương trình thực hiện theo yêu cầu của người quản trị.
- *Hệ thống con (Environment Subsystems)* và hệ thống liên kết động (Subsystem DLL) kết hợp với nhau cho phép các kiểu ứng dụng khác nhau hoạt động được như môi trường Win32, Win64 hay DOS 32. Trong đó, hệ thống liên kết động chuyển các hàm ứng dụng thành các hàm dịch vụ hệ thống trực tiếp.

Các chức năng cơ bản của chế độ nhân gồm có:

- *Thực thi (Executive)* thực hiện việc quản lý các tiến trình và luồng, quản lý bộ nhớ, vào/ra ...
- *Nhân (Kernel)* chịu trách nhiệm điều độ luồng, đồng bộ giữa các tiến trình, xử lý ngắn
- *Các trình điều khiển thiết bị (Device Drivers)* làm nhiệm vụ giao tiếp giữa quản lý vào/ra của phần thực thi và phần cứng cụ thể. Các trình điều khiển này cũng có thể liên lạc với hệ thống file, mạng hay giao thức khác.
- *Lớp phần cứng trừu tượng (Hardware Abstraction Layer - HAL)* giấu đi các chi tiết phần cứng giúp cho hệ điều hành có thể hoạt động trên nhiều phần cứng khác nhau với giao tiếp không đổi.
- *Các chức năng cửa sổ và đồ họa (Windowing and Graphics Functions)* cung cấp giao diện đồ họa cho người dùng như vẽ các cửa sổ các đối tượng đồ họa.

Kiến trúc của Windows rất giống với các hệ điều hành khác như Linux hay Mac OS X. Điểm khác biệt căn bản là việc xử lý đồ họa. Windows nhúng chức năng này vào phần nhân để nhằm tăng hiệu năng đồ họa. Linux thì loại bỏ chức năng này ra khỏi phần nhân để tăng độ tin cậy.

I.3 Giao diện của Windows

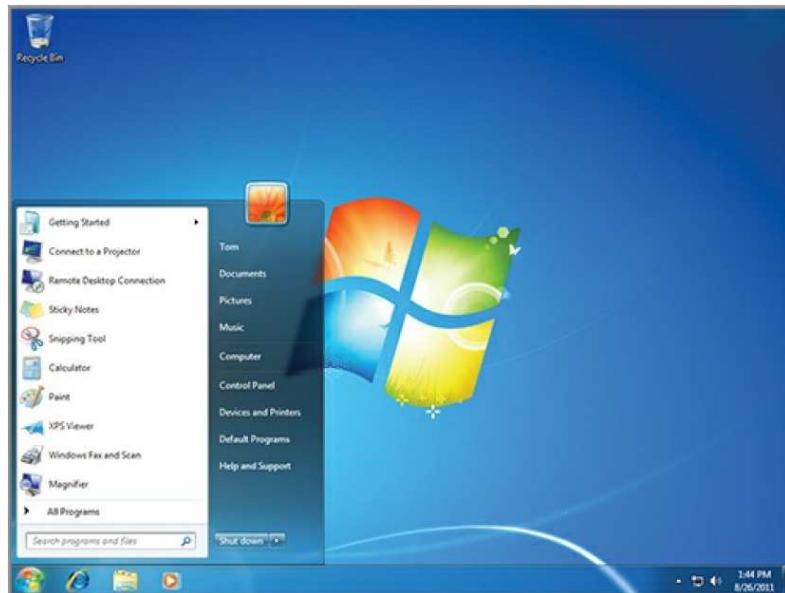
Hệ điều hành Windows có ba cách giao tiếp chính giúp làm việc với các ứng dụng và thực hiện các công việc quản trị. Hầu hết người dùng thông thường sử dụng GUI song người quản trị lại được lợi hơn từ giao diện dòng lệnh và Windows PowerShell.

- *Giao diện đồ họa GUI*

Giao diện người dùng đồ họa trong Windows bao gồm các cửa sổ, nút bấm, hộp văn bản và các phần tử định hướng khác. Phần tử quan trọng trong GUI đó chính là menu khởi động (*Start*) và thanh tác vụ (*Taskbar*) như trong hình dưới đây. Menu khởi động cho phép người quản trị truy nhập vào tất cả các chức năng của hệ điều hành cũng như các chương trình người

quản trị. Thanh tác vụ cho phép truy nhập nhanh đến các ứng dụng và cho biết tình trạng của các chương trình người quản trị.

Phần quan trọng khác, đó là màn hình làm việc (*desktop*). Đây là nơi chứa các biểu tượng các chương trình người dùng hay hệ thống hoặc các chương trình tiện ích như tra cứu thông tin thời tiết, chứng khoán... Khi các chương trình người dùng chạy, chúng sử dụng không gian này để hiện thị thông tin cho người dùng.



Hình I-4. Giao diện GUI Windows

- *Giao diện dòng lệnh*

Giao diện này là giao diện xưa nhất của Microsoft đó chính là dòng lệnh DOS. Trong môi trường Windows, nó không còn thực sự là DOS dù có nhiều câu lệnh DOS vẫn còn dùng được và được kích hoạt thông qua chương trình *cmd.exe*. Thông qua giao diện này người dùng có thể thực thi các thao tác cấu hình cho hệ điều hành hay chạy các chương trình DOS cũ.

- *Giao diện PowerShell*

Đây là giao diện dòng lệnh mới của Windows và là môi trường nên dùng cho các tác vụ quản trị. Thực tế, Microsoft hỗ trợ tập các lệnh trong môi trường PowerShell được gọi là *cmdlet* để thực hiện các tác vụ quản trị mong muốn.

Một trong những tính năng quan trọng của PowerShell là khả năng lập trình đơn giản (*scripting*). Với các hàm lô-gic và các biến, người quản trị có thể tự động hóa các tác vụ thuận tiện hơn rất nhiều so với giao diện DOS cũ. Hơn thế, PowerShell còn cho phép thực thi các lệnh từ xa nhờ hỗ trợ từ hệ điều hành.

I.4 Hệ thống file của Windows

Hệ điều hành Windows sử dụng chủ yếu 2 hệ thống file: FAT* thừa hưởng từ DOS, và NTFS† được sử dụng rộng rãi.

Hệ thống file FAT là một kiểu hệ thống file đơn giản nhất. Nó bao gồm một cung mô tả hệ thống file (*cung khởi động-boot sector*), bảng cấp phát các khối cấp phát và không gian lưu trữ file và thư mục. Các file được lưu vào thư mục và mỗi thư mục là một mảng gồm các bản ghi 32 byte dùng để mô tả các file hay thuộc tính mở rộng như tên file dài. Bản ghi file trả tới khói lưu trữ đầu tiên của file. Các khói lưu trữ tiếp theo được tìm bằng cách truy theo liên kết trong bảng cấp phát.

Bảng cấp phát chứa mảng các mô tả khói cấp phát. Mỗi phần tử trong mảng này tương ứng với một phần tử cấp phát. Số thứ tự của phần tử mảng giúp tương ứng với vị trí của khói cấp phát trong không gian lưu trữ. Giá trị không của phần tử trong mảng cho biết khói cấp phát tương ứng chưa được sử dụng. Giá trị khác không cho biết vị trí của phân tử mảng cũng chính là khói lưu trữ kế tiếp.

Trong hệ thống file FAT gồm có FAT12, FAT16 và FAT32 tương ứng với của số lượng tối đa các khói cấp phát là 2^{12} , 2^{16} và 2^{32} . Đến nay hệ thống FAT chủ yếu dùng cho các thiết bị lưu trữ ngoài như thẻ nhớ hay USB.

Hệ thống file NTFS được đưa ra cùng với Windows NT. Đến nay là hệ thống file chủ yếu của hệ điều hành Windows. Hệ thống file này mềm dẻo và hỗ trợ nhiều kiểu thuộc tính file bao gồm kiểm soát truy nhập, mã hóa, nén... Mỗi file trong hệ thống NTFS được lưu bằng một mô tả file trong bảng file chính (master file table) và nội dung của file. Bảng file chính chứa toàn bộ thông tin về file như kích cỡ, cấp phát, tên... Các khói cấp phát đầu tiên và cuối cùng của hệ thống file chứa các cài đặt của hệ thống file. Hệ thống file này sử dụng các giá trị 48 hay 64 bit để tham chiếu file nên hỗ trợ các thiết bị lưu trữ cỡ lớn.

Bảng dưới đây cho thấy khả năng của từng hệ thống file.

Bảng I-1. Tương quan các hệ thống file Windows

	FAT16	FAT32	NTFS
Tương thích	DOS, Windows	Windows 95 và mới hơn	Windows NT 4.0 và mới hơn
Kích cỡ	4GB	32GB	2TB hay lớn hơn
Số file	~65000	~4.000.000	~4.000.000.000
Kích cỡ file tối đa	4GB	4GB	16TB

* FAT- File Allocation Table: Bảng cấp phát file

† New Technology File System: hệ thống file công nghệ mới.

I.5 Giới thiệu Windows Registry

Danh mục đăng ký (*Registry*) là một cơ sở dữ liệu của Windows và là nơi lưu các thông tin quan trọng về phần cứng, các chương trình, các cài đặt, và các hồ sơ về tài khoản người dùng trong máy tính. Windows liên tục tham chiếu đến các thông tin trong danh mục này.

Người dùng thường không nên tự ý sửa đổi các thông tin lưu trong danh mục đăng ký vì các chương trình và ứng dụng sẽ thực hiện toàn bộ các sửa đổi cần thiết một cách tự động. Mặt khác, các hư hỏng có thể làm cho Windows thậm chí là máy tính không thể hoạt động bình thường.

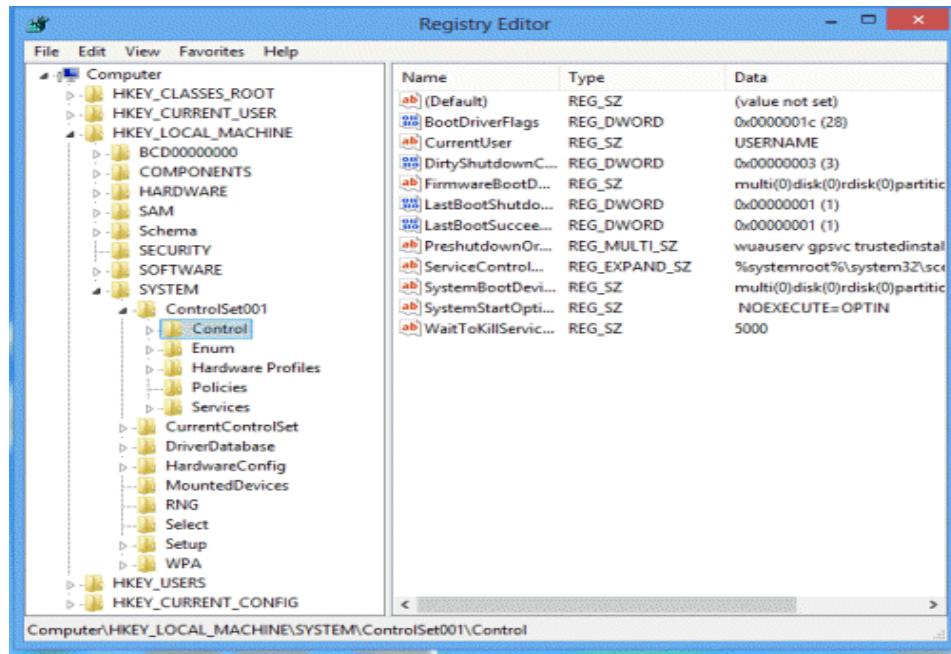
Về cơ bản danh mục đăng ký là cơ sở dữ liệu phân cấp để lưu các cài đặt ở mức thấp cho Windows và các ứng dụng. Mỗi mục đăng ký bao gồm hai thành phần cơ bản khóa (*key*) và các giá trị. Các khóa đăng ký chứa các đối tượng. Các giá trị đăng ký là các đối tượng cụ thể. Các khóa có thể chứa các giá trị cụ thể hay các khóa khác nữa. Việc tham chiếu đến các khóa giống như đường dẫn trong Windows.

Trong danh mục đăng ký được định nghĩa trước, các khóa gốc tiêu biểu gồm có:

- *HKEY_CLASSES_ROOT*: Lưu thông tin ứng dụng như tên file và đăng ký của các đối tượng COM
- *HKEY_CURRENT_USER*: lưu thông tin về người quản trị đăng nhập hiện thời.
- *HKEY_LOCAL_MACHINE*: Lưu thông tin hệ thống
- *HKEY_USERS*: Lưu thông tin về toàn bộ tài khoản trên máy.
- *HKEY_CURRENT_CONFIG*: Lưu thông tin về máy hiện thời.

Các khóa trong danh mục đăng ký đều có thể bị hạn chế truy nhập thông qua danh sách kiểm soát truy nhập tương tự như việc kiểm soát truy nhập trong hệ thống file NTFS.

Các giá trị của mục đăng ký là cặp tên/dữ liệu lưu bên trong các khóa như trong Hình I-5. Các giá trị khóa có thể nhận một số kiểu dữ liệu tiêu biểu nhị phân, từ, hay chuỗi ký tự được mô tả tương ứng bằng các từ khóa REG_BINARY, REG_DWORD và REG_SZ.



Hình I-5. Danh mục đăng ký trong Windows

Để xem và thay đổi các giá trị trong danh mục đăng ký Windows cung cấp phần mềm RegEdit.exe có thể chạy từ dòng lệnh. Chương trình này cũng cung cấp các chức năng sao lưu và khôi phục các khóa trong cây Registry. Việc truy nhập các khóa cụ thể bị chỉ định bởi quyền của người dùng trong Windows.

Chương II. CÀI ĐẶT VÀ QUẢN TRỊ CÁC THÀNH PHẦN CƠ BẢN CỦA WINDOWS

Chương này giới thiệu các dịch vụ quan trọng được hệ điều hành máy chủ Windows cung cấp và các yêu cầu cơ bản về phần cứng với lớp các phiên bản máy chủ. Phần này giới hạn việc trình bày các yêu cầu với phiên bản Windows 2012. Tiếp theo, các khái niệm và cách thức quản lý máy tính chạy hệ điều hành Windows cũng được nêu ra. Việc này giúp sinh viên làm quen với các khái niệm cũng như công cụ quản lý của Windows trên máy tính cục bộ gồm có các trình điều khiển thiết bị, hệ thống file, các chương trình của Windows.

II.1 Cài đặt Windows

Máy chủ là thuật ngữ mô tả một máy tính mà kết hợp cả thiết bị phần cứng và phần mềm để xử lý các công việc khác nhau qua môi trường mạng. Về cơ bản máy chủ được thiết kế để cung cấp các dịch vụ và chạy các ứng dụng trong điều kiện tài năng, thời gian dài và có khả năng chịu lỗi. Thông thường tên máy chủ sẽ gắn với hệ điều hành chạy trên phần cứng máy chủ như máy chủ Windows cho hệ điều hành Microsoft Windows hay máy chủ Linux sử dụng hệ điều hành Linux.

Phần dưới đây giới thiệu quá trình lựa chọn và cài đặt cho máy chủ Microsoft Windows với trọng tâm là bản Server 2012 và có liên hệ với bản Server 2008.

II.1.1 Các dịch vụ

Vai trò hay chức năng máy chủ là công việc chủ yếu mà máy chủ sẽ thực hiện. Thực tế, máy chủ có thể đồng thời cung cấp nhiều chức năng hay dịch vụ cho người dùng cũng như là các máy tính khác trong mạng. Các chức năng phổ biến của máy chủ bao gồm: dịch vụ file, dịch vụ in ấn, dịch vụ Web, truy nhập từ xa, máy chủ thư điện tử, máy chủ cơ sở dữ liệu

Trong thời gian vừa qua, khái niệm ảo hóa ngày càng trở nên phổ biến và quen thuộc. Công nghệ này cho phép nhiều hệ điều hành có thể chạy đồng thời trên cùng một máy tính vật lý. Như vậy, việc phân tách các dịch vụ sao cho việc thay đổi trên các máy ảo không ảnh hưởng tới nhau được đơn giản hóa và thuận tiện. Mặt khác, công nghệ này cho phép giảm thiểu chi phí thông qua việc chia sẻ phần cứng và tận dụng tối đa năng lực của các thiết bị.

Các dịch vụ quan trọng của máy chủ Windows bao gồm:

- *Xác thực thư mục động (Active Directory Certificate Services)*: Dịch vụ tạo và quản lý chứng thực khóa công khai cho hệ thống an ninh dùng công nghệ khóa công khai.
- *Miền thư mục động (Active Directory Domain Services)*: Lưu thông tin về người quản trị, máy tính và các thiết bị khác trong mạng. Ngoài ra, dịch vụ này giúp

người quản trị quản lý các thông tin trên an toàn và làm thuận tiện cho việc chia sẻ và phối hợp giữa các người quản trị.

- *Liên kết thư mục động (Active Directory Federation Services)*: Hỗ trợ công nghệ đăng nhập một lần trên Web bằng cách liên kết hay chia sẻ một cách an toàn định danh người dùng, quyền truy nhập giữa các tổ chức với nhau.
- *Thư mục động rút gọn (Active Directory Lightweight Directory Services)*: Dùng để lưu dữ liệu mà không cần dịch vụ miền thư mục động
- *Quản lý quyền thư mục động (Active Directory Rights Management Services)*: Công nghệ bảo vệ thông tin cho phép các ứng dụng bảo mật thông tin khỏi việc sử dụng trái phép.
- *Máy chủ ứng dụng (Application Server)*: Cung cấp giải pháp hoàn chỉnh cho việc cài đặt và quản lý các ứng dụng doanh nghiệp phân tán: .Net, Web, Message Queuing, COM+
- *Quản lý DHCP (Dynamic Host Configuration Protocol)*: Cho phép máy chủ tự động cấp phát địa chỉ Internet cho các máy tính và thiết bị dùng DHCP và tự động hóa cấu hình (địa chỉ DNS, gateway) các máy tính và thiết bị.
- *Tên miền DNS (Domain Name System)*: Phương pháp tiêu chuẩn liên kết các tên và địa chỉ Internet.
- *Dịch vụ file*: Cung cấp công nghệ cho việc quản lý lưu trữ, sao lưu, tên miền, tìm kiếm nhanh và truy nhập của người quản trị.
- *Dịch vụ ảo hóa Hyper-V*: Cho phép tạo và quản lý máy ảo và tài nguyên. Trong đó, mỗi máy ảo cung cấp môi trường thực thi riêng biệt giúp chạy nhiều hệ điều hành đồng thời.
- *Truy nhập và chính sách mạng (Network Policy and Access Services)*: Cho phép người dùng kết nối cục bộ hay từ xa, kết nối các mạng, cho phép quản lý truy nhập tập trung cũng như chính sách cho máy khách.
- *In ấn tài liệu (Print and Document Services)*: Giúp quản trị máy in một cách tập trung và cho phép chia sẻ máy in với các người dùng trong mạng.
- *Dịch vụ đầu cuối (Terminal Services)*: Cho phép người dùng truy nhập các ứng dụng Windows cài trên máy chủ đầu cuối. Người dùng có thể kết nối tới máy chủ đầu cuối để chạy và sử dụng tài nguyên mạng
- *Web (Internet Information Services-IIS)*: Cho phép chia sẻ thông tin trên mạng Internet và Intranet.

II.1.2 Chuẩn bị cài đặt

Việc lựa chọn phiên bản cũng như xác định yêu cầu về dịch vụ mà máy chủ cung cấp và phần cứng của máy chủ có vai trò hết sức quan trọng. Với phiên bản Server 2008 việc cài đặt phức tạp do có nhiều lựa chọn như bản 32 hay 64 bit, liệu có cần giao diện đồ họa hay chỉ cần giao diện dòng lệnh (với bản Server Core). Việc thay đổi lựa chọn sẽ dẫn đến việc phải cài lại máy chủ từ đầu, thậm chí phải thay đổi phần cứng.

Kể từ bản Server 2008 R2, nền tảng 32 bit không còn được hỗ trợ nữa. Điều này một phần do phần lớn các phần mềm quan trọng sử dụng nền tảng 64 bit cũng như phần cứng hiện đại hỗ trợ nền tảng này. Bản Server 2012 không còn hỗ trợ bộ xử lý Itanium và bỏ phiên bản Web Server so với bản Server 2008 R2. Như vậy, Server 2012 cung cấp các phiên bản sau:

1. Trung tâm dữ liệu (*Datacenter*): được thiết kế dùng cho các máy chủ mạnh và lớn với 64 bộ xử lý và có các tính năng chịu lỗi như thay nóng bộ xử lý. Phiên bản này chỉ bán thông qua nhà sản xuất thiết bị hoặc cấp phép theo khối (volume-licensing).
2. Tiêu chuẩn (*Standard*): chứa đựng đầy đủ các chức năng và chỉ khác phiên bản *Datacenter* ở số lượng máy ảo.
3. Cơ bản (*Essential*): so với bản *tiêu chuẩn* thì có chức năng lỗi máy chủ ServerCore, máy ảo Hyper-V và liên kết thư mục động và tối đa là 25 người dùng.
4. Thiết yếu (*Foundation*): là phiên bản rút gọn hướng đến doanh nghiệp nhỏ chỉ cần các chức năng máy chủ thiết yếu như dịch vụ file hay in ấn hay ứng dụng.

Yêu cầu phần cứng tối thiểu để chạy máy chủ Server 2008 và 2012 như trong bảng dưới đây:

Bảng II-1. Cấu hình tối thiểu.

	Server 2008	Server 2012
Bộ xử lý	1GHz(x86)-1.4GHz(x64)	1.4GHz x64
RAM	512MB	512MB
Ổ cứng	10GB	32GB
Khác	DVD-ROM, màn hình, bàn phím, kết nối mạng	

Sự khác biệt giữa hai bản Server 2008 và 2012 còn thể hiện qua khả năng quản lý phần cứng cũng như các tính năng máy chủ như trong các bảng dưới đây.

Bảng II-2. Khả năng quản lý phần cứng và ảo hóa.

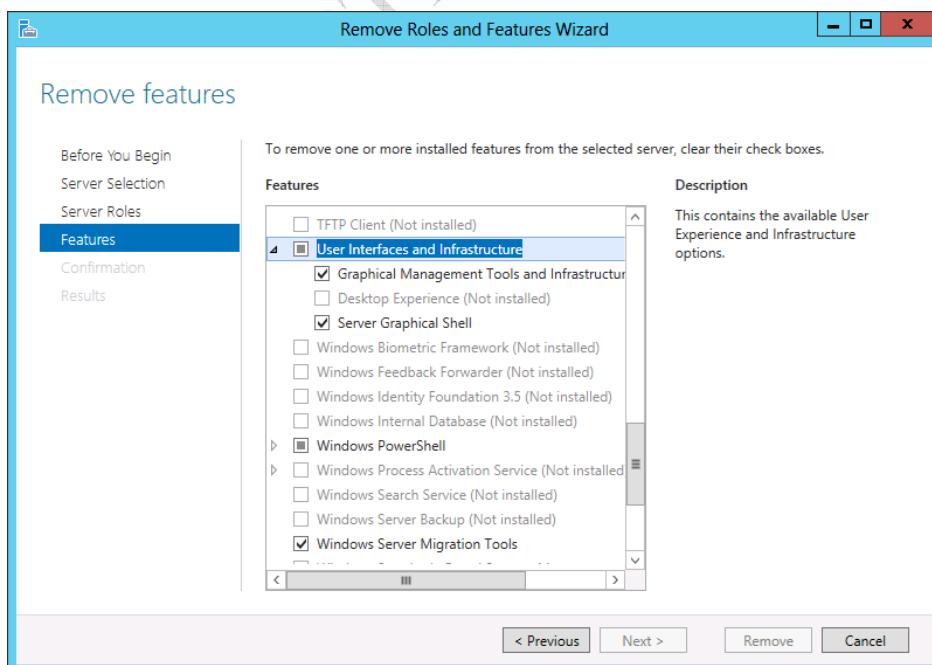
	Server 2008	Server 2012
Bộ xử lý	64	320
Bộ nhớ vật lý	1TB	4TB
Bộ xử lý ảo trên máy chủ	512	2048
Bộ xử lý trên máy ảo	4	64
Bộ nhớ trên máy ảo	64GB	1TB
Số lượng các nốt liên kết (cluster)	16	64

Bảng II-3. Các tính năng của Server 2008 và 2012.

	Server 2008	Server 2012
Dịch vụ thư mục động	Có	Có
Hỗ trợ ảo hóa thư mục động	Không	Có
Hỗ trợ ảo hóa VDI-Virtual Desktop Infrastructure	Có	Có
Sao lưu Hyper-V	Không	Có
Di chuyển lưu trữ trực tiếp (live storage migration)	Không	Có
Hạn chế IP động	Không	Có
ServerCore	Có	Có
Quản lý nhiều máy chủ	Không	Có
Windows PowerShell	Có	Có

II.1.3 Các lựa chọn cài đặt

Việc cài đặt *ServerCore*, giao diện người dùng sẽ ở mức tối thiểu và không còn giao diện đồ họa quen thuộc của Windows. Tuy nhiên, lựa chọn này mang lại một số ưu điểm như sử dụng phần cứng tối thiểu, giảm không gian lưu trữ, bớt việc cập nhật các mô-đun đồ họa, và giảm rủi ro lỗ hổng bảo mật. Một số tính năng quản trị và dịch vụ mạng không được hỗ trợ khi cài đặt ở chế độ này như: dịch vụ liên kết thư mục động, máy chủ fax, dịch vụ truy nhập và chính sách mạng, các dịch vụ làm việc từ xa (*remote desktop*) và dịch vụ cài đặt qua mạng (*Windows Deployment Services*).



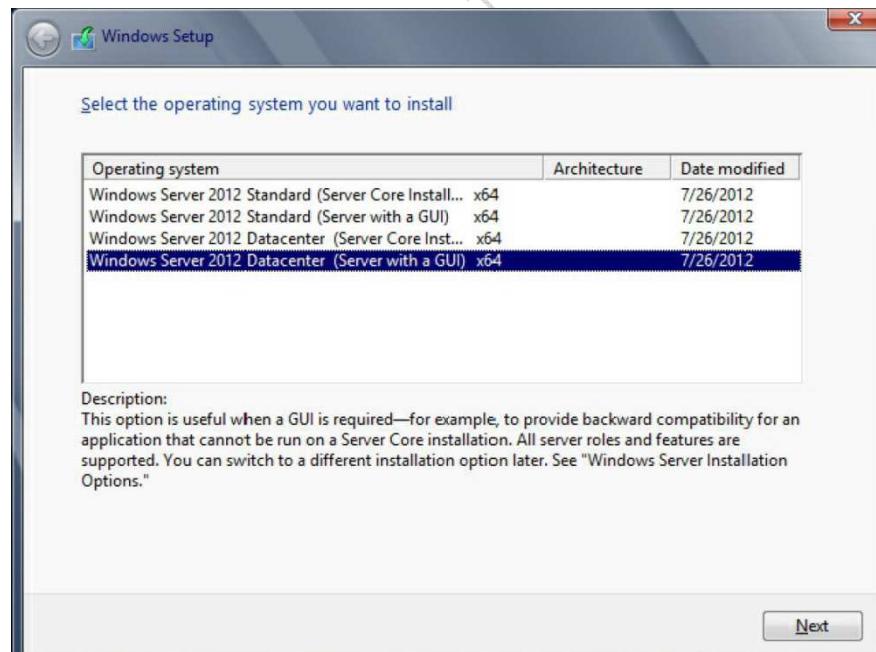
Hình II-1. Lựa chọn chức năng cài đặt.

Cài đặt giao tiếp máy chủ tối thiểu (*Minimal Server Interface*) là giải pháp dung hòa giữa các làm việc với môi trường Windows truyền thống và giao tiếp dòng lệnh. Các phần tử giao diện được cung cấp có trình duyệt IE, các thành phần căn bản của Windows như phần vỏ (*shell*), màn hình làm việc, duyệt file và ứng dụng màn hình làm việc. Một số chức năng trong Control Panel được chuyển thành các ứng dụng shell như quản lý chương trình (*Programs and features*), quản trị giao tiếp mạng (*Network and sharing center*), quản trị các thiết bị, hiển thị... Để lựa chọn cài đặt giao diện tối thiểu này cần loại bỏ chức năng vỏ đồ họa máy chủ “*Server Graphical Shell*” như trong Hình II-1.

II.1.4 Cài đặt sử dụng giao diện

Phần này sử dụng cách cài đặt mới bản Server 2012. Về cơ bản giao diện đồ họa cung cấp đầy đủ thông tin và thao tác sử dụng chuột nên việc cài đặt tương đối dễ dàng và thuận tiện cho người dùng để hoàn tất quá trình cài đặt.

Để cài đặt cần chuẩn bị đĩa khởi động DVD hay thẻ nhớ USB. Sau khi khởi động thành công, Server 2012 yêu cầu cung cấp các thông tin cơ bản như ngôn ngữ, định dạng thời gian và tiền tệ, kiểu bàn phím. Bước tiếp theo, chương trình cài đặt sẽ hiển thị lựa chọn cài đặt các phiên bản cho người quản trị như trong hình dưới đây. Người quản trị sẽ lựa chọn phiên bản phù hợp với nhu cầu của mình.

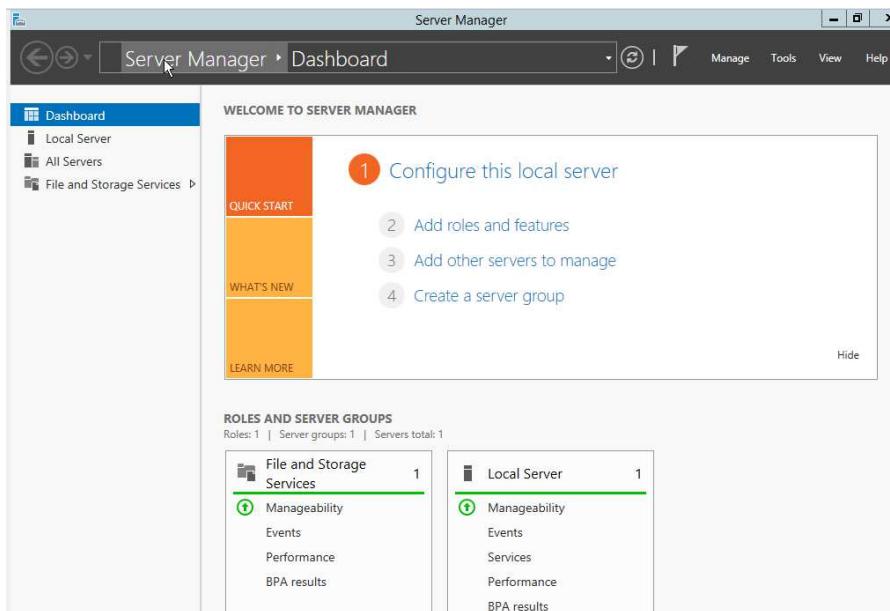


Hình II-2. Các lựa chọn phiên bản cài đặt.

Các bước tiếp theo, người quản trị lựa chọn kiểu nâng cấp từ hệ thống cũ hay cài mới và chấp nhận các điều khoản sử dụng của Microsoft. Khi cài mới người quản trị cần chỉ định ổ cứng và phân vùng dùng để cài đặt. Trong trường hợp đặc biệt như sử dụng ổ đĩa theo chuẩn RAID, người quản trị cần cung cấp trình điều khiển cho chương trình cài đặt thông qua chức năng nạp “*Load driver*”. Đến đây chương trình cài đặt sẽ thực hiện việc giải nén và chép các

chương trình và đoạn mã sang thiết bị lưu trữ của máy chủ. Tùy thuộc vào cấu hình cụ thể của máy tính, quá trình này có thể mất khoảng 20 phút hay lâu hơn.

Sau khi chương trình cài đặt thành công và máy tính khởi động lại, người quản trị cần cài đặt mật khẩu quản trị máy chủ. Thông thường, mật khẩu này phải đủ phức tạp: có độ dài hơn 8 ký tự, có chữ hoa, số và ký tự đặc biệt. Kết thúc đăng nhập, người quản trị sẽ thấy được màn hình khái quát cho việc quản lý máy chủ như trong hình dưới đây và có thể tiếp tục cài đặt các dịch vụ cần thiết cho mục đích sử dụng của mình.



Hình II-3. Màn hình khái quát cho quản trị máy chủ.

II.2 Trình điều khiển thiết bị

Do máy tính sử dụng nhiều thiết bị phần cứng khác nhau nên việc đảm bảo các thiết bị vận hành chính xác rất quan trọng. Với môi trường máy chủ, việc lựa chọn thiết bị tiêu chuẩn và hỗ trợ kỹ thuật là thiết yếu cho việc vận hành. Về cơ bản, trình điều khiển thiết bị là các chương trình kiểm soát thiết bị giúp máy tính/người dùng sử dụng được các thiết bị này. Để khai thác tối đa thiết bị, định kỳ cần cập nhật trình điều khiển từ nhà sản xuất thiết bị hoặc hệ điều hành.

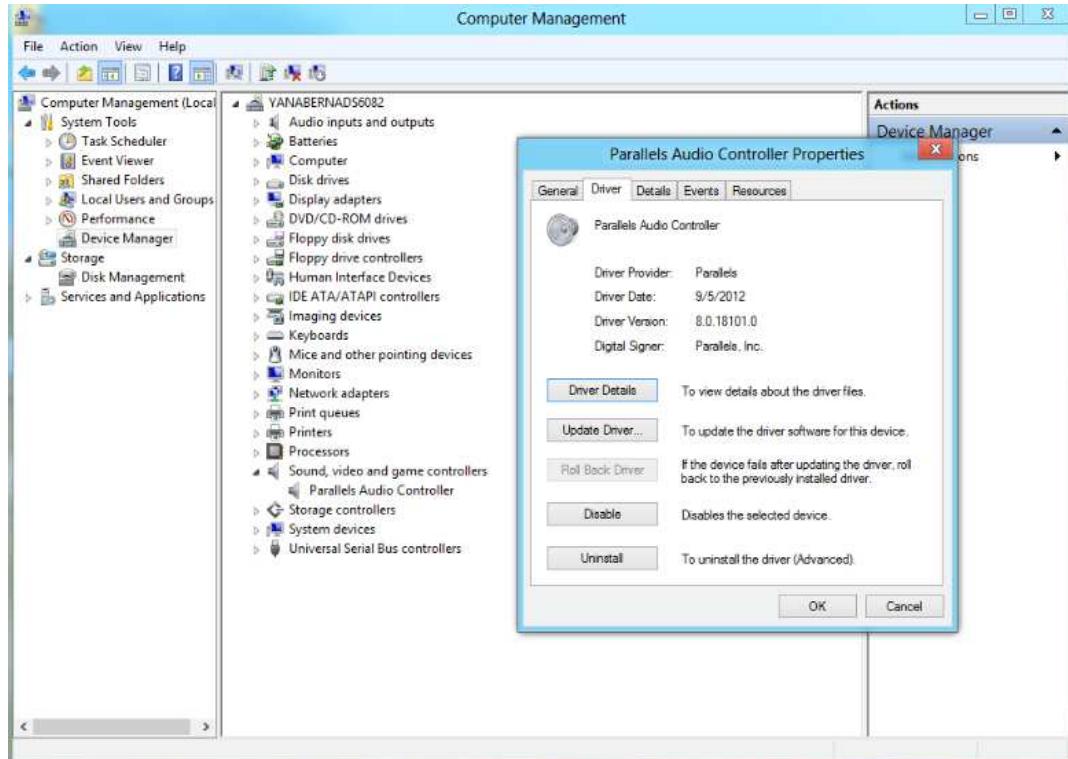
Để hoạt động được, mỗi thiết bị cần được đặt cấu hình để sử dụng một phần hoặc tất cả các tham số sau:

- Số ngắt (*Interrupt Request - IRQ*)
- Kênh truy nhập bộ nhớ trực tiếp (*Direct Memory Access -DMA*)
- Địa chỉ cổng vào/ra
- Dải địa chỉ ô nhớ

Để đơn giản hóa và thuận tiện cho việc sử dụng máy tính Intel và Microsoft đã xuất thiết bị cắm-chạy (*Plug and Play - PnP*). Các thiết bị này được máy tính và hệ điều hành nhận biết, cấu hình một cách tự động và cài đặt trình điều khiển phù hợp. Hệ điều hành tự động yêu cầu

cài đặt phần mềm điều khiển nếu phần mềm này không có sẵn. Các trình điều khiển được kiểm tra tính tương thích và toàn vẹn kỹ lưỡng được gọi trình điều khiển đã được xác nhận (*signed driver*).

Để quản lý các thiết bị như tình trạng cài đặt, trạng thái các phần mềm điều khiển, người quản trị sử dụng chương trình “*Device Manager*” như hình dưới đây.



Hình II-4. Trình quản lý thiết bị Device Manager và hộp thoại thuộc tính thiết bị.

Với mỗi thiết bị người quản trị được cung cấp chức năng

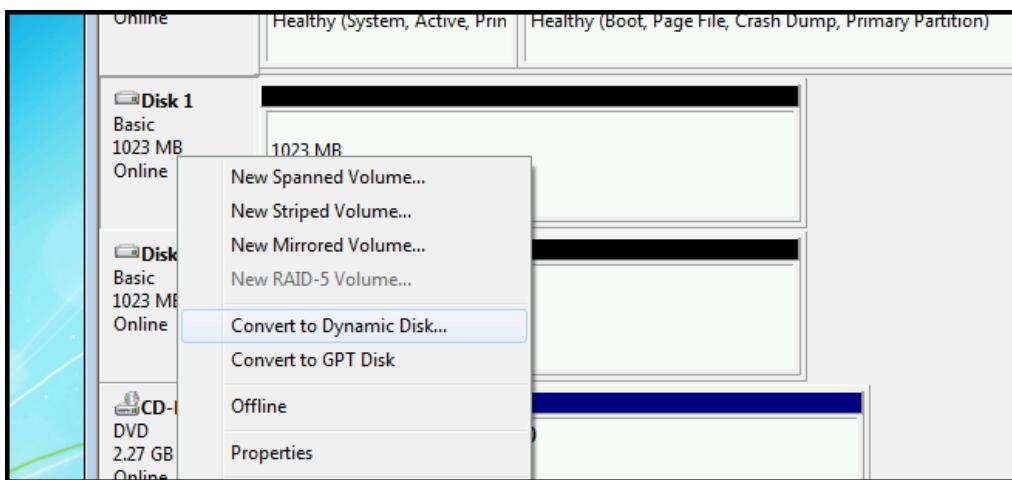
- *Thông tin chi tiết*: hiện thông tin về file chương trình điều khiển, vị trí trong ổ đĩa, nhà cung cấp...
- *Cập nhật*: giúp tải về phần mềm điều khiển mới nhất.
- *Quay lui trình điều khiển*: Sử dụng lại trình điều khiển cũ khi bản cập nhật gây lỗi
- *Cấm/cho phép*: sử dụng hay không cho phép sử dụng thiết bị.
- *Gỡ bỏ*: loại bỏ phần mềm điều khiển.

II.3 Hệ thống lưu trữ

“*Disk Management*” cung cấp giao diện đồ họa cho việc quản trị thiết bị lưu trữ. Các ổ đĩa có thể được phân chia thành các vùng lưu trữ theo kiểu truyền thống MBR (*Master Boot Record*) với tối đa 4 vùng hay theo kiểu mới GPT (*GUID partition table*) với tối đa 128 vùng. Mặt khác, phân vùng truyền thống MBR chỉ hỗ trợ kích thước tối đa cho mỗi vùng là 2TB.

Điều cần chú ý để máy tính khởi động được từ phân vùng dùng GPT cần máy tính hỗ trợ cơ chế khởi động UEFI* (*Unified Extensible Firmware Interface*).

Mỗi ổ đĩa có hai dạng: cơ bản và động. Ổ đĩa cơ bản là kiểu ổ đĩa truyền thống và là kiểu mặc định khi khởi tạo hay định dạng ổ đĩa. Kiểu ổ đĩa động cung cấp các chức năng tiên tiến như có khả năng mở rộng hay thu hẹp không gian lưu trữ một cách linh hoạt, hỗ trợ các chức năng RAID[†] mềm. Việc thay đổi kiểu ổ đĩa được thực hiện dễ dàng thông qua giao diện đồ họa như trong hình dưới đây.



Hình II-5. Giao tiếp chuyển đổi kiểu và dạng ổ đĩa.

Với mỗi phân vùng (*volume*) có thể lựa chọn một trong các dạng sau:

- Ổ đơn (*Simple Volume*): tương ứng với 1 phân vùng đơn khi dùng đĩa cứng cơ bản.
- Ổ mở rộng (*Spanned Volume*): Ổ có thể mở rộng trên nhiều ổ đĩa cứng khác nhau. Từ hệ điều hành, người dùng chỉ thấy có 1 ổ duy nhất,
- Ổ phân đoạn (*Striped Volume*): Cung cấp RAID mềm mức 0.
- Ổ đúp (*Mirrored Volume*): Cung cấp RAID mềm mức 1.
- Ổ RAID 5 (*RAID 5 Volume*): Cung cấp RAID mềm mức 5.

II.4 Người dùng và quyền truy nhập

Để sử dụng được máy tính sử dụng hệ điều hành Microsoft Windows, mỗi một người dùng cần phải có tài khoản riêng còn gọi là tài khoản người dùng. Tài khoản này được sử dụng khi:

- Người dùng truy nhập vào mạng
- Cho phép người dùng đăng nhập vào máy hay miền thư mục động.

Tài khoản cho phép người dùng truy nhập vào máy tính cụ thể được gọi là tài khoản cục bộ (*local account*). Tài khoản này chỉ có giá trị đối với một máy tính duy nhất. Khi người

* UEFI-Unified Extensible Firmware Interface: Giao tiếp firmware mở rộng hợp nhất.

† RAID - Redundant Array of Independent Disks: Chuỗi dự phòng các ổ đĩa độc lập

dùng muôn sử dụng các tài nguyên trong mạng của một miền (*domain*) người dùng cần tài khoản miền (*domain account*). Tài khoản này được tạo trên máy chủ miền và được phép truy nhập vào các tài nguyên của miền. Các thông tin người dùng được lưu trong cơ sở dữ liệu miền và được sao chép tới các máy chủ miền.

Để thuận tiện cho việc quản trị, Windows tạo sẵn một số tài khoản như quản trị (*Administrator*) và khách (*Guest*). Ngoài ra, các người dùng có vai trò và yêu cầu truy tương tự nhau có thể được xếp vào nhóm người dùng (*User group*). Điều này giúp cho việc quản trị được dễ dàng và thuận tiện. Tương tự như tài khoản người dùng, nhóm người dùng cũng phân biệt nhóm cục bộ và nhóm miền. Cụ thể như sau:

- Nhóm miền cục bộ (*Domain local group*) tương ứng với nhóm tài khoản ở bất kỳ miền nào có giá trị cục bộ.
- Nhóm toàn thể (*Global group*) chứa tài khoản người dùng và nhóm toàn thể khác áp dụng cho một miền cụ thể.
- Nhóm vạn năng (*Universal group*) áp dụng cho nhiều miền, chứa các nhóm toàn thể của các miền khác.

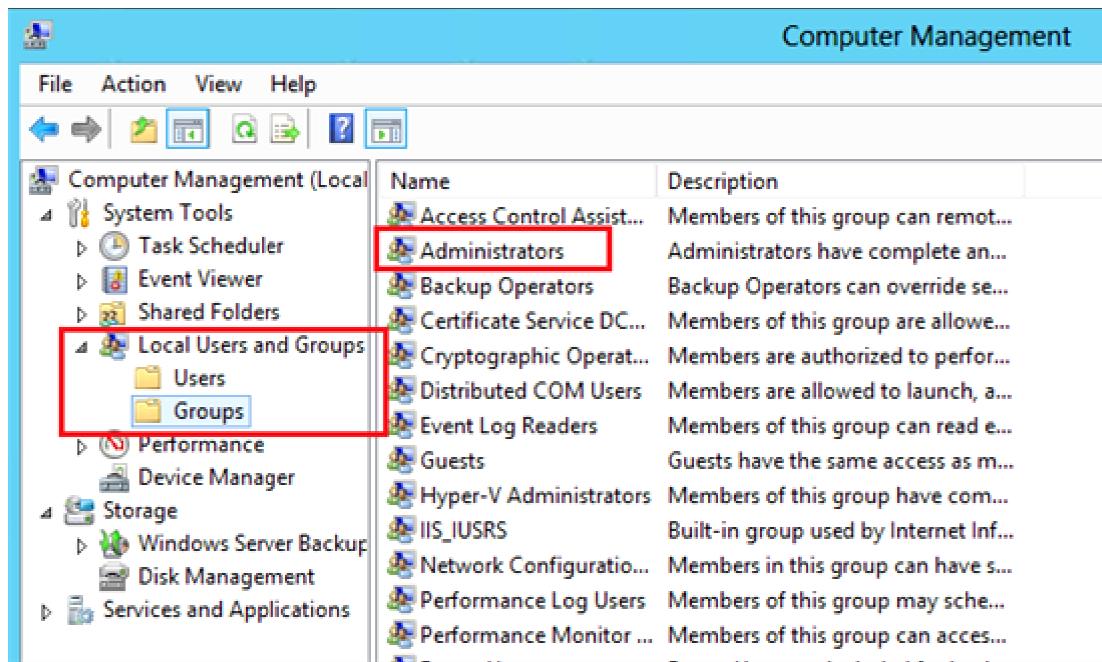
Để đơn giản cho công việc quản trị Windows Server cung cấp các nhóm tạo sẵn:

- *Domain Admins*: dùng cho các thành viên làm nhiệm vụ quản trị.
- *Domain Users*: nhóm người dùng miền.
- *Account Operators*: thành viên nhóm có thể tạo, xóa và sửa nhóm và tài khoản người dùng.
- *Backup Operators*: Sao lưu và khôi phục máy chủ miền
- *Authenticated Users*: người dùng hợp lệ
- *Everyone*: bao gồm tất cả các người dùng.

Để quản trị người dùng cục bộ, người dùng quản trị truy nhập “*Local User and Group*” của “*Server manager*” như trong Hình II-6 dưới đây. “*Active Directory Users and Computers*” cung cấp chức năng quản lý các máy tính và người dùng trong miền.

Mỗi tài khoản người dùng cần cung cấp các thông tin cơ bản sau:

- Tên người dùng: được dùng để định danh người sử dụng khi truy nhập vào mạng
- Mật khẩu: được gán cho từng tài khoản người dùng và đảm bảo chỉ người dùng được phép mới truy nhập được vào mạng
- Các thuộc tính của tài khoản người dùng như họ tên, số điện thoại, thư điện tử



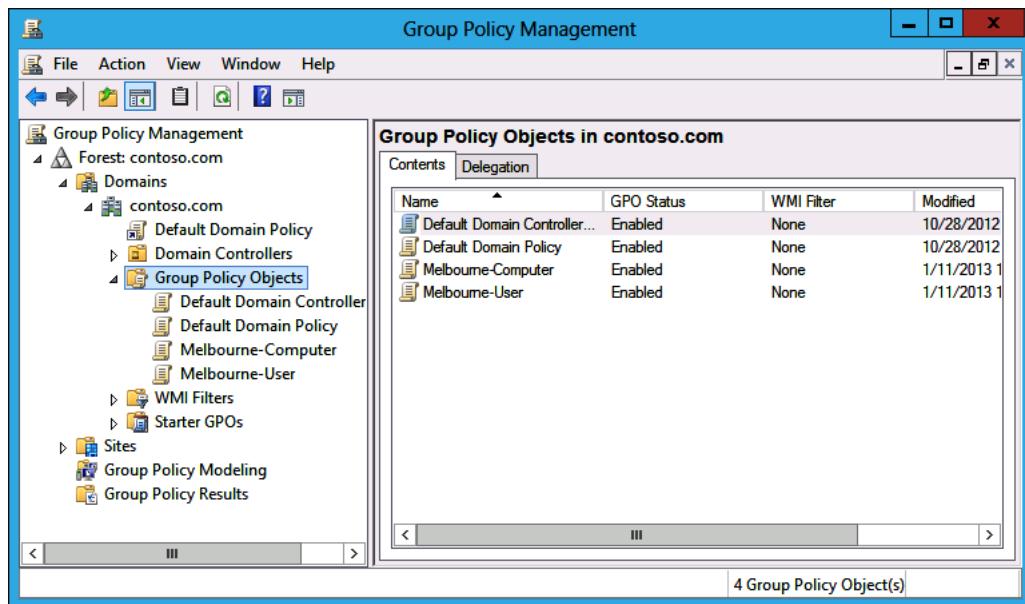
Hình II-6. Giao diện quản trị người dùng và nhóm cục bộ

Với mỗi tài nguyên có kiểm soát truy nhập người dùng có thể thực hiện hay cấp các quyền tiêu biểu như sau:

- Toàn quyền kiểm soát (*Full control*) : bao gồm quyền đọc, ghi, sửa và thực thi đối tượng tài nguyên, thay đổi thuộc tính và quyền; cũng như lấy quyền sở hữu các đối tượng tài nguyên.
- Sửa (*Modify*): cho phép đọc ghi sửa và thay đổi thuộc tính đối tượng tài nguyên.
- Đọc (*Read*): Hiển thị dữ liệu, thuộc tính, chủ sở hữu và quyền của các đối tượng tài nguyên.
- Ghi (*Write*): Ghi và thêm dữ liệu vào đối tượng tài nguyên và đọc hay thay đổi các thuộc tính tài nguyên.

II.5 Chính sách nhóm

Công cụ quản trị nhóm là tính năng quan trọng với Windows cho phép kiểm soát môi trường làm việc với tài khoản người dùng và máy tính. Ngoài ra, quản trị chính sách nhóm cho phép quản lý và cấu hình tập trung với hệ điều hành, ứng dụng và các cài đặt của người dùng giúp đơn giản hóa công việc quản trị.



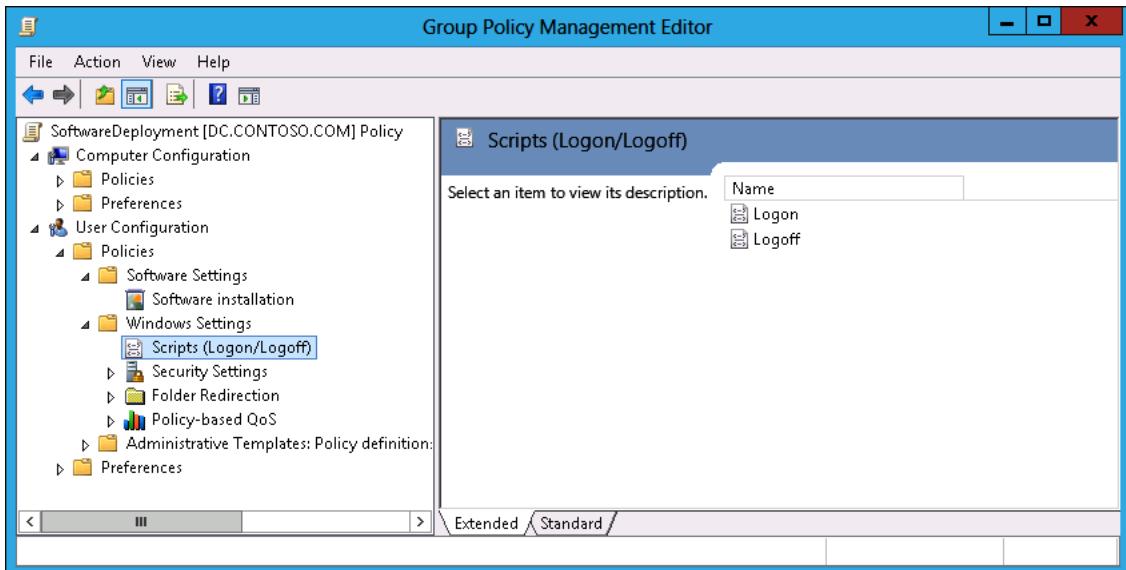
Hình II-7. Giao diện quản trị chính sách nhóm.

Chính sách nhóm xây dựng dựa trên các đối tượng chính sách nhóm GPO (*Group policy objects*). Đây là tập hợp các hướng dẫn cấu hình mà máy tính có thể áp dụng cho miền, vị trí (*site*) hay ở cấp độ thấp hơn. Mặc dù, việc áp dụng các chính sách nhóm làm thay đổi danh mục đăng ký (*Registry*) song việc này vẫn dễ dàng hơn nhiều so với việc sửa đổi bằng tay.

Các đối tượng chính sách nhóm bao gồm các cài đặt của người dùng và máy tính. Các cài đặt có thể liên quan đến hệ thống (*System settings*) bao gồm cài đặt ứng dụng, màn hình làm việc và các dịch vụ hệ thống. Ngoài ra còn có thể là các cài đặt như:

- Cài đặt an ninh (*Security settings*): cài đặt an ninh mạng, miền và máy tính cục bộ
- Cài đặt phần mềm (*Software installation settings*): Quản lý việc cài đặt phần mềm, cập nhật và gỡ bỏ.
- Cài đặt mã (*Scripts settings*): Các đoạn mã dùng khi máy tính bật và đóng, người dùng đăng nhập hay thoát.
- Cài đặt chuyển hướng thư mục (*Folder redirection settings*): Thư mục của người dùng trên mạng.

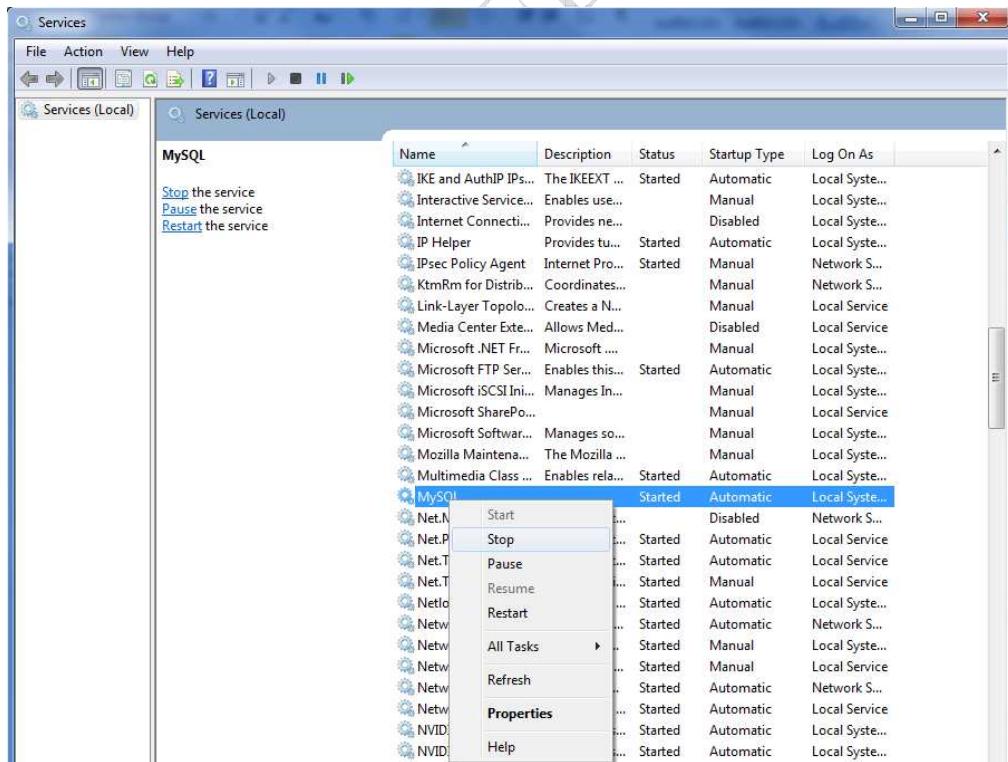
Chính sách nhóm có thể sử dụng trong máy tính cụ thể và có giá trị cục bộ dùng để xây dựng các chính sách giám sát việc hoạt động của máy tính như là xác định việc lưu các sự kiện an ninh trong “*Event viewer*”. Mặt khác, việc xác định người dùng hay nhóm người dùng có đặc quyền gì với máy tính cũng được thiết lập thông qua chính sách nhóm. Tương tự, quản trị hệ thống có thể áp dụng các biện pháp an ninh như cấm hay cho phép các cài đặt an ninh của máy tính, cụ thể thay đổi tên của tài khoản hay truy nhập vào ổ đĩa nhất định.



Hình II-8. Giao diện gán chính sách cho việc đăng nhập/xuất.

II.6 Các dịch vụ của Windows

Dịch vụ là chương trình đang chạy (còn gọi là tiến trình) nhằm thực hiện chức năng hệ thống cụ thể như phục vụ việc truy nhập file, in ấn, thông báo lỗi... Thông thường, các dịch vụ hoạt động ở chế độ nền mà không cần giao diện người dùng. Việc quản trị các dịch vụ sử dụng giao diện thông qua trình Services như trong hình dưới đây.



Hình II-9. Giao diện quản trị dịch vụ và thuộc tính của dịch vụ.

Dịch vụ có thể được chạy theo các cách như sau:

- **Tự động (Automatic):** Tự động chạy khi hệ thống khởi động.
- **Tự động khởi động trễ (Automatic Delayed Start):** Tự động khởi động sau các dịch vụ được dán nhãn tự động khởi động xong (khoảng 2 phút).
- **Thủ công (Manual):** Người dùng hay dịch vụ phụ thuộc có thể khởi động dịch vụ. Dịch vụ kiểu này không được chạy khi hệ thống khởi động.
- **Cấm (Disable):** Ngăn chặn dịch vụ được chạy do người dùng hay hệ thống cũng như dịch vụ phụ thuộc.

Các tài khoản mà dịch vụ có thể dùng để chạy gồm có:

- **Hệ thống (Local System):** Tài khoản có rất nhiều đặc quyền và truy nhập toàn bộ tài nguyên trên máy cục bộ
- **Dịch vụ cục bộ (NT Authority\LocalService):** Có đặc quyền giống như người dùng cục bộ. Khi truy nhập mạng không cần mật khẩu và phiên làm việc.
- **Dịch vụ mạng (NT Authority\NetworkService):** có cùng mức truy nhập như người dùng cục bộ. Khi sử dụng mạng giống như tài khoản cục bộ.

Để đảm bảo an toàn và hạn chế rủi ro, nên sử dụng tài khoản với quyền tối thiểu để chạy các dịch vụ.

Chương III. QUẢN TRỊ CÁC MÁY CHỦ DỊCH VỤ CỦA WINDOWS SERVER

Chương này trình bày cách thức triển khai và quản lý các dịch vụ căn bản cho môi trường mạng của Windows. Các dịch vụ gồm có tên miền và cấu hình máy tính tự động, chia sẻ và quản lý các tài nguyên mạng như thư mục động, máy in, dịch vụ truy nhập từ xa, dịch vụ Web. Trong các dịch vụ này thư mục động là dịch vụ quan trọng và tiêu biểu của hệ điều hành máy chủ Windows. Dịch vụ này cho phép quản lý thông nhất người dùng và các tài nguyên mạng.

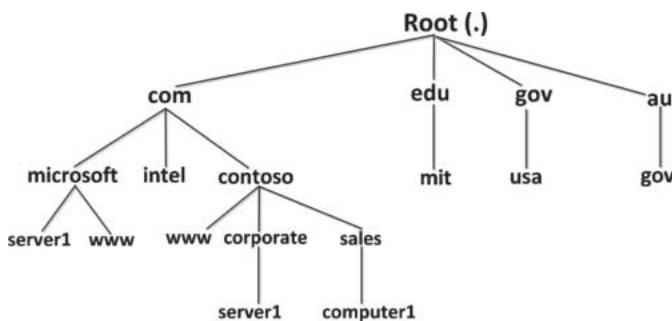
III.1 Máy chủ dịch vụ DNS và DHCP

III.1.1 Dịch vụ tên miền DNS

Dịch vụ tên miền là dịch vụ thiết yếu trong mạng Internet. Mỗi khi người dùng truy nhập tài nguyên trên mạng như trang Web, người dùng phải nhập vào địa chỉ trang web. Máy tính của người dùng sử dụng dịch vụ DNS để xác định vị trí vật lý (địa chỉ mạng) của máy tính chứa nội dung trang web mà người dùng muốn truy nhập đến.

Về mặt kỹ thuật, DNS là hệ thống quản lý cơ sở dữ liệu phân tán dựa trên mô hình phân cấp chủ/khách để chuyển đổi tên máy chủ hay tên miền thành địa chỉ mạng Internet. DNS mang lại các ưu điểm sau:

- Dễ sử dụng và đơn giản: người dùng chỉ cần nhớ tên của máy tính hay tài nguyên mạng thay vì các con số của địa chỉ mạng.
- Mở rộng: phân tán công việc phân rã tên/địa chỉ mạng trên nhiều máy chủ và cơ sở dữ liệu.
- Nhất quán: các địa chỉ mạng có thể thay đổi trong khi tên của các máy vẫn giữ nguyên làm cho các tài nguyên mạng dễ dàng xác định hơn.



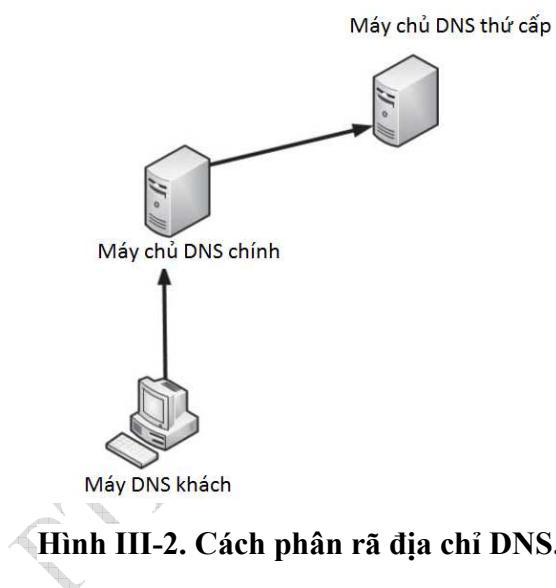
Hình III-1. Cấu trúc cây tên miền.

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

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

Miền gốc nằm trên đỉnh của cây tên miền

- Tên miền gốc .com, .edu, .vn
- Tên miền mức 2: microsoft.com

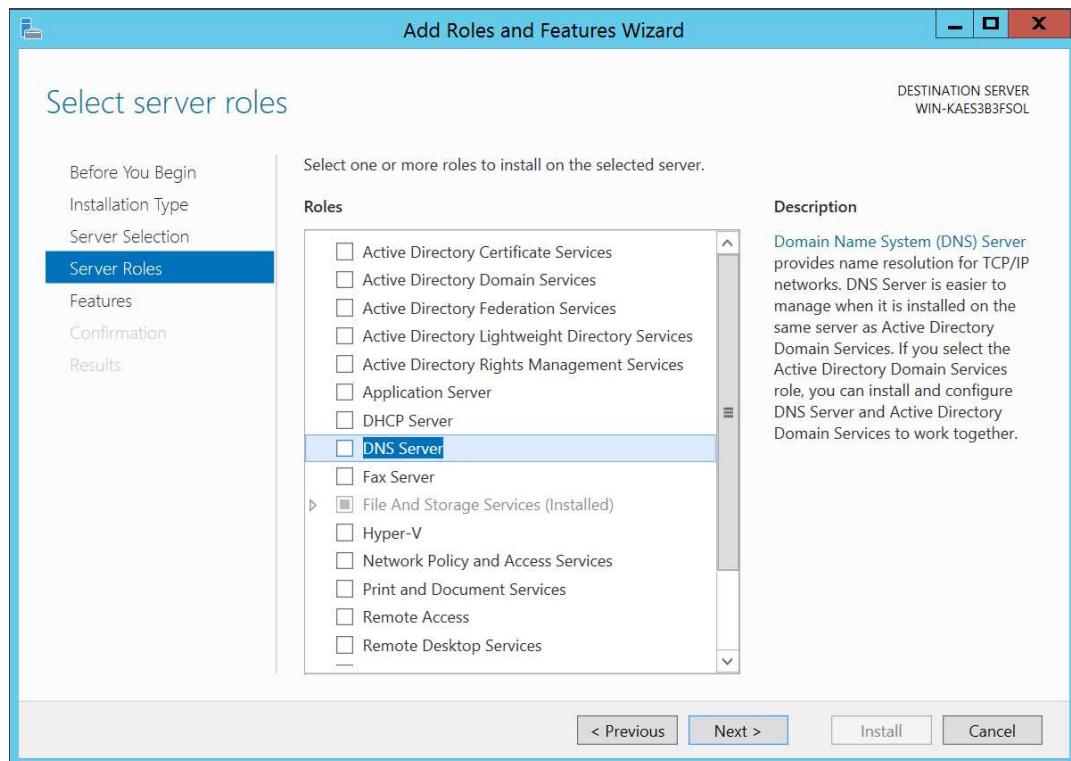


Hình III-2. Cách phân rã địa chỉ DNS.

Mỗi khi cần xác định địa chỉ máy DNS khách (máy người dùng) gửi yêu cầu tới máy chủ DNS chính hay máy chủ DNS của mạng ứng với người dùng. Nếu máy chủ DNS chính có sẵn thông tin thì nó sẽ gửi trả thông điệp kết quả cho người dùng. Nếu không, máy chủ DNS này sẽ chuyển tiếp yêu cầu của người dùng tới máy chủ DNS thứ cấp. Quá trình tiếp diễn cho đến khi nhận được kết quả.

Cài đặt DNS

Việc cài đặt máy chủ DNS khá dễ dàng qua tiện ích “*Server Manager*”. Chức năng máy chủ DNS được liệt kê trong phần lựa chọn các chức năng cài đặt như trong hình dưới. Người quản trị tuân theo hướng dẫn của tiện ích để hoàn tất việc cài đặt.



Hình III-3. Giao diện chọn chức năng DNS.

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

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

Các dạng bản ghi DNS

Các thông tin của máy chủ DNS được lưu vào các bản ghi có dạng như sau

- Bản ghi khởi đầu SOA: là bản ghi đầu tiên trong cơ sở dữ liệu xác định các tham số chung cho vùng DNS bao gồm định danh máy chủ ủy quyền của vùng đó.

Ví dụ: @ IN SOA win2k3r2.example.com. hostmaster.example.com.(....)

- Bản ghi máy chủ: thông tin căn bản ánh xạ tên của một máy chủ ra địa chỉ mạng Internet

Ví dụ: SMTP IN A 192.168.3.144

- Bản ghi CNAME: ánh xạ máy chủ tới một tên có sẵn

Ví dụ: www IN CNAME chaos.example.com.

- Bản ghi NS: lưu định danh các máy chủ DNS trong miền

Ví dụ: *example.com. IN NS Hostname.example.com*

- Bản ghi dịch vụ SRV: hỗ trợ việc tự động phát hiện các tài nguyên TCP/IP có trên mạng

Ví dụ: *ldap.tcp.example.com. 86400 IN SRV 10 100 389 hsv.example.com*

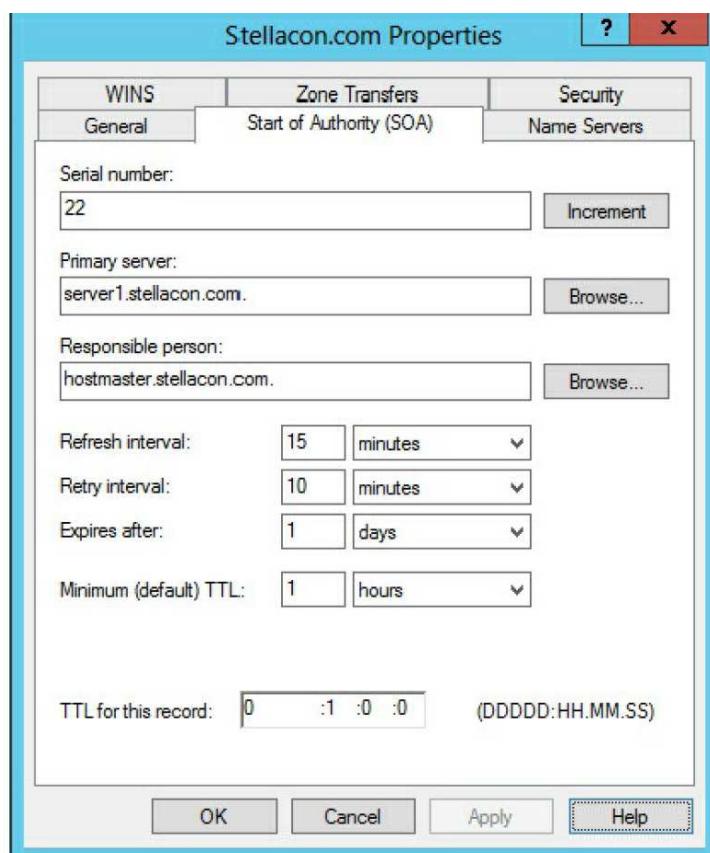
- Bản ghi con trả PTR: là các bản ghi tìm kiếm ngược

Ví dụ: *10.1.168.192.in-addr.arpa. IN PTR www.example.com.*

- Bản ghi máy chủ thư: chỉ định máy chủ nhận thư của miền.

Ví dụ: *example.com. IN MX 10 mail.example.com.*

Việc điền các thông tin vào các bản ghi này có thể được thực hiện một cách thuận tiện thông qua việc sử dụng giao diện đồ họa như cửa sổ nhập bản ghi SOA dưới đây.



Hình III-4. Cửa sổ nhập bản ghi SOA.

Một số điểm chú ý

Khi cài đặt và cấu hình máy chủ DNS, cần xem xét một số vấn đề sau:

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

Với mức độ sử dụng tiêu biểu, mỗi máy chủ DNS cần khoảng 4MB bộ nhớ để chạy, khi số lượng các bản ghi tăng thì máy chủ DNS cần thêm bộ nhớ để hoạt động. Trung bình 1000 bản ghi cần thêm khoảng 100KB bộ nhớ.

Trong mạng tốc độ cao với kết nối tương đối tin cậy thì có thể sử dụng một máy chủ DNS. Song nếu mạng có nhiều máy và dùng thiết kế một mạng con thì có thể cần nhiều hơn một máy chủ DNS để đảm bảo độ tin cậy. Với hầu hết các trường hợp nên sử dụng hai máy chủ để lưu các thông tin về DNS nhằm nâng cao độ chịu đựng lỗi.

III.1.2 Dịch vụ DHCP

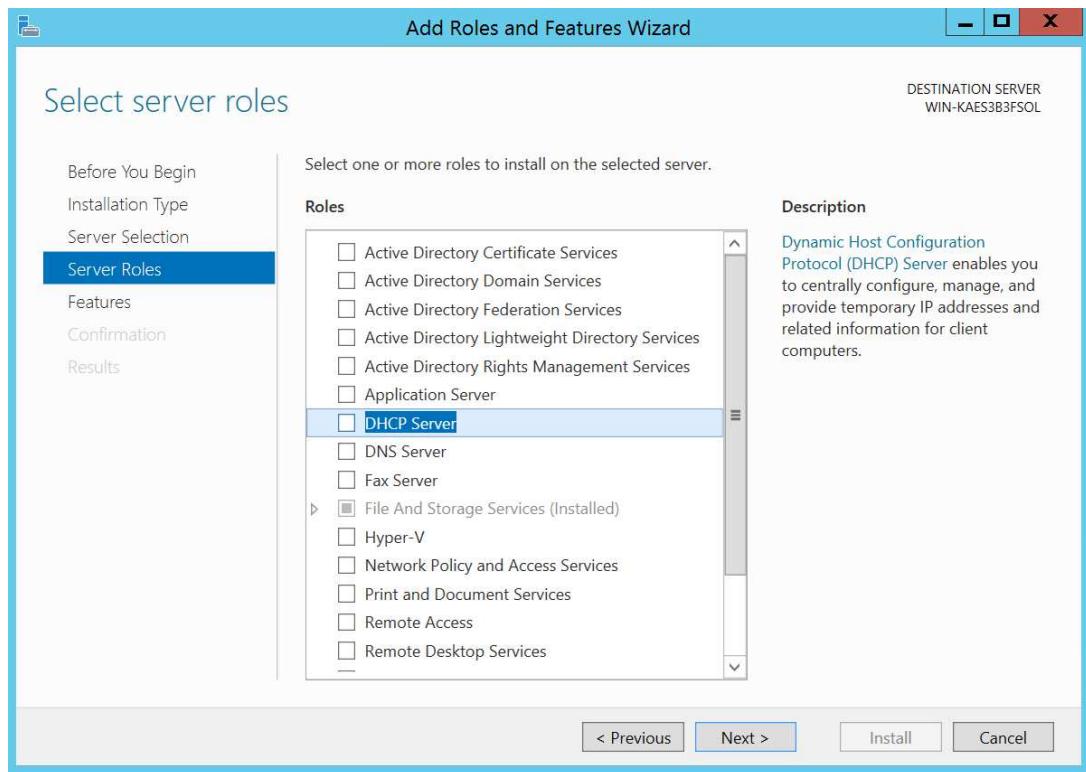
DHCP giúp việc quản lý và cấp phát tập trung và tự động địa chỉ mạng Internet cho các máy tính trong mạng. Ngoài ra, dịch vụ này còn giúp cài đặt các tham số khác một cách tự động cho các máy tính trong mạng như địa chỉ máy chủ DNS, cổng kết nối ra bên ngoài.

Máy chủ DHCP duy trì danh sách các địa chỉ Internet và cấp cho các máy tính trong mạng sử dụng theo khoảng thời gian xác định thường gọi là cho thuê địa chỉ. Việc sử dụng DHCP làm cho việc cấu hình mạng trở nên dễ dàng đặc biệt khi có nhiều máy tính. Dải địa chỉ mạng Internet được sử dụng hiệu quả hơn do địa chỉ Internet chỉ được cấp phát khi có yêu cầu. Tuy nhiên, máy chủ DHCP trở thành điểm thắt nút trong mạng. Nếu máy chủ này không hoạt động toàn bộ các máy tính sẽ không được đặt cấu hình chính xác và sẽ không hoạt động theo.

Khi xây dựng hạ tầng cho DHCP cần xem xét số lượng mạng vật lý hay lô-gíc cần tự động cấu hình IP, vị trí bộ định tuyến và số mạng LAN ảo. Trên cơ sở đó xác định các tham số cần thiết cho máy chủ DHCP hoạt động.

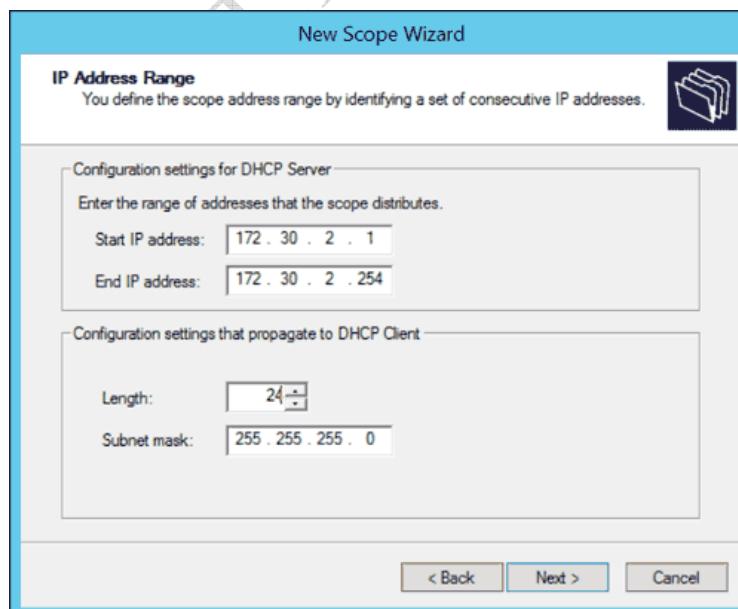
Tham số quan trọng cần xác định là dải địa chỉ mà máy chủ DHCP quản lý. Trong dải địa chỉ này cần xác định các nhóm địa chỉ dành riêng không dùng để cấp phát cho các máy tính trong mạng. Nhóm địa chỉ có thể phục vụ mục đích riêng như gán cố định cho các máy chủ/dịch vụ của mạng. Không gian địa chỉ còn lại dùng để cấp phát cho các máy trong mạng.

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



Hình III-5. Cài đặt dịch vụ DHCP.

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



Hình III-6. Định nghĩa dải địa chỉ cho cấp phát động DHCP.

III.1.3 Kiểm tra cài đặt

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

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

III.2 Thư mục động

Thư mục động (*Active Directory*) là công nghệ cung cấp dịch vụ thư mục của Microsoft. Về cơ bản, dịch vụ thư mục nhằm lưu trữ, tổ chức, và đảm bảo truy nhập các thông tin trong thư mục. Trong môi trường mạng, dịch vụ thư mục mạng được dùng để xác định, quản lý, quản trị và tổ chức các mục, tài nguyên mạng dùng chung như ổ đĩa, thư mục, máy in, người dùng...

III.2.1 Các dịch vụ

Thư mục động sử dụng cách thức đặt tên theo kiểu tên miền Internet và cung cấp một số dịch vụ căn bản như sau:

- Giao thức truy nhập thư mục đơn giản LDAP (*Lightweight Directory Access Protocol*) là giao thức mức ứng dụng dùng cổng 389 cho truy vấn và thay đổi dữ liệu sử dụng dịch vụ thư mục mạng trên mạng Internet. Các đối tượng trong thư mục được tổ chức theo giới hạn của cơ quan hay địa lý.
- Cơ chế xác thực Kerberos sử dụng giao thức xác thực mạng máy tính cho phép các máy xác định định danh của mình qua mạng không an toàn một cách đảm bảo.
- Quản trị mạng tập trung cho phép tổ chức các tài nguyên mạng bao gồm người dùng, nhóm, máy in, máy tính và các đối tượng khác sao cho các người dùng mạng được gán mật khẩu, quyền sử dụng các đối tượng này.

Khả năng quản trị mạng tập trung là một trong những tính năng quan trọng và thiết yếu với việc chia sẻ và kiểm soát truy nhập tới các tài nguyên của vị trí (*site*) hay miền.

III.2.2 Tổ chức thư mục động

Về mặt lô-gíc thư mục động bao gồm

- Đơn vị tổ chức (*Organisation Units*): là các đối tượng bên trong một miền cho phép bố trí và nhóm các tài nguyên lại để làm thuận tiện cho công việc quản trị và cho phép ủy thác (*delegate*) các quyền quản trị.
- Miền (*Domain*) là đơn vị lô-gíc các máy tính và tài nguyên mạng xác định ranh giới an ninh. Miền sử dụng một cơ sở dữ liệu miền động đơn lẻ để chia sẻ thông tin chung về an ninh và người dùng cho phép quản lý tập trung toàn bộ người dùng, nhóm và tài nguyên mạng. Một cơ quan hay doanh nghiệp có thể có nhiều miền tương ứng với cơ cấu tổ chức.

- Cây (*Tree*) chứa một hay nhiều miền dùng chung không gian định danh gốc. Có thể hình dung cây tập hợp các miền chia sẻ không gian tên Internet như fit.ptit.edu.vn.
- Rừng (*Forest*) chứa một hay nhiều cây và không gian định danh có thể tách biệt. Miền đầu tiên trong rừng được gọi là miền gốc của rừng (*forest root domain*).
- Quan hệ tin cậy (*Trust relationship*) cho phép người dùng từ các miền khác nhau sử dụng tài nguyên mạng của các miền.

Trong mỗi miền của thư mục động có máy chủ đặc biệt gọi là máy chủ miền (*Domain controller*) chịu trách nhiệm lưu bản sao thông tin tài khoản và an ninh của miền. Để chống lỗi có thể sử dụng nhiều máy chủ miền. Tất cả các máy chủ miền trong một miền nhận các thay đổi và sao chép các sửa đổi này vào phần miền được lưu trong toàn bộ các máy chủ còn lại. Kết quả, tất cả các máy chủ miền đều ngang hàng với nhau và cùng quản lý việc sao lưu.

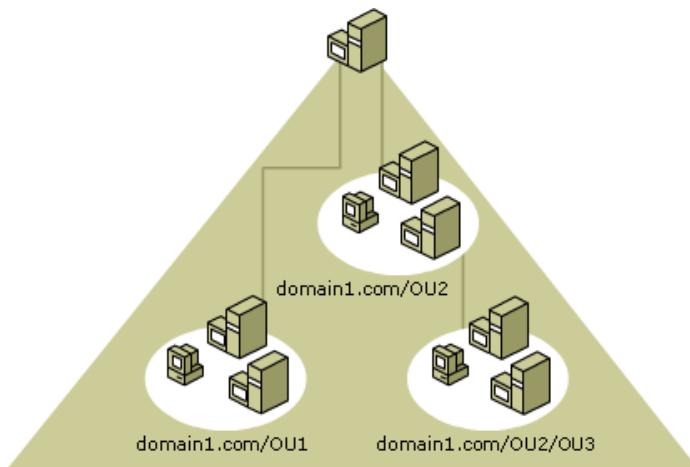
Máy chủ danh mục toàn cục (*global catalog*) là máy chủ miền lưu bản sao đầy đủ của toàn bộ các đối tượng của thư mục động của miền mà máy chủ hoạt động. Các ứng dụng và người dùng truy vấn danh mục toàn cục để xác định bất kỳ đối tượng nào trong thư mục động. Danh mục này được tạo ra một cách tự động khi cài đặt máy chủ miền đầu tiên.

Máy chủ miền chỉ đọc là máy chủ miền đặc biệt dùng cho các nhánh phòng ban của tổ chức và các máy chủ đặt trong môi trường an ninh kém. Máy chủ miền này chỉ lưu trữ bản sao không sửa được của thư mục động.

Máy chủ miền duy trì danh mục toàn cục (*Global catalog*) chứa đựng thông tin của từng đối tượng trong cây và rừng. Danh mục toàn cục giúp truy nhập các đối tượng giữa các miền khác nhau cũng như lưu các thuộc tính được tìm kiếm thường xuyên như tên người dùng, tên máy tính. Danh mục này được tự động tạo ra khi triển khai máy chủ miền đầu tiên của rừng (*forest*).

Mặt khác danh mục toàn cục được dùng khi người dùng đăng nhập giúp liệt kê thành viên nhóm và xác định định danh người dùng khi có nhiều miền.

Như phần đầu đã đề cập, đơn vị tổ chức OU (*Organisation Unit*) trợ giúp việc sắp xếp các đối tượng trong miền và giảm thiểu số miền cần thiết. Đây là phần tử nhỏ nhất mà người quản trị có thể cài đặt các chính sách nhóm hay ủy thác quyền quản trị. Đơn vị tổ chức có thể lưu trữ người dùng, nhóm, máy tính và các đơn vị tổ chức khác. Các đơn vị tổ chức tạo trước (như máy tính, người dùng) thì không thể gán quyền hay chính sách nhóm.



Hình III-7. Đơn vị tổ chức của thư mục động.

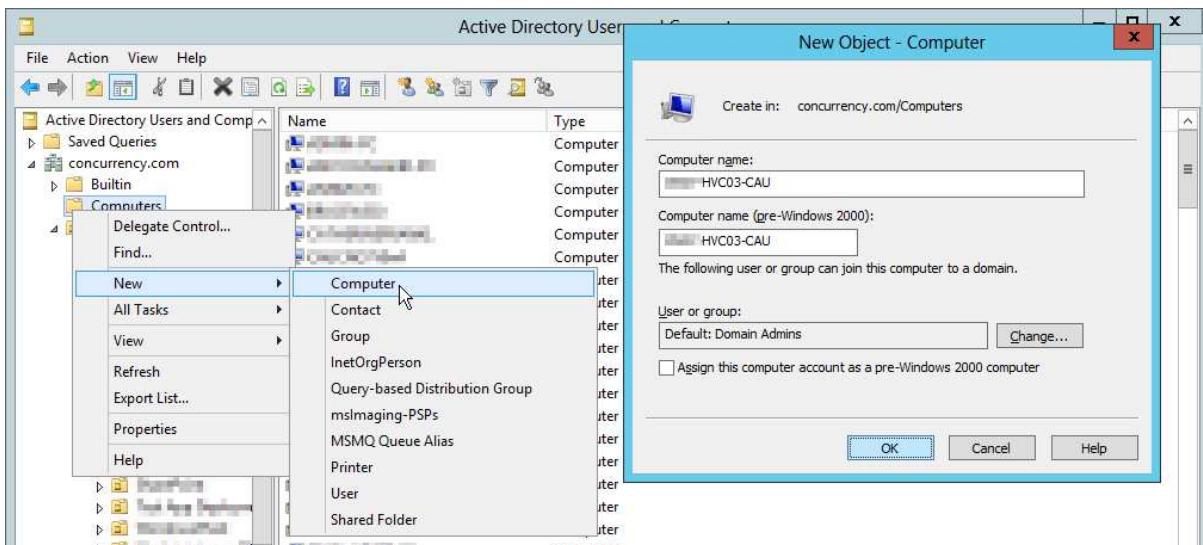
Trong thư mục động, các đối tượng chính là tập được đặt tên riêng biệt chứa đựng các thuộc tính hay đặc tính thể hiện tài nguyên mạng của thư mục động. Các đối tượng phổ biến trong thư mục động là máy tính, người dùng, nhóm. Mỗi đối tượng được gắn số duy nhất gọi là GUID (*Globally unique identifier*) hay định danh an ninh (*Security identifier*).

Lược đồ (*Schema*) trong thư mục động xác định định dạng các đối tượng và các thuộc tính hay trường trong mỗi đối tượng. Ví dụ: người dùng có tên, họ số điện thoại, thư điện tử. Các lược đồ này có thể được mở rộng một cách linh hoạt để hỗ trợ nhiều ứng dụng khác nhau.

Tài khoản người dùng trong thư mục động, còn gọi là tài khoản người dùng miền, được lưu trong máy chủ miền cho phép người dùng truy nhập tới các tài nguyên bên trong một miền miễn là người dùng đó có đủ quyền phù hợp. Liên kết với tài khoản người dùng là danh sách thư mục và dữ liệu về môi trường làm việc của người dùng và cài đặt ứng dụng. Có ba kiểu hồ sơ người dùng như sau:

- Hồ sơ người dùng cục bộ (*Local user profile*): được lưu trong ổ cứng cục bộ mà người dùng đăng nhập.
- Hồ sơ người dùng di chuyển (*Roaming user profile*): được tạo và lưu trong thư mục chia sẻ trên máy chủ mạng. Với bất cứ máy tính nào trong miền người dùng có cùng một cài đặt.
- Hồ sơ người dùng bắt buộc (*Mandatory user profile*): được dùng như hồ sơ người dùng chuyển vùng nhưng các thay đổi của người dùng không được lưu lại.

Tài khoản ứng với máy tính cung cấp công cụ để theo dõi và giám sát việc truy nhập của máy tính vào mạng và tài nguyên của miền và tương ứng duy nhất với một máy tính.



Hình III-8. Tạo tài khoản máy tính trong miền.

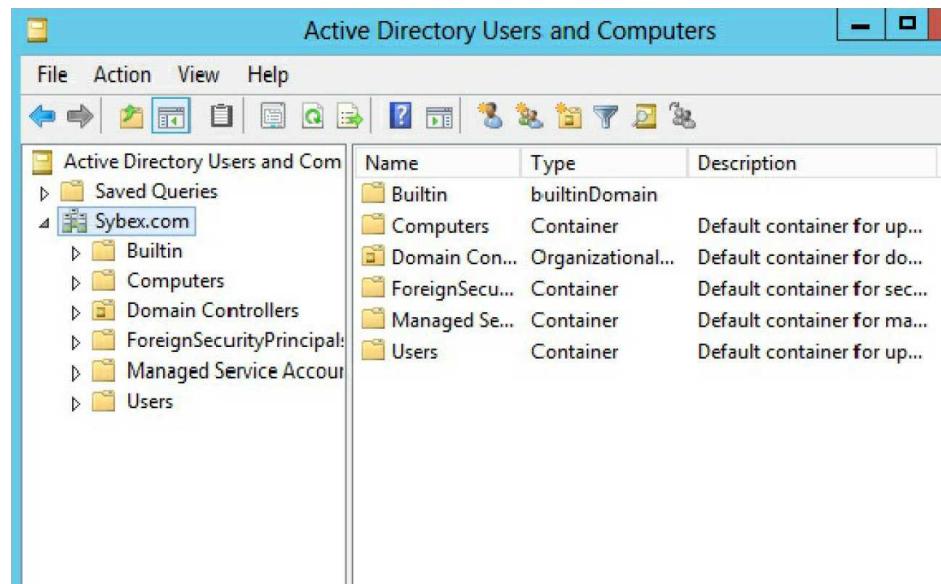
Để người dùng và máy tính có thể truy nhập được các tài nguyên của miền, người dùng và máy tính cần phải thực hiện thao tác gia nhập miền. Nói cách khác, người quản trị miền cần phải thêm máy tính vào trong danh sách quản lý của miền.

III.2.3 Tiện ích quản trị

Để thực hiện việc quản trị tập trung, thư mục động được trang bị các phần mềm chức năng như sau:

- *Active Directory Users and Computers* dùng để quản lý người dùng, nhóm, các máy tính và đơn vị tổ chức
- *Active Directory Domains and Trusts* cho phép quản trị các độ tin cậy miền, các mức phục vụ miền và rùng và hậu tiếp tố tên người dùng
- *Active Directory Sites and Services* quản trị bản sao thư mục giữa các điểm.
- *Active Directory Administrative Center* quản trị và cung cấp thông tin trong thư mục bao gồm quản lý người dùng, nhóm, máy tính, miền, máy chủ miền và các đơn vị tổ chức.

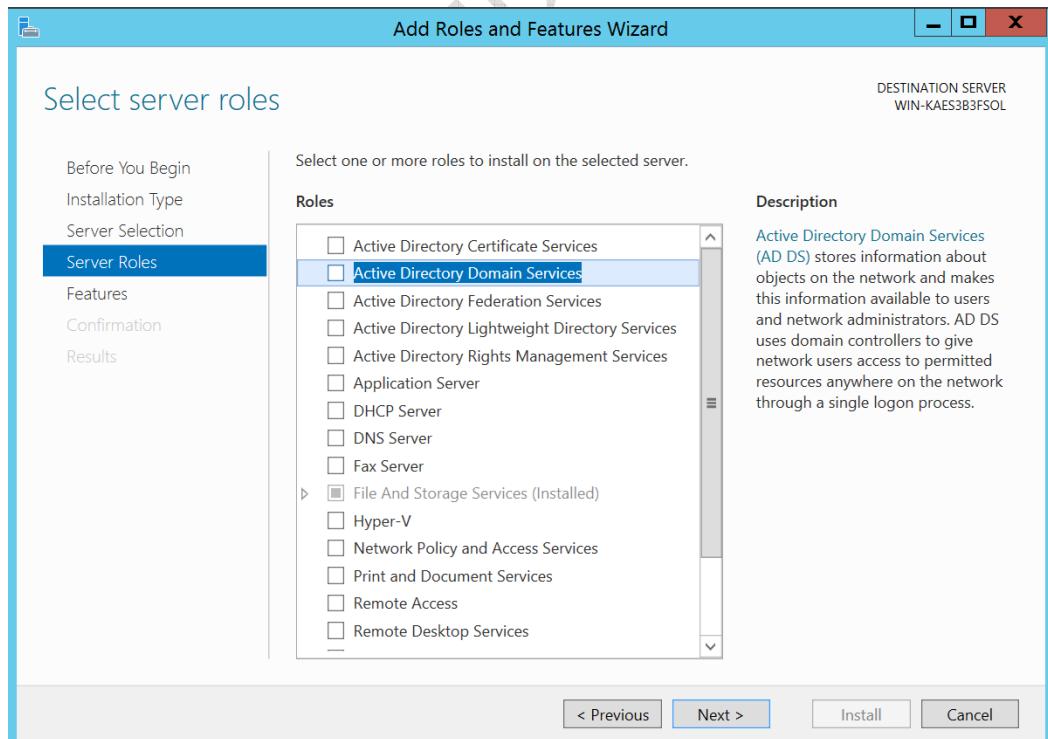
Hình III-9 giới thiệu các chức năng quản lý máy tính và người dùng cơ bản trong thư mục động với tên miền được định nghĩa là Sybex.com. Phía dưới tên miền chính là các tài nguyên có thể quản lý được của hệ thống mạng.



Hình III-9. Giao diện quản trị người dùng thư mục động.

III.2.4 Cài đặt

Việc cài đặt thư mục động là quá trình đơn giản và dễ dàng. Ở những phiên bản đầu người quản trị cần phải xác định máy chủ miền chính và máy chủ miền dự phòng. Việc thay đổi vai trò có thể dẫn đến việc cài đặt lại hệ điều hành. Với bản Server 2012, người quản trị có thể lựa chọn máy chủ miền sau khi cài đặt thành công dịch vụ thư mục động.



Hình III-10. Cài đặt dịch vụ thư mục động.

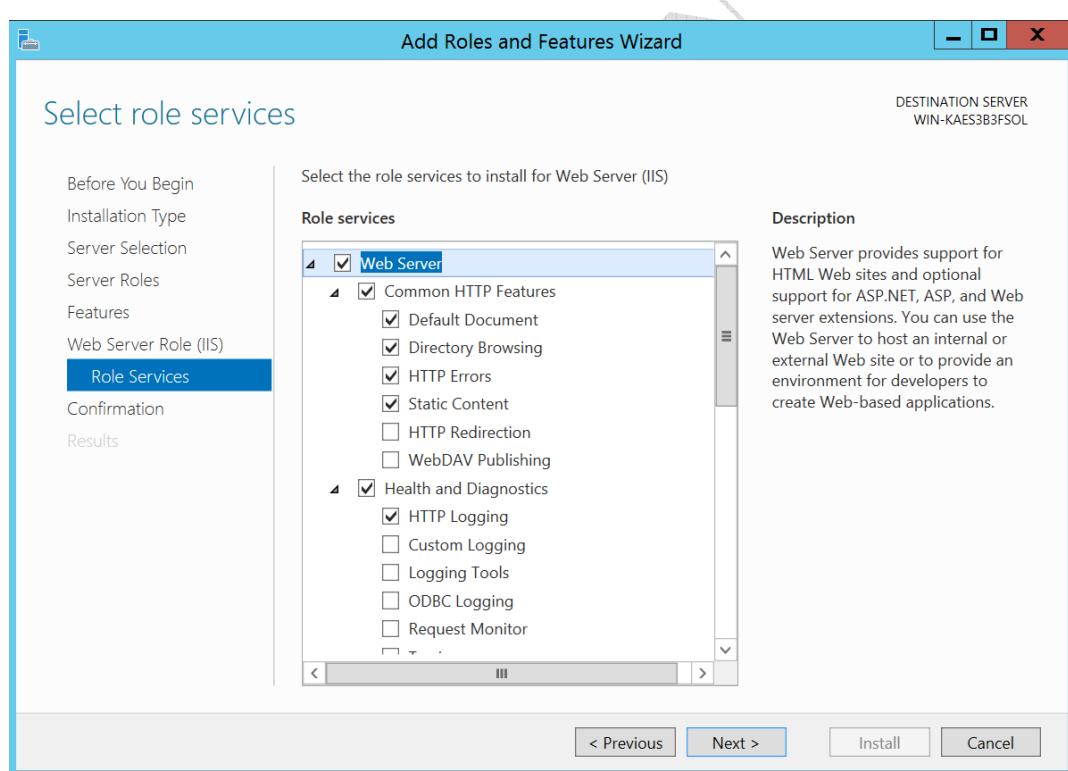
Giao diện quản lý máy chủ cho phép người quản trị lựa chọn chức năng thư mục động như trong hình và thực hiện theo các hướng dẫn của chương trình để hoàn tất việc cài đặt.

Để kiểm tra việc cài đặt, người quản trị có thể theo dõi trong mục “Event Log” hoặc kiểm tra trong danh mục các chương trình hỗ trợ việc quản trị để xem các tiện ích quản trị của thư mục động.

III.3 Dịch vụ web

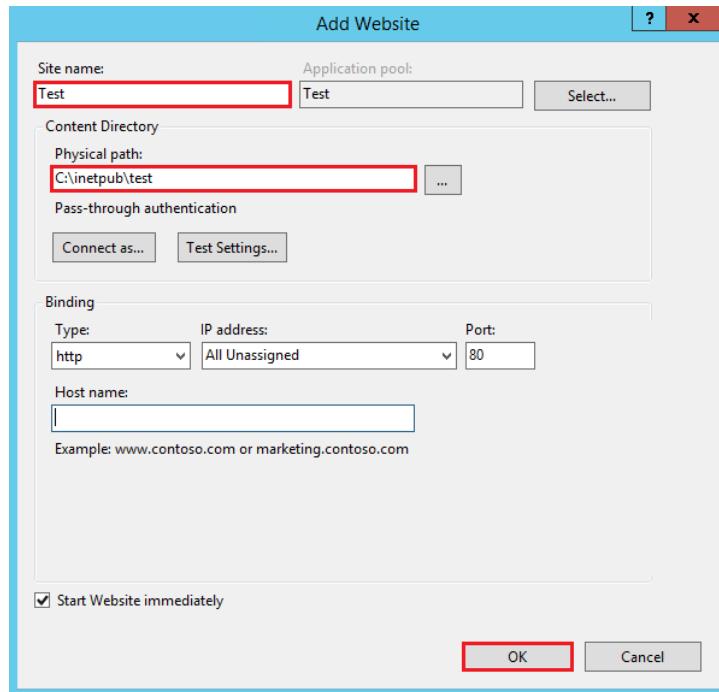
Web là hệ thống các tài liệu dạng siêu văn bản liên kết với nhau (trang web) mà người dùng có thể xem được nhờ trình duyệt. Các tài liệu Web được soạn thảo nhờ vào ngôn ngữ đánh dấu HTML. Các trang web truyền thống là trang web tĩnh. Nghĩa là, nội dung các trang này không thay đổi nếu không có sự can thiệp của con người. Các trang web được lưu trong máy chủ web và dùng cổng số 80 để người dùng truy nhập vào.

Trong môi trường máy chủ Windows, dịch vụ Web được cung cấp thông qua dịch vụ thông tin Internet IIS (*Internet Information Services*). Ngoài dịch vụ Web, người quản trị có thể cài đặt dịch vụ truyền file và gửi thư điện tử thông qua dịch vụ thông tin này. Việc cài đặt máy chủ IIS khá đơn giản thông qua tiện ích thêm chức năng của máy chủ từ chương trình “*Server Manager*” như trong hình sau.



Hình III-11. Cài đặt máy chủ IIS.

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



Hình III-12. Các tham số cài đặt trang chủ Web.

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

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

Để kiểm soát việc truy nhập tới các trang chủ Web, người quản trị có thể đặt hạn chế về địa chỉ mạng thông qua chức năng thiết lập luật hạn chế (*Add Allow Restriction Rule*) của máy chủ IIS. Mặt khác, có thể thiết lập các cơ chế xác thực để xác định người dùng được phép truy nhập vào trang web. Có một số cách thức như sau:

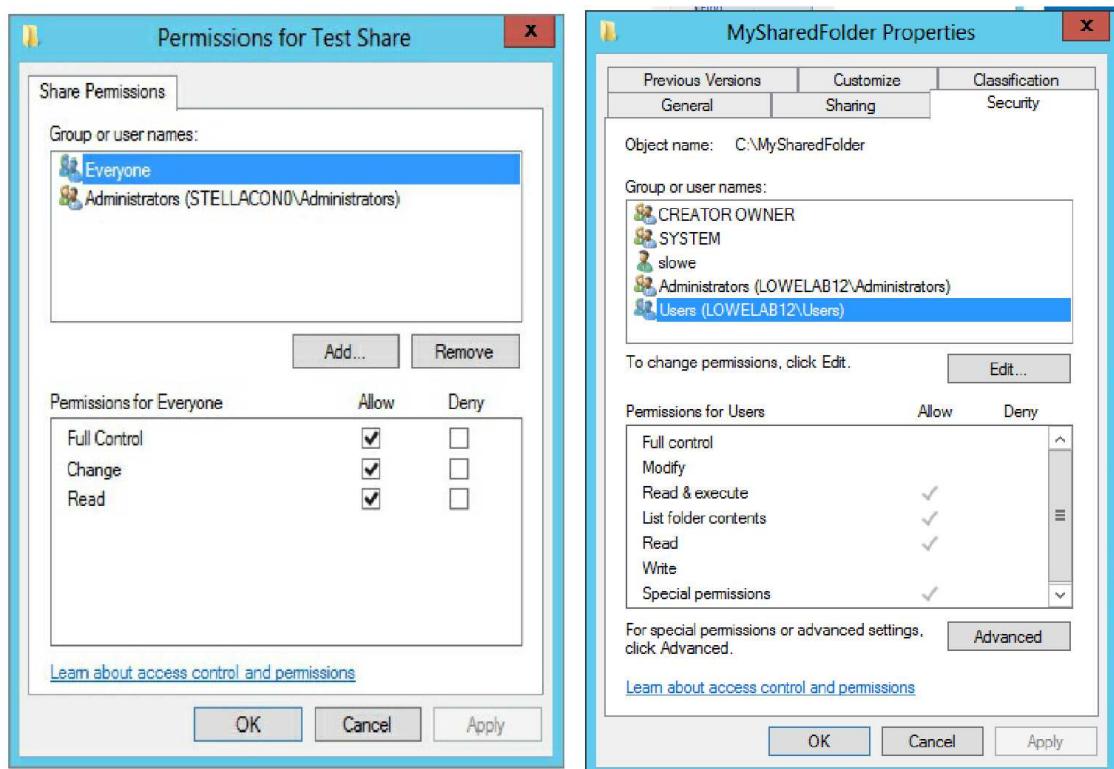
- Nặc danh (*Anonymous*): cho phép bất cứ người dùng nào cũng được truy nhập mà không cần xác thực.
- Xác thực cơ bản (*Basic Authentication*): yêu cầu người dùng cung cấp tên và mật khẩu hợp lệ. Tuy nhiên cách này không mã hóa thông tin nên chứa đựng rủi ro an toàn.
- Xác thực số (*Digest Authentication*): dùng máy chủ miền xác thực.
- Xác thực Windows (*Windows Authentication*): sử dụng giao thức NTLM hay Kerberos để xác thực.

III.4 Dịch vụ file và in ấn

III.4.1 Dịch vụ file.

Dịch vụ file cho phép người dùng lưu trữ và chia sẻ các dữ liệu, chương trình với người dùng khác trong mạng. Việc truy nhập thành công các file chia sẻ phải căn cứ vào quyền truy nhập mà người dùng có được. Trong môi trường Windows có thể áp dụng hai hình thức đảm bảo an ninh

- Quyền với thư mục chia sẻ. Hình thức này chỉ áp dụng với thư mục và các quyền của người dùng giới hạn: Đọc/Ghi/Sở hữu
- Đặt quyền file/thư mục sử dụng cách thức phân quyền NTFS để kiểm soát việc truy nhập. Hình thức này cho phép giám sát tốt hơn và các quyền chi tiết hơn.



Hình III-13. Quyền với thư mục chia sẻ (bên trái) và NTFS (bên phải).

Việc thực hiện chia sẻ file có thể được thực hiện trực tiếp từ trình duyệt file của Windows. Khi này hình thức chia sẻ là chia sẻ thư mục đòi hỏi người dùng phải có tài khoản và quyền phù hợp trên máy tính chia sẻ. Nói cách khác, người dùng và quyền chỉ có giá trị cục bộ trên máy tính chia sẻ.

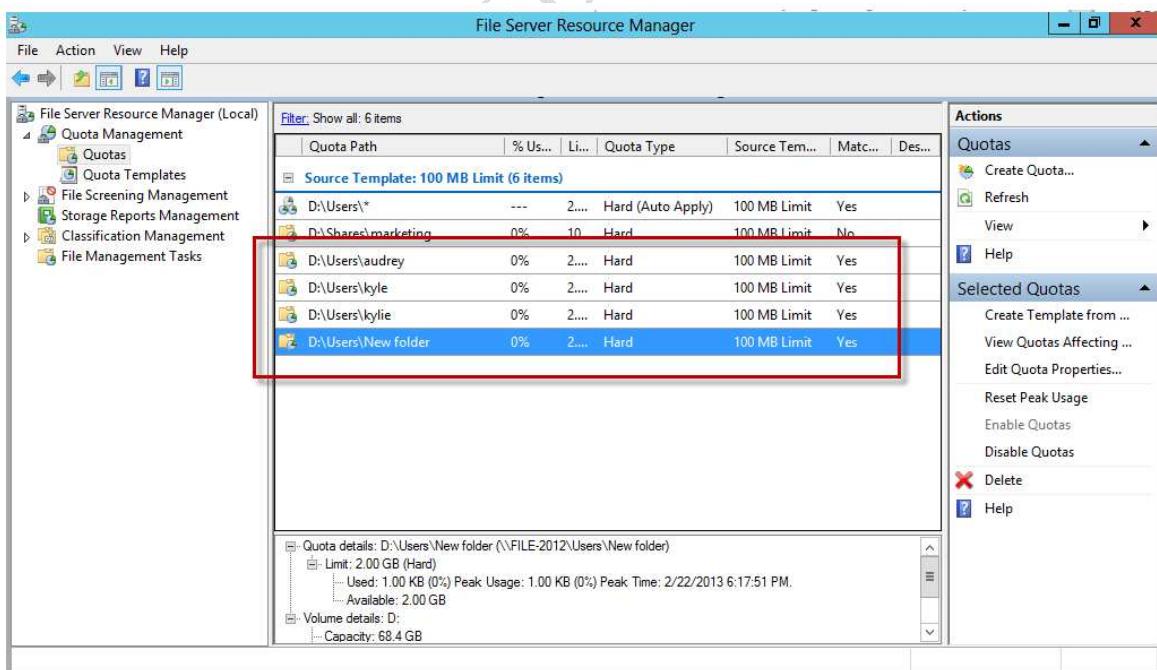
Khi thực hiện việc chia sẻ qua thư mục động thì hình thức kiểm soát truy nhập sử dụng cơ chế giống NTFS. Như vậy người dùng cần phải có tài khoản và quyền phù hợp trong thư mục động đó.

Để kiểm soát không gian lưu trữ, người quản trị có thể áp dụng giới hạn lưu trữ (*disk quotas*). Có một số cách để áp đặt giới hạn lưu trữ:

- Đặt giới hạn theo từng ổ đĩa. Cách này giới hạn toàn bộ không gian lưu trữ của ổ đĩa cho toàn bộ người dùng.
- Đặt giới hạn theo người dùng. Cách này cho phép đặt giới hạn trên từng ổ đĩa với từng người dùng.
- Tạo các mẫu giới hạn (*quota template*). Cho phép cài đặt giới hạn cho nhiều ổ đĩa trên cùng 1 vật lý mà không phải đặt giới hạn cho từng ổ đĩa riêng biệt.

Để kiểm soát và quản lý các khối lượng và các dạng dữ liệu lưu trên máy chủ, Microsoft cung cấp tiện ích quản lý tài nguyên máy chủ file (*File Server Resource Manager*) với các chức năng tiêu biểu:

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



Hình III-14. Giao diện quản trị giới hạn lưu trữ.

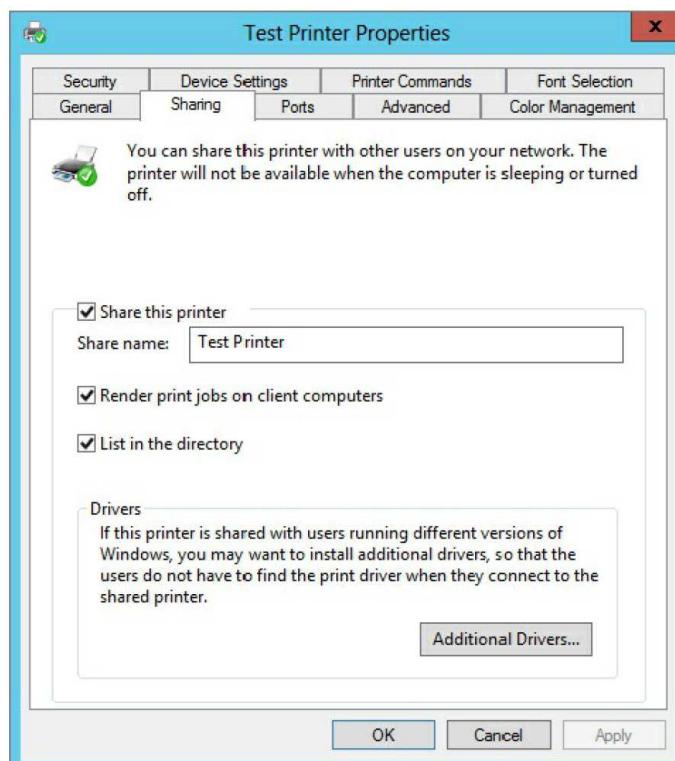
III.4.2 Dịch vụ in

Một trong những dịch vụ quan trọng trong mạng là in ấn. Các máy in mạng được kết nối trực tiếp với mạng hay thông qua máy tính cho phép người dùng trong mạng có thể sử dụng

các dịch vụ của máy in. Các máy chủ in ẩn là máy tính kết nối với máy in và làm nhiệm vụ xử lý các yêu cầu in ẩn từ các người dùng trong mạng. Windows phân biệt:

- Thiết bị in (máy in vật lý): kết nối trực tiếp với máy chủ
- Máy in (máy in lô-gíc): giao tiếp với máy in vật lý
- Trình điều khiển máy in: giúp giao tiếp với máy in và che dấu thông tin chi tiết về máy in.

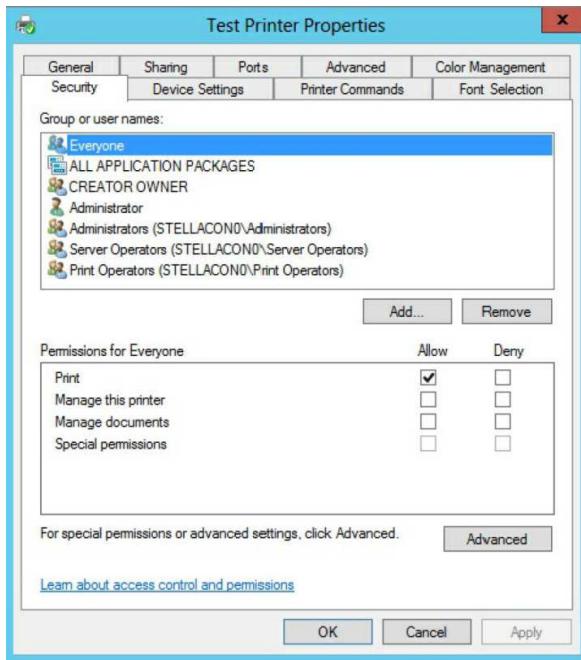
Để máy tính kết nối được với máy in cần có trình điều khiển thích hợp và để chia sẻ máy in vật lý cần cài đặt máy in phù hợp. Việc chia sẻ máy in có thể được thực hiện dễ dàng thông qua giao diện của Windows sau khi cài đặt thành công trình điều khiển.



Hình III-15. Chia sẻ máy in.

Các truy nhập của người dùng tới máy in chia sẻ chịu kiểm soát quyền truy nhập. Cụ thể các quyền như sau:

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



Hình III-16. Người dùng và quyền truy nhập máy in.

III.5 Dịch vụ truy nhập từ xa

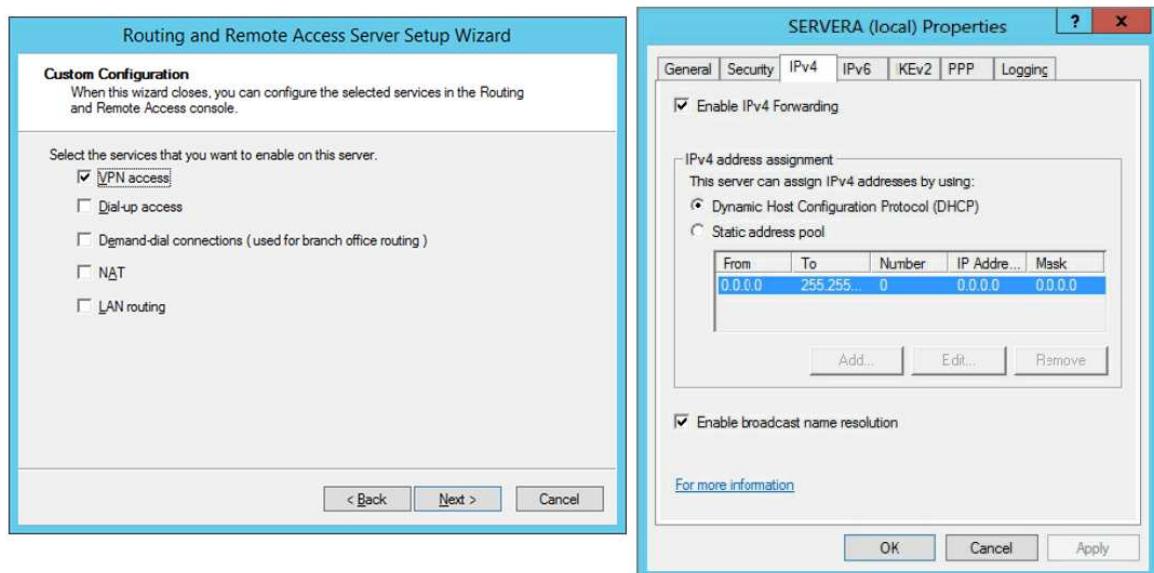
Dịch vụ truy nhập từ xa cho phép người dùng kết nối từ bên ngoài vào máy chủ dịch vụ bên trong để truy nhập dữ liệu và các ứng dụng như làm việc trên máy tính thông thường. Cùng với sự phát triển của các công nghệ truyền dữ liệu tốc độ cao dịch vụ truy nhập từ xa trở nên tiện dụng hơn.

Dịch vụ truy nhập từ xa thường sử dụng mạng riêng ảo VPN (*Virtual Private Networks*) hỗ trợ các giao thức:

- *Point-to-Point Tunneling Protocol (PPTP)*: Đơn giản khi triển khai song song bảo mật yếu
- *Layer 2 Tunneling Protocol (L2TP)*: Dùng chuẩn IPSec.
- *Secure Socket Tunneling Protocol (SSTP)*: dùng giao thức http bảo mật

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

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



Hình III-17. Lựa chọn cài đặt VPN(trái) và cấu hình VPN qua kết nối IPv4.

Để sử dụng VPN, bên phía người dùng thực hiện việc cấu hình kết nối thông qua tiện ích quản trị kết nối mạng.

Ngoài việc sử dụng VPN để truy nhập vào các dịch vụ mà máy chủ cung cấp, người quản trị có thể sử dụng dịch vụ có kết quả tương tự đó là dịch vụ màn hình làm việc từ xa (*Remote Desktop Connections*). Dịch vụ này có số lượng kết nối rất hạn chế so với dịch vụ VPN.

Trong bản Server 2012, dịch vụ này có thể được thay thế bởi dịch vụ truy nhập trực tiếp (*DirectAccess*). Bên phía người dùng không cần thiết phải khởi tạo kết nối VPN để truy nhập vào các tài nguyên của miền. Để sử dụng dịch vụ này, máy tính của người dùng cần cài đặt bản Windows 7 Ultimate trở lên.

Chương IV. BẢO TRÌ, KHẮC PHỤC LỖI VÀ GIÁM SÁT HOẠT ĐỘNG CỦA WINDOWS

Việc đảm bảo hệ thống vận hành một cách ổn định và an toàn luôn là vấn đề đặc biệt quan trọng. Chương này giới thiệu các chức năng cập nhật của Windows và một số cách thức giúp tự động thực hiện việc cập nhật. Bên cạnh đó, các chức năng sao lưu và khôi phục hệ điều hành Windows cũng được giới thiệu cho sinh viên. Cuối chương mô tả cách thức xử lý căn bản giúp cho việc phát hiện và khắc phục các tình huống sự cố trong quá trình vận hành hệ thống Windows.

IV.1 Cập nhật các bản vá Windows

Windows là hệ thống phức tạp với rất nhiều bộ phận khác nhau. Để đảm bảo Windows hoạt động tin cậy và an toàn, người quản trị cần phải kiểm tra xem Microsoft có đưa ra bất kỳ các cập nhật cho Windows nào hay không bao gồm các bản sửa lỗi, gói dịch vụ, hay trình điều khiển. Khi có bản cập nhật, người quản trị cần cài đặt các bản cập nhật này sớm nhất có thể.

Một cách để đảm bảo việc cập nhật được kịp thời là sử dụng tiện ích “*Windows Update*”. Chương trình này sẽ quét hệ thống để xác định các bản cập nhật và sửa lỗi cần thiết. Microsoft phân loại các bản cập nhật thành ba loại: quan trọng, khuyến nghị, và tùy chọn. Giao diện của chương trình này như trong hình dưới đây.



Hình IV-1. Cài đặt chương trình cập nhật Windows.

Bản cập nhật quan trọng mang lại những lợi ích đáng kể với hệ thống như cải thiện an toàn, bảo mật, và độ tin cậy. Những bản cập nhật này cần được cài đặt ngay lập tức và việc

cài đặt có thể được thực thi một cách tự động. Các bản cập nhật khuyến nghị xử lý những vấn đề không nghiêm trọng hay giúp cải thiện trải nghiệm của hệ thống. Cho dù bản cập nhật loại này không nhằm loại trừ các lỗi nghiêm trọng song chúng có thể cải thiện hiệu năng hệ thống một cách tương đối. Các bản cập nhật tùy chọn có thể là các trình điều khiển hay phần mềm mới nhằm cải thiện các trải nghiệm của hệ thống.

Tùy thuộc vào kiểu cập nhật, Microsoft có thể phân chia thêm thành các loại như sau:

- *Cập nhật an ninh*: là bản cập nhật nhằm vào một sản phẩm/bộ phận cụ thể để vá các lỗ hổng an ninh. Nguy cơ tồn thương về an ninh được đánh giá dựa trên mức độ nghiêm trọng của chúng và được chia thành: nghiêm trọng, quan trọng, vừa phải, và thấp.
- *Cập nhật rất quan trọng*: là bản vá lỗi cho vấn đề cụ thể như các lỗi nghiêm trọng hay các lỗi không liên quan đến an ninh.
- *Gói dịch vụ*: là tập các bản cập nhật đã được kiểm tra.

Với hệ thống nhỏ việc sử dụng tính năng tự động cập nhật rất hữu ích và giúp tiết kiệm thời gian. Khi này chương trình cập nhật chạy ở chế độ nền không ảnh hưởng đáng kể đến các chương trình khác.

Trong mạng lớn có hàng trăm máy tính thì chương trình *Windows Update* không phù hợp. Khi này, cần sử dụng dịch vụ cập nhật máy chủ Windows WSUS (*Windows Server Update Services*). Dịch vụ này cho phép người quản trị quản lý việc phân phối các bản cập nhật và các bản vá lỗi tới các máy tính trong miền quản lý. WSUS tải về các bản cập nhật từ Microsoft hay từ các máy chủ WSUS khác.

IV.2 Sao lưu và khôi phục dự phòng

Sao lưu và khôi phục là các hoạt động tối quan trọng đảm bảo việc vận hành hệ thống được an toàn và tin cậy. Về cơ bản, sao lưu (*back-up*) là tạo các bản sao của dữ liệu để có thể khôi phục (*restore*) dữ liệu gốc trong tình huống lỗi.

Mặc dù, mục đích của việc sao lưu là rất rõ ràng song người quản trị cần phải đánh giá nhiều lựa chọn để xác định cách sao lưu/khôi phục phù hợp với máy tính chịu sự quản trị của mình. Các dữ liệu sao lưu có thể được lưu trữ trên nhiều phương tiện khác nhau như ổ đĩa cứng, ổ đĩa quang, hay băng từ. Băng từ đã từng là phương tiện sao lưu phổ biến nhờ có khả năng lưu trữ khối lượng lớn dữ liệu và chi phí thấp song tốc độ truy nhập chậm. Ổ đĩa quang mặc phái vấn đề suy giảm chất lượng lưu trữ theo thời gian. Ổ cứng trở thành phương tiện sao lưu phổ biến do chi phí giảm, tốc độ truy nhập cao. Trên thực tế thường sử dụng ở dạng ổ đĩa kết nối qua mạng nhằm nâng cao dung lượng và độ an toàn.

Việc sao lưu toàn bộ hệ thống là hoàn toàn có thể làm được song người quản trị cần cân nhắc giữa các lần sao lưu sao cho phù hợp. Người quản trị có thể phân biệt loại file cần được sao lưu như chương trình và dữ liệu. Trên cơ sở đó áp dụng các chính sách sao lưu và lựa chọn phương tiện sao lưu.

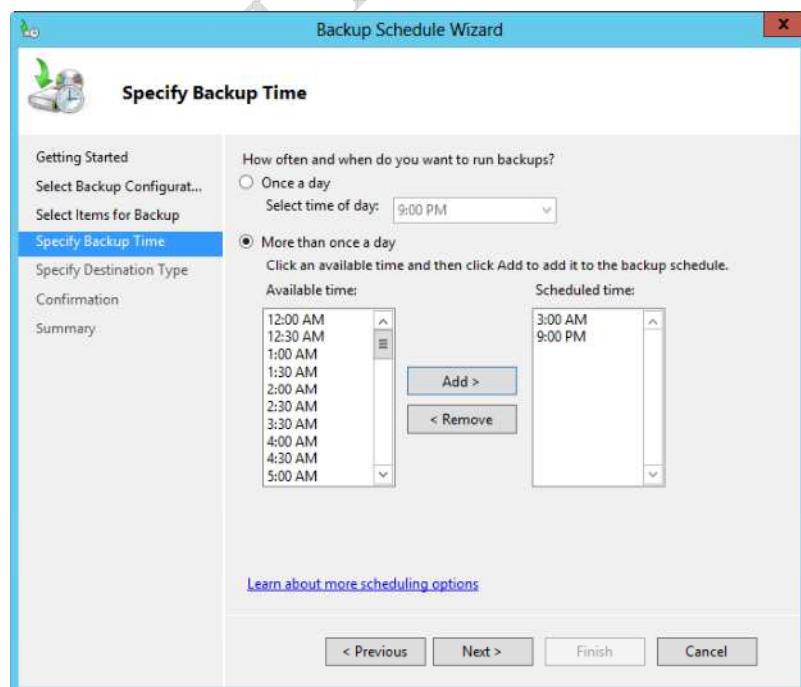
Mặt khác người quản trị có thể lựa chọn các phương pháp như sau để thực hiện việc sao lưu:

- *Trực tuyến*: Dùng đĩa cứng hoặc chuỗi đĩa cứng có thể khôi phục ngay lập tức. Phương pháp này đòi hỏi chi phí cao vì toàn bộ dữ liệu được sao lưu đồng thời với quá trình chạy của hệ thống.
- *Cận trực tuyến*: thường dùng băng từ, thời gian khôi phục lâu hơn
- *Không trực tuyến*: cần thao tác của người quản trị để thực hiện sao lưu. Cách này mất nhiều thời gian cho việc sao lưu và khôi phục
- *Sao lưu toàn bộ/sao lưu phòng thảm họa*: sao lưu toàn bộ hệ thống phòng sự cố có thể chuyển sang vị trí khác để hoạt động. Thực chất, cách này đòi hỏi không chỉ dự phòng về dữ liệu mà cả về thiết bị.

Khi thực hiện các thao tác sao lưu người quản trị có thể áp dụng các chính sách lưu sau đây:

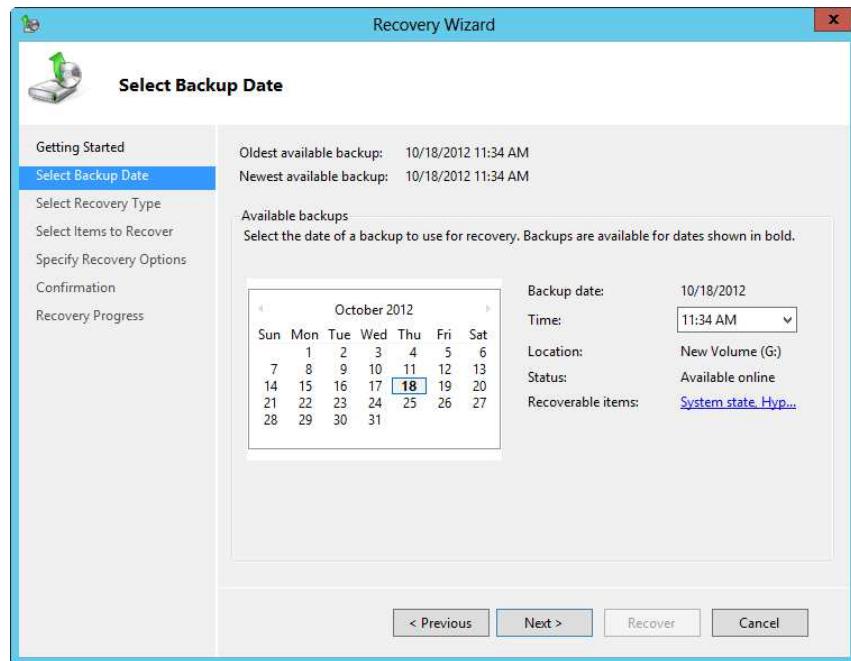
- *Sao lưu toàn bộ*: Tạo bản sao toàn bộ file và dữ liệu
- *Sao lưu tăng dần*: Sao lưu toàn bộ tiếp theo là sao lưu tăng dần
- *Sao lưu khác biệt*: Sao lưu toàn bộ tiếp theo là sao lưu các file và dữ liệu khác biệt.

Để thuận tiện cho việc quản trị, Microsoft cung cấp chương trình sao lưu và khôi phục “Windows Server Backup”. Chương trình cho phép người quản trị lựa chọn các chính sách, loại file cũng như phương tiện sao lưu khác nhau. Việc sao lưu có thể được tiến hành theo lịch của người quản trị.



Hình IV-2. Cấu hình thời gian thực hiện sao lưu.

Người quản trị có thể chọn việc khôi phục được thực hiện căn cứ vào dữ liệu được sao lưu như trong hình sau:



Hình IV-3. Chọn dữ liệu sao lưu theo ngày để khôi phục.

Ngoài ra tùy thuộc vào cách sao lưu mà người quản trị có thể lựa chọn việc khôi phục toàn bộ hệ thống hay một phần trạng thái của hệ thống. Cách này thường áp dụng khi hệ thống hoạt động không tin cậy do cài đặt các bản cập nhật không tương thích hoàn toàn với hệ thống đang chạy.

IV.3 Khắc phục các sự cố trong Windows

Có hai cách tiếp cận khi xử lý lỗi và thực tế thì cả hai cách này bổ trợ cho nhau:

- *Kinh nghiệm* : Xử lý vấn đề cụ thể đã gặp từ trước. Thông thường cách này dựa vào việc nhận biết các triệu chứng lỗi hay các thông báo lỗi.
- *Hệ thống*: nhằm xử lý triệt để vấn đề và giảm thiểu việc dự đoán nguyên nhân.

Để xác định và xử lý triệt để lỗi trong quá trình vận hành hệ thống, người quản trị có thể áp dụng các bước như sau:

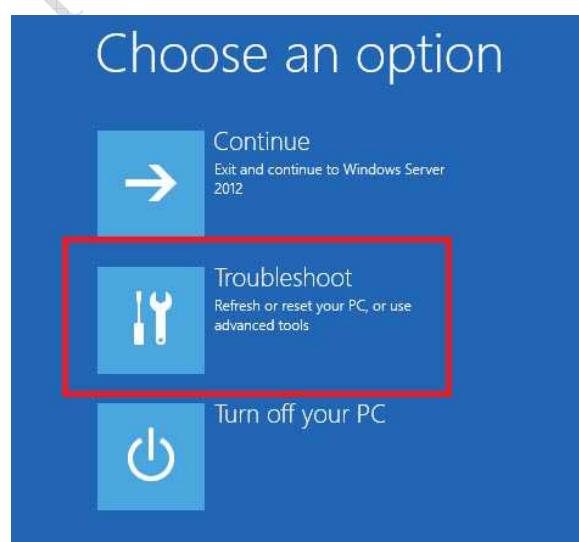
1. *Tìm ra vấn đề*: xác định và ghi lại các triệu chứng của sự cố và tìm trong thư viện kỹ thuật như “Microsoft Knowledge Base” hay cộng đồng trên mạng
2. *Dánh giá cấu hình hệ thống*: tìm hiểu các thay đổi cấu hình (kiểm tra trong *Event viewer*) diễn ra trong khoảng thời điểm xảy ra sự cố. Ngoài ra, liệt kê hay theo dõi các giải pháp có thể và cố gắng cách ly vấn đề bằng cách loại trừ phần cứng và phần mềm bằng cách chạy phần mềm kiểm tra đánh giá hoặc theo dõi file nhật ký.

3. *Thực hiện kế hoạch*: thử các giải pháp tiềm năng và có kế hoạch với sự việc bất ngờ đặc biệt khi giải pháp không có tác dụng hay ảnh hưởng tiêu cực đến hệ thống.
4. *Kiểm tra kết quả*: nếu vấn đề vẫn tồn tại thì thực hiện lại các bước trên
5. *Chủ động*: luôn ghi chú lại các thay đổi thực hiện trong khi xử lý sự cố. Việc này đặc biệt hữu ích trong tình huống giải pháp dự kiến không giải quyết được sự cố.

Windows đi kèm với nhiều công cụ trợ giúp cho việc theo dõi trạng thái hoạt động của hệ thống như:

- System Information
- Event Viewer
- Task Manager
- Resource Monitor
- Performance Monitor
- System Configuration
- Memory Diagnostics tool

Microsoft cung cấp “*Recovery Console*” để giúp người quản trị xử lý trường hợp hệ thống không khởi động được. Chương trình *Recovery console* có thể được sử dụng qua giao diện dòng lệnh hoặc đồ họa. Với giao diện tối thiểu, chương trình này cho phép người quản trị thực hiện một số thao tác sửa lỗi cơ bản như loại bỏ các cấu hình tiềm ẩn lỗi, chạy hệ thống ở chế độ cấu hình tối thiểu (*safe mode*). Bên cạnh đó, chương trình này cung cấp một số lệnh như kiểm tra ổ đĩa *chkdsk*, tắt hay cho phép dịch vụ chạy qua câu lệnh *enable/disable*, sửa phân vùng khởi động *fixboot*, liệt kê các dịch vụ và trình điều khiển có trong máy tính *listsvc...*



Hình IV-4. Lựa chọn sửa lỗi.

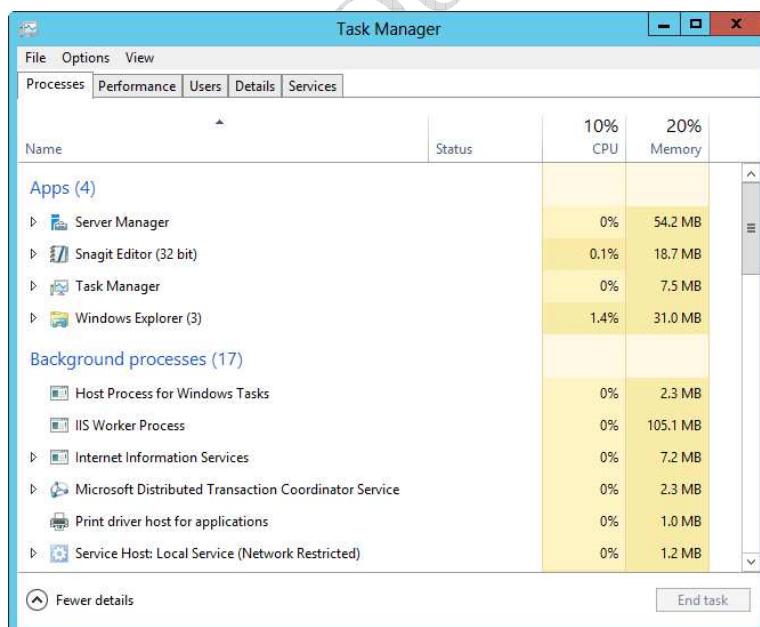
IV.4 Giám sát hoạt động và kiểm toán Windows

Giám sát và tinh chỉnh hiệu năng là quá trình theo dõi việc vận hành của hệ thống để xác lập tiêu chuẩn cơ sở, xác định và xử lý vấn đề tiềm năng. Microsoft cung cấp một số công cụ cho người quản trị theo dõi hiệu năng và việc sử dụng tài nguyên hệ thống như giám sát hiệu năng (*Performance Monitor*), quản lý công việc (*Task Manager*), giám sát tài nguyên (*Resource Monitor*), và xem bản ghi sự kiện (*Event Viewer*).

IV.4.1 Chương trình quản lý nhiệm vụ

Chương trình quản lý nhiệm vụ theo dõi thông tin tổng thể về hiệu năng, các ứng dụng và tiến trình đang chạy, danh sách người dùng đăng nhập vào hệ thống. Như vậy, người quản trị có thể xác định được tình trạng chung của hệ thống. Về chức năng, chương trình cung cấp các thông tin như sau:

- Mục ứng dụng: cho biết danh sách ứng dụng đang chạy và trạng thái tương ứng.
- Tiến trình: các tiến trình của người dùng đang chạy trong hệ thống.
- Dịch vụ: các dịch vụ Windows đang chạy.
- Hiệu năng: theo dõi việc sử dụng các tài nguyên phần cứng như bộ xử lý, bộ nhớ, ổ đĩa.
- Kết nối mạng: giám sát các giao tiếp mạng được cài đặt và việc sử dụng chung.
- Người dùng: thông tin về người dùng đăng nhập vào hệ thống.



Hình IV-5. Chương trình quản lý nhiệm vụ.

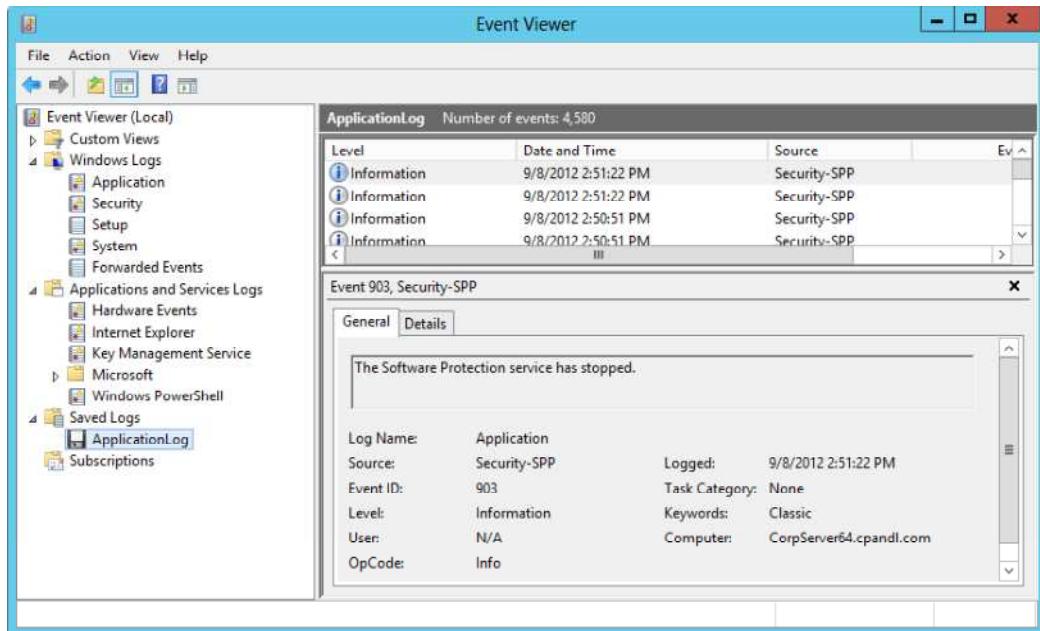
Không những vậy, chương trình quản lý công việc còn cho phép tương tác với các chương trình đang chạy hay người dùng đăng nhập vào hệ thống như chấm dứt chương trình hay loại bỏ người dùng ra khỏi hệ thống đang chạy.

IV.4.2 Nhật ký Windows

Hệ điều hành Windows định nghĩa sự kiện là bất cứ điều gì đáng kể xảy ra khi vận hành hệ điều hành hay ứng dụng. Các sự kiện này cần được lưu lại phục vụ mục đích theo dõi. Các thông tin có được theo dõi như cảnh báo, các lỗi, hay các sự kiện kiểm toán.

Có hai kiểu file nhật ký sự kiện là:

- Nhật ký Windows: lưu lại các sự kiện hệ thống nói chung liên quan đến ứng dụng, an ninh, cài đặt và các thành phần hệ thống;
- Nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng hay dịch vụ cụ thể.



Hình IV-6. Chương trình xem các sự kiện được lưu lại.

Để xem nhật ký sự kiện, người quản trị sử dụng chương trình “Event Viewer” như trong hình trên. Với mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau:

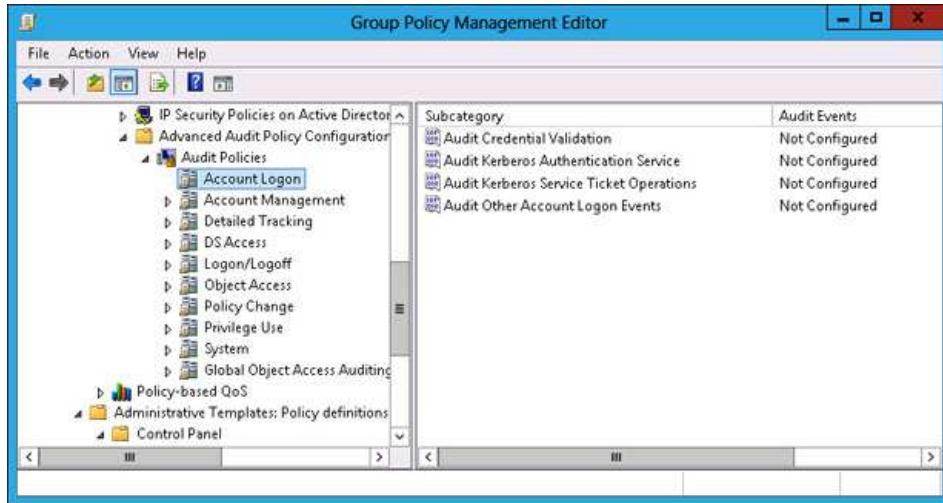
- *Thông tin*: Thông báo thông thường về thao tác được thực hiện thành công.
- *Cảnh báo*: Mô tả sự kiện không nghiêm trọng nhưng cần chú ý để tránh các vấn đề xa hơn.
- *Lỗi*: Cho biết một lỗi hay vấn đề không nghiêm trọng xảy ra.
- *Nghiêm trọng*: Cho thấy một lỗi nghiêm trọng hay vấn đề rất đáng kể xảy ra.
- *Kiểm toán thành công*: Mô tả sự kiện kiểm toán an ninh thành công như yêu cầu.
- *Kiểm toán thất bại*: Mô tả sự kiện kiểm toán an ninh không thành công như yêu cầu.

IV.4.3 Kiểm toán

Việc kiểm toán cho phép người quản trị theo dõi cả truy nhập thực tế và cố thử truy nhập hay các sửa đổi các đối tượng và chính sách của hệ thống. Các đối tượng có thể là thư mục và file cũng như các đối tượng an ninh của hệ thống. Cách chính sách kiểm toán hỗ trợ việc đảm

bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần để ý.

Có hai tập chính sách kiểm toán trong một đối tượng chính sách nhóm GPO: chính sách kiểm toán truyền thống và nâng cao. Chính sách truyền thống có từ bản Server 2000. Chính sách này có nhược điểm là chúng không đủ cụ thể và khó cấu hình. Chính sách nâng cao khắc phục nhược điểm này và cung cấp 10 nhóm cài đặt với 58 chính sách kiểm toán riêng lẻ.



Hình IV-7. Chính sách kiểm toán nâng cao.

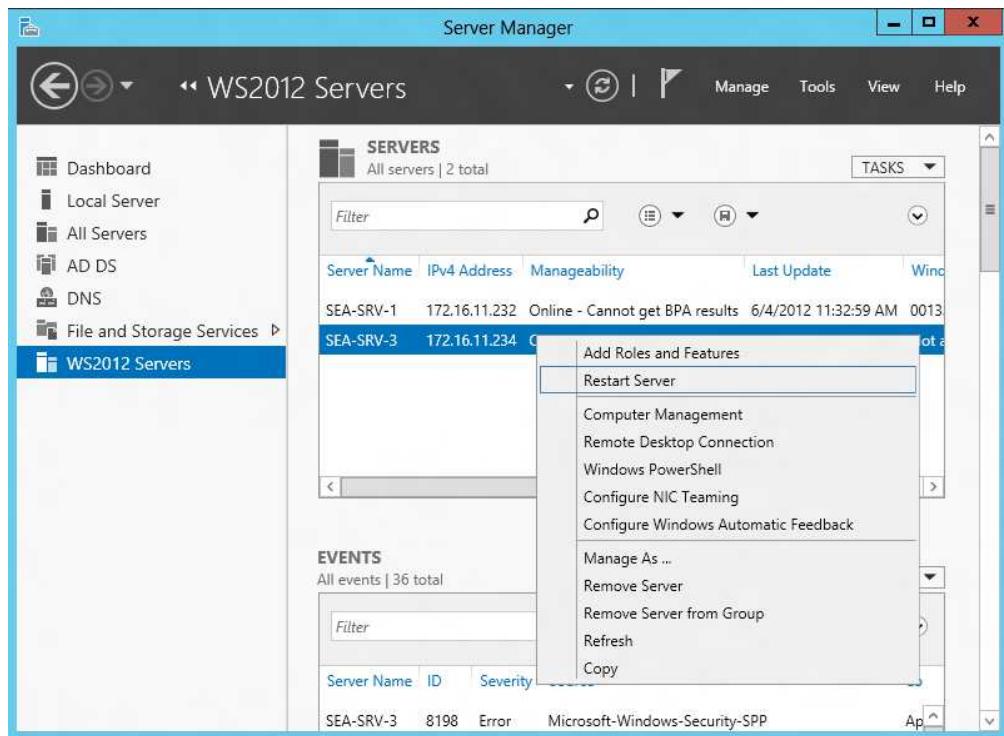
Các nhóm chính sách tiêu biểu bao gồm:

- *Đăng nhập*: theo dõi việc xác thực thông tin đăng nhập
- *Quản lý tài khoản*: theo dõi các thao tác thay đổi tài khoản như người dùng, máy tính...
- *Theo dõi chi tiết*: theo dõi việc chạy chương trình, các lời gọi hàm từ xa...
- *Truy nhập thư mục động*: theo dõi việc truy nhập hay các chức năng của thư mục động.
- *Truy nhập đối tượng*: theo dõi việc truy nhập các file, thư mục hay ứng dụng.

IV.5 Giới thiệu các công cụ quản trị Windows từ xa

Để quản trị Windows từ xa, người quản trị có thể sử dụng các dịch vụ màn hình làm việc từ xa (*Remote Desktop Services*) cho phép sử dụng ứng dụng và dữ liệu trên máy tính ở xa.

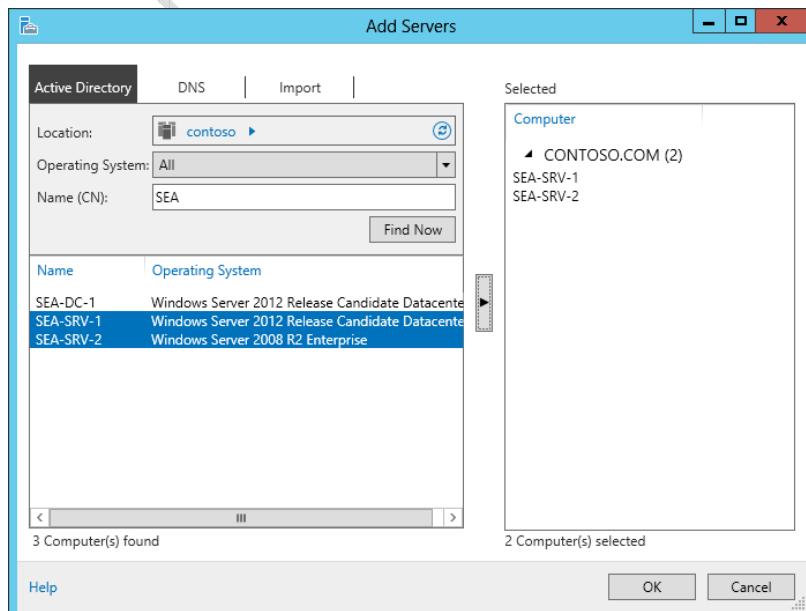
Với bản Server 2012, người quản trị có thể truy nhập máy chủ Windows cục bộ hay ở xa trực tiếp thông qua chương trình “*Server Manager*”. Khi này các máy tính được quản lý trông giống như các file bên trong thư mục (Hình IV-8). Người quản trị tương tác với các máy chủ thông qua giao diện tiêu chuẩn của Windows.



Hình IV-8. Danh sách các máy chủ được quản trị từ giao diện.

Thông qua giao diện, người quản trị có thể truy nhập tới các chức năng cài đặt cấu hình hay quản trị máy chủ như trên máy cục bộ. Điều này giúp đơn giản hóa và thuận tiện cho việc quản trị.

Ngầm định, bản Server 2012 được cấu hình để cho phép chức năng quản trị từ xa. Bản Server 2008 cũng có thể được quản trị từ xa qua “Server Manager” tuy nhiên với bản Server 2003 thì bị hạn chế. Trên bản Server 2012, người quản trị có thể dùng câu lệnh *Configure-SMRemoting* để cho phép hay cấm tính năng quản trị từ xa.



Hình IV-9. Thêm máy chủ để quản trị.

Để quản trị các máy chủ trong hệ thống, người quản trị cần thực hiện các thao tác thêm máy chủ để quản lý từ chức năng “*Add server*” của chương trình “*Server Manager*” như trong hình sau. Sau khi có được các máy chủ cần quản lý, người quản trị có thể thực hiện các thao tác như tập hợp các sự kiện, theo dõi các dịch vụ và hiệu năng từ các máy được quản lý một cách thuận tiện và dễ dàng.

PTIT.EDU.VN

Phần II - Quản trị hệ điều hành Linux/Unix

Phần II giới thiệu lịch sử phát triển của hệ điều hành Unix, một trong những hệ điều hành lâu đời nhất, và nguồn gốc, quá trình phát triển của hệ điều hành Linux. Cũng giống như phần đầu, mở đầu phần II trình bày các khái niệm và kiến trúc cơ bản của hệ điều hành Unix/Linux và các chức năng căn bản của hệ điều hành này. Chương kế tiếp trình bày các yêu cầu phần cứng tối thiểu và nên có khi cài đặt hệ điều hành và cách thức quản trị máy tính như các trình điều khiển, hệ thống lưu trữ cũng như các dịch vụ tiêu biểu. Chương thứ 3 của phần này tập trung vào việc cài đặt và quản lý các dịch vụ máy chủ bao gồm tên miền, cấu hình máy tính tự động và các dịch vụ chia sẻ tài nguyên mạng Internet khác như thư điện tử, file và in ấn.

Chương cuối cùng trình bày các cách thức giúp cho việc vận hành Linux/Unix được ổn định và an toàn hơn qua các chức năng cập nhật, sao lưu và khôi phục hệ thống. Ngoài ra, sinh viên cũng làm quen với một số công cụ trợ giúp việc giám sát, quản trị và khắc phục sự cố. Cuối chương giới thiệu các chức năng ngôn ngữ căn bản của việc lập trình *shell*.

Chương V. GIỚI THIỆU CÁC HỆ ĐIỀU HÀNH LINUX/UNIX

Chương này giới thiệu lịch sử phát triển của hệ điều hành lâu đời nhất, Unix, và sự ra đời của Linux cũng như các biến thể của nó. Chương này cũng giới thiệu kiến trúc và các bộ phận căn bản của hệ điều hành bao gồm cách thức tương tác với người dùng, hệ thống file và các phiên bản của hệ điều hành.

V.1 Lịch sử phát triển

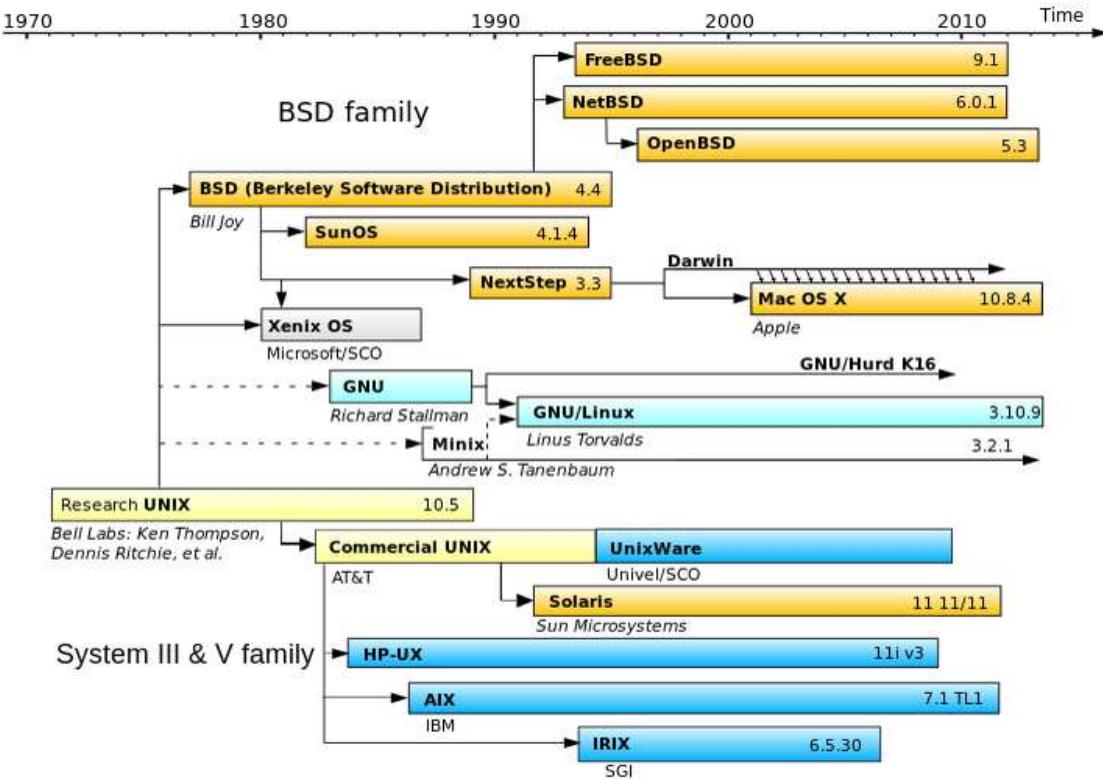
Unix là họ hệ điều hành máy tính hỗ trợ đa nhiệm và đa người dùng phát triển từ phiên bản Unix của AT&T từ những năm 1970. Một số đặc tính quan trọng của UNIX vẫn còn được tiếp tục duy trì đến ngày nay:

- Mỗi một chương trình chỉ làm một nhiệm vụ thật tốt
- Đầu ra của mỗi chương trình có thể là đầu vào cho chương trình khác
- Viết các nhân nhỏ nhất có thể được

Hệ điều hành UNIX nhanh chóng phổ biến bên trong công ty AT&T và được sử dụng trong các máy tính cỡ nhỏ. Việc công ty AT&T cấp phép sử dụng UNIX dẫn đến sự ra đời các biến thể thương mại cũng như sử dụng trong môi trường học thuật. Các mốc thời gian quan trọng của các phiên bản được thể hiện trong Hình V-1 dưới đây.

Trung tâm Berkeley của Trường Đại học Tổng hợp California phát triển biến thể Unix gọi là BSD (*Berkeley Software Distribution*) đóng vai trò nền tảng quan trọng cho việc phát triển các biến thể sử dụng trong môi trường học thuật. Trong khi đó công ty AT&T tiếp tục phát triển UNIX dưới tên gọi *System III* và sau này là *System V*.

Hệ điều hành UNIX sử dụng thiết kế mô-đun với các phần mềm chức năng được xây dựng đơn giản và rõ ràng do vậy Unix dễ dàng phát triển và mở rộng. Một điểm quan trọng của UNIX là được viết bằng ngôn ngữ lập trình C nên dễ dàng chuyển đổi nền tảng hay phần cứng khác nhau. Người dùng chỉ cần thực hiện việc biên dịch là phần mềm là có thể sử dụng được trên hệ thống mới. UNIX được sử dụng trên nhiều hệ thống/nền tảng khác nhau như máy chủ, máy trạm và thiết bị di động.



Hình V-1. Mốc thời gian của các phiên bản UNIX và LINUX.

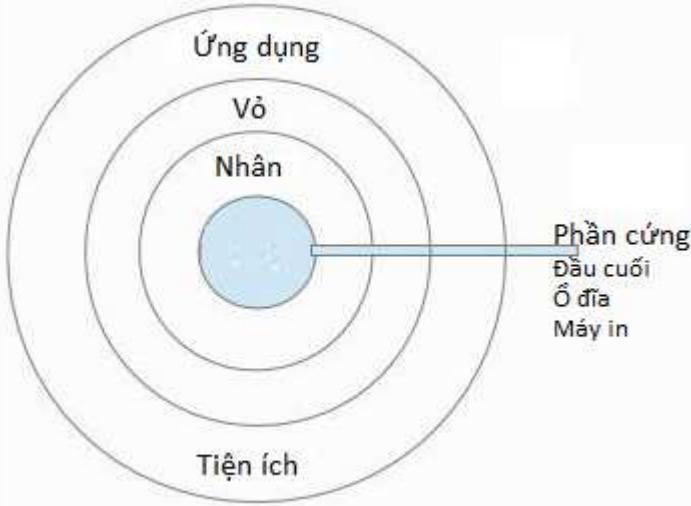
Vào năm 1984 Richard Stallman khởi xướng Hội Phần mềm miễn phí FSF (*Free Software Foundation*) và khởi động dự án GNU để tạo ra phiên bản miễn phí của hệ điều hành UNIX. Mục tiêu của FSF là cho phép các phần mềm có thể được phân phối, sử dụng, đọc và sửa chữa mà không phải trả bất kỳ chi phí nào. FSF đã sử dụng thành công khói lượng khổng lồ các phần mềm quan trọng như trình biên dịch gcc, phần mềm soạn thảo Emacs...

Linux là hệ điều hành mã nguồn mở cho PC được phát triển vào năm 1991 bởi Linus Torvalds. Nhân Linux mở cho mọi người có thể sửa đổi, cải tiến tính năng và có thể được tích hợp với các phần mềm FSF khác. Chính vì vậy Linux trở nên phổ biến và dễ dàng sửa đổi. Trong cộng đồng LINUX, các tổ chức khác nhau sử dụng các cách kết hợp các thành phần phần mềm khác nhau để tạo ra các phiên bản khác nhau vì vậy các phiên bản này còn được gọi là các bản phân phối (*distribution*) như RedHat, Slackware, Debian và Mandrake.

V.2 Kiến trúc của hệ điều hành

Về cơ bản kiến trúc của hệ điều hành LINUX/UNIX bao gồm các bộ phận chính như sau:

- **Nhân:** là phần cốt lõi của hệ điều hành chịu trách nhiệm tương tác trực tiếp với phần cứng và đảm bảo cho hầu hết các hoạt động của hệ thống. Phần nhân chứa các chương trình quản lý bộ nhớ, CPU, quản lý file và các trình điều khiển thiết bị.



Hình V-2. Kiến trúc cơ bản LINUX/UNIX

- *Vỏ* : Giao tiếp với phần nhân và nhận câu lệnh từ người dùng. Có thể coi vỏ là chương trình thông dịch đặc biệt dùng để thực thi các câu lệnh của hệ điều hành như gọi các chương trình. Một số dạng vỏ như:
 - sh (*Bourne shell*): vỏ nguyên thủy của UNIX
 - bash (*Bourne again shell*): vỏ mặc định của LINUX
 - csh (*C shell*): rất giống với ngôn ngữ C dùng phổ biến trên dòng BSD.
- *Giao diện đồ họa*: được chạy ở mức ứng dụng và phát triển dựa trên hệ thống “*X Window*”. Các giao diện quản lý giao diện đồ họa phổ biến như CDE (*Common Desktop Environment*), KDE (*K Desktop Environment*) hay GNOME. Các giao diện quản lý cho phép người dùng tương tác một cách với hệ thống thông qua các thiết bị giao tiếp như chuột, bàn phím, âm thanh.
- *Dịch vụ hệ thống*: cung cấp các chương trình chạy ở chế độ nền hay câu lệnh hệ thống trợ giúp người dùng như dịch vụ truy nhập từ xa, quản trị máy tính
- *Ứng dụng người dùng*: là các chương trình chạy theo yêu cầu của người dùng như trình biên dịch gcc, bộ ứng dụng văn phòng Star office.

LINUX được phát triển như là một hệ thống miễn phí thay thế cho hệ thống thương mại của UNIX. LINUX hoạt động được trên nhiều phần cứng khác nhau trong khi hầu hết các phiên bản UNIX chỉ hoạt động trên một hạ tầng phần cứng duy nhất. Do lịch sử phát triển, LINUX và UNIX có nền tảng chung song cũng rất khác nhau. Rất nhiều công cụ, tiện ích tiêu chuẩn trong LINUX thực sự được phát triển từ các sản phẩm tương tự trong UNIX.

V.3 Giao diện của Linux/Unix

Người dùng làm việc với LINUX/UNIX thông qua giao diện dòng lệnh (*Command Line Interface - CLI*) hoặc giao diện đồ họa. Giao diện CLI được cung cấp thông qua lớp vỏ với

khả năng tùy biến và tự động hóa thực thi các câu lệnh (*lập trình*) thuận tiện. Với những công việc đơn giản như chạy chương trình hay quản lý file thì giao diện đồ họa đơn giản và thuận tiện hơn với người dùng mới. Song giao diện đồ họa yêu cầu phần cứng cao hơn và chạy chậm hơn so với giao diện dòng lệnh.

V.3.1 Vỏ

Vỏ được kích hoạt thông qua chương trình đặc biệt gọi là đầu cuối (*terminal*). Thông thường, người dùng có thể cài đặt vỏ ngầm định từ hồ sơ đăng nhập hay kích hoạt vỏ từ dấu nhắc của chương trình đầu cuối như lệnh *sh* cho vỏ nguyên thủy của UNIX hay lệnh *bash* cho “*Bourne shell*”. Về cơ bản, các vỏ cung cấp các chức năng tương tự nhau dù cú pháp có thể khác đôi chút. Hiện nay, 2 loại vỏ dùng phổ biến hơn cả là *tsch* và *bash*.

Một số câu lệnh tiêu biểu có thể sử dụng với giao diện dòng lệnh:

- *ls*: liệt kê thư mục
- *mkdir* tạo thư mục
- *cp*: chép file
- *rm*: xóa file
- *mv*: chuyển file
- *vi*: trình soạn thảo
- *cd*: chuyển thư mục
- *man*: trợ giúp
- *passwd*: đổi mật khẩu
- *mount*: cài đặt ổ đĩa vào cây thư mục
- *umount*: gỡ cài đặt ổ đĩa khỏi cây thư mục
- *top*: liệt kê các chương trình đang chạy
- *init 3*: chế độ khởi động

Khi nhập câu lệnh qua giao diện dòng lệnh, người dùng có thể sử dụng các ký tự đặc biệt như chuyển hướng vào/ra với dữ liệu của chương trình như “>,<, |” hay “?,*” để đại diện cho các ký tự người dùng muốn so sánh.

Ví dụ để liệt kê tất các file có đuôi *.doc* trong thư mục hiện thời và lưu kết quả vào file khác có thể được thực hiện qua câu lệnh *ls *.doc > kq.txt*.

V.3.2 Giao diện đồ họa

Hệ thống “*X Window*” cung cấp các chức năng đồ họa cơ sở cho các hệ thống LINUX/UNIX hiện đại. *X Window* được xây dựng dựa trên kiến trúc chủ/khách và có thể hoạt động trên nhiều nền tảng khác nhau. Việc cung cấp giao diện đồ họa cho phép người dùng tương tác với hệ thống cần có các chương trình quản lý giao diện. Các giao diện đồ họa có thể được cài đặt sau khi người dùng cài đặt thành công hệ điều hành. Người dùng có thể lựa chọn các giao diện đồ họa tiêu biểu cho LINUX/UNIX như sau:

X Windows

Hệ thống giao diện đồ họa X Windows được Viện Công nghệ Massachusetts phát minh ra vào những năm 1980. Mục đích của hệ thống này là để đảm bảo tính độc lập hoàn toàn với các thiết bị và giao tiếp mạng. Hệ thống được thiết kế để dễ dàng chuyển đổi sang các kiểu thiết bị phần cứng mới và đề cho các chương trình hoạt động ở máy tính này có thể hiển thị kết quả ở máy khác. Đặc điểm thứ hai này rất hữu dụng cho phép máy tính cấu hình yếu hơn có thể tận dụng năng lực của máy tính mạnh và đắt tiền hơn.

X Windows trở thành chuẩn không chính thức cho UNIX. Chương trình chủ *X Server* kiểm soát các dịch vụ của X Windows bao gồm cả các thiết bị phần cứng như bàn phím, chuột, thiết bị hiển thị... và dịch vụ phần mềm như phông chữ, màu sắc. Các chương trình truy nhập đến các chức năng hiển thị gọi là chương trình khách.

Các chương trình quản lý giao diện làm nhiệm vụ thay đổi kích cỡ cửa sổ, hiện thị các chương trình hay ẩn các biểu tượng của người dùng... Khi khởi động X Windows, người dùng có thể lựa chọn chương trình quản lý giao diện mà mình cài đặt.

Unity

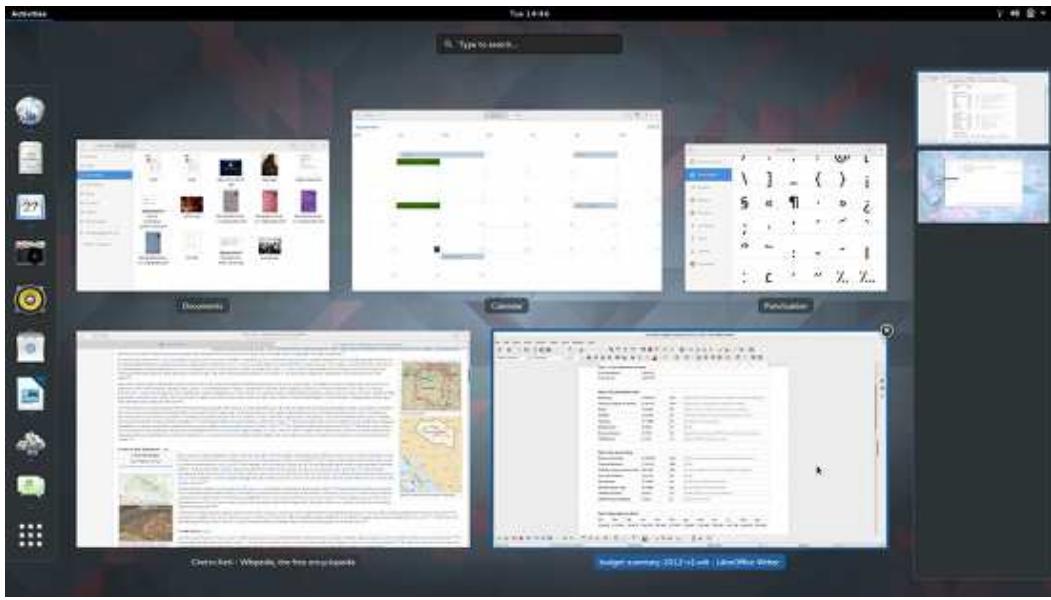
Unity là môi trường làm việc đồ họa của phiên bản Ubuntu do công ty Canonical phát triển. Unity hoạt động trên nền GNOME và dùng hầu hết các ứng dụng và công cụ của GNOME. Khá nhiều chức năng giao diện của Unity giống với Windows 7 như thanh nhiệm vụ, giao tiếp dùng phím tắt hay chuột.



Hình V-3. Màn hình làm việc Unity

GNOME

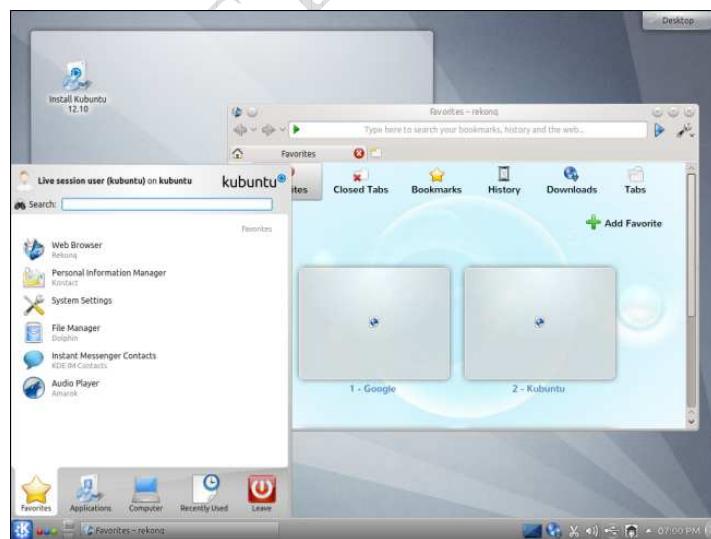
Đây là môi trường làm việc phổ biến nhất với đặc trưng đơn giản và khá gọn nhẹ. GNOME được Miguel de Icaza và Federico Mena xây dựng từ năm 1997. GNOME được chọn làm môi trường làm việc mặc định cho người dùng của Ubuntu, Fedora và Debian. Phiên bản GNOME 3 được thiết kế mới hoàn toàn và hướng tới các thiết bị hỗ trợ giao tiếp chạm.



Hình V-4. Màn hình làm việc GNOME.

KDE

KDE thường phức tạp hơn so với GNOME do cung cấp nhiều tùy chọn cấu hình và tính năng hơn. Cách bố trí các phần tử giao diện của KDE trông khá giống môi trường làm việc của Microsoft Windows. KDE phù hợp với người dùng muốn có nhiều lựa chọn để cấu hình máy tính làm việc của theo yêu cầu mình.



Hình V-5. Màn hình làm việc KDE

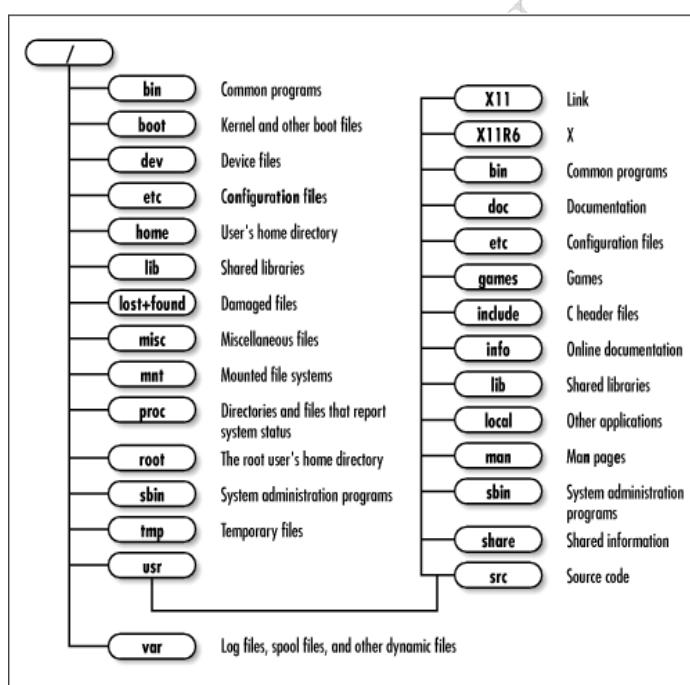
V.4 Hệ thống file của Linux/Unix

Hệ thống file cung cấp phương tiện tổ chức dữ liệu trên các thiết bị lưu trữ và giúp che dấu các chi tiết vật lý như cung (*sector*) hay liên cung (*cluster*) với người dùng. Hệ thống file

của LINUX/UNIX có cấu trúc dạng cây. Gốc của cây cũng đồng thời gọi là gốc hệ thống file được phân biệt bằng ký tự “/”. Phía dưới gốc là các file và thư mục như trong hình dưới đây.

Ý nghĩa của các thư mục tiêu biểu như sau:

- `/`: thư mục gốc
- `/dev`: thư mục lưu các file mô tả thiết bị sử dụng trong hệ thống
- `/etc`: lưu file cấu hình của hệ thống
- `/home`: thư mục của người dùng
- `/sbin`: các chương trình quản trị hệ thống
- `/tmp`: nháp dùng để lưu các file tạm thời
- `/usr`: chương trình người dùng
- `/var`: chứa các file nhật ký hoạt động của hệ thống và các chương trình người dùng.



Hình V-6. Cây thư mục LINUX/UNIX

Các hệ thống file phổ biến được LINUX/UNIX hỗ trợ như sau:

- *Hệ thống file mở rộng (Extended File System)*. Phiên bản ext2 là hệ thống file cổ nhất và vẫn được sử dụng của LINUX. Đây là hệ thống file đơn giản có khả năng chống lại việc phân mảnh hệ thống file tuy nhiên có tốc độ truy nhập chậm. Các phiên bản ext3 và ext4 ra đời giải quyết các điểm yếu của phiên bản nguyên thủy và cung cấp các tính năng cao cấp hơn như khả năng chịu lỗi, mở rộng kích thước lưu trữ.

- *Hệ thống FAT* là hệ thống file đơn giản song không có khả năng chịu lỗi và dễ bị phân mảnh. Hệ thống file này nay vẫn được sử dụng cho các thiết bị lưu trữ ngoài như thẻ nhớ hay thẻ nhớ USB.
- *Hệ thống file xfs* hướng tới các doanh nghiệp hay công ty lớn, hiệu năng cao, có khả năng chịu lỗi tốt thông qua cơ chế nhật ký (*log*). *xfs* là hệ thống file 64 bit có khả năng quản lý dung lượng lưu trữ tới 10^6 TB.

Để sử dụng được các hệ thống file trên các thiết bị lưu trữ người dùng phải thực hiện thao tác “*gắn*” (*mount*) hệ thống file đó vào trong một thư mục của hệ điều hành. Thao tác này có thể được lập trình tự động khi máy tính khởi động hoặc khi người dùng đăng nhập vào hệ thống.

V.5 Các phiên bản chính của Linux/Unix

Unix là một trong những dòng hệ điều hành lâu đời với nhiều tính năng quan trọng như đa người dùng, chia sẻ tài nguyên và các tính năng này có ảnh hưởng mạnh mẽ đến các dòng hệ điều hành hiện thời. Với mục tiêu ban đầu tạo ra hệ điều hành có môi trường làm việc làm việc tương tự UNIX, ngày nay các hệ điều hành dựa trên Linux đã thay thế hầu hết các phiên bản thương mại UNIX. Cùng với sự phát triển mạnh mẽ của mã nguồn mở, các phiên bản Linux đã thu hút không chỉ giới học thuật hay người dùng cuối mà rất nhiều công ty lớn đã cung cấp các giải pháp hệ thống khác nhau dựa trên nền Linux. Dưới đây trình bày tóm tắt các phiên bản cơ bản của hai dòng hệ điều hành UNIX và Linux.

V.5.1 Các phiên bản Unix

System V là phiên bản thương mại quan trọng trong những năm 1980 do công ty AT&T phát triển. Phiên bản UNIX này làm cơ sở cho nhiều phiên bản thương mại do các công ty lớn phát triển và đưa ra thị trường như HP, IBM. Các phiên bản thương mại đáng kể gồm có: AIX do công ty IBM phát triển từ năm 1990, Sun Solaris do công ty SUN Microsystems, HP-UX do *Hewlett Packard* từ 1990...

Sự phát triển mạnh mẽ của máy tính cá nhân PC khiến cho việc chạy UNIX và các phần mềm truyền thống trên PC trở nên dễ dàng và thuận tiện hơn. Việc phát triển của các sản phẩm và cộng đồng sử dụng mã nguồn mở làm cho thị phần của UNIX thu nhỏ so với LINUX. Đến nay, các phiên bản UNIX vẫn còn được sử dụng trong các hệ thống chuyên biệt.

Phiên bản BSD được phát triển bởi Trung tâm Nghiên cứu hệ thống máy tính của Trường Tổng hợp California. Đây là phiên bản có nhiều ảnh hưởng trong giới học thuật. Phiên bản nguyên thủy vẫn chứa các đoạn mã nguồn riêng của AT&T và được công ty này cấp phép. Kể từ bản 4.4, BSD không còn chịu các hạn chế bản quyền và cấp mã nguồn tới mọi người dùng.

V.5.2 Các phiên bản Linux

LINUX là hệ điều hành cung cấp máy tính lập trình UNIX phong phú và miễn phí theo Giấy phép GNU công cộng. Hệ điều hành này được phát triển vào năm 1991 do Linus

Tovalds và được tiếp tục bởi cộng đồng và nhiều nhà sản xuất. Sau đây là các phiên bản tiêu biểu.

Debian do Ian Murdock phát triển vào năm 1993. Đây là một trong những phiên bản LINUX phổ biến nhất do tính tin cậy và có bộ quản lý phần mềm mạnh. Phiên bản này được cung cấp từ địa chỉ <http://www.debian.org/>. Các biến thể từ phiên bản này bao gồm:

- *Ubuntu*, www.ubuntu.com, được hỗ trợ từ công ty Canonical Ltd.
- *Knoppix*, <http://www.knoppix.org/>, cho phép chạy từ đĩa quang phù hợp với việc phục hồi hệ thống.
- *Linspire*, www.linspire.com, phù hợp với người dùng phổ thông quen thuộc với môi trường Microsoft Windows.

Redhat do công ty Redhat, www.redhat.com, hỗ trợ và phát triển, hướng tới nhóm người dùng công ty và xí nghiệp. Phiên bản miễn phí của RedHat có tên là Fedora cũng do công ty duy trì và phát triển. Một biến thể khác là Mandrake cung cấp giao diện thân thiện và dễ dùng, hỗ trợ thiết bị phần cứng tốt www.mandriva.com.

SlackWare, có địa chỉ tại www.slackware.com, là phiên bản Linux hướng tới giao diện dòng lệnh, khó sử dụng với người dùng mới.

SuSE có địa chỉ tại www.opensuse.org. Phiên bản này cung cấp giao diện người dùng thân thiện và cấu hình phần cứng qua giao diện đồ họa.

Chương VI. CÀI ĐẶT VÀ QUẢN TRỊ CÁC THÀNH PHẦN CƠ BẢN CỦA LINUX/UNIX

Chương này trình bày các yêu cầu cần thiết cho việc cài đặt hệ điều hành Linux, cụ thể tập trung vào phiên bản Ubuntu dành cho máy chủ. Ngoài ra, phần này giới thiệu cách thức và các công cụ hỗ trợ cho việc quản lý chương trình và máy tính cục bộ. Các công việc quản trị thiết yếu bao gồm các trình điều khiển thiết bị, hệ thống file, quản lý người dùng và các chương trình.

VI.1 Cài đặt Linux/Unix

Kể từ chương này, các nội dung cài đặt và thiết lập quản trị sẽ tập trung vào phiên bản LINUX do công ty Canonical cung cấp. Đây là phiên bản UNIX có giao diện thân thiện và được hỗ trợ dài hạn.

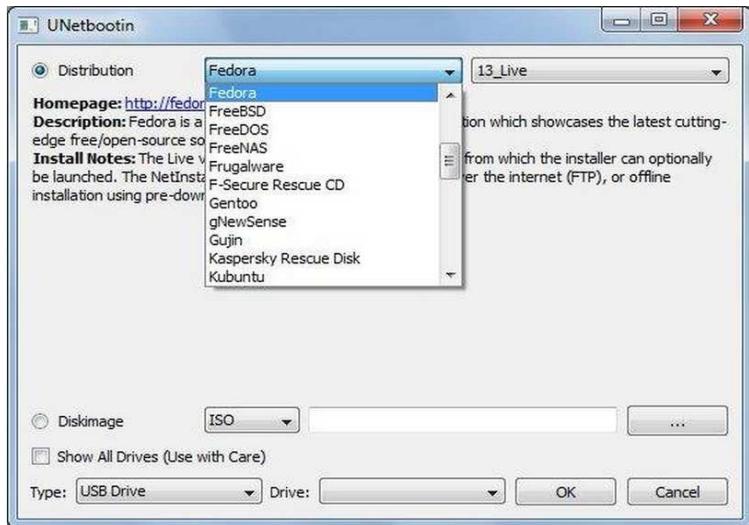
Yêu cầu phần cứng tối thiểu cho việc cài máy chủ LINUX là bộ xử lý hỗ trợ tập lệnh x86 hoặc x64, tần số 300MHz, dung lượng bộ nhớ 192MB, ổ cứng 1GB (với giao diện đồ họa cần nhiều hơn ~2GB). Tùy thuộc vào các chương trình chạy trên máy chủ mà yêu cầu phần cứng có thể thay đổi, người quản trị cần lập kế hoạch về các chương trình sẽ chạy để có cấu hình phù hợp.

VI.1.1 Cài đặt

Để chuẩn bị cho việc cài đặt, người quản trị cần tải về gói phần mềm cài đặt phù hợp dưới dạng file ISO từ trang Web của nhà cung cấp (<http://www.ubuntu.com/download/server>) trong đó:

- I386 cho máy tính hỗ trợ tập lệnh x86
- AMD64 cho máy tính hỗ trợ tập lệnh x64

Người quản trị có thể tạo đĩa cài từ CD/DVD bằng cách ghi đĩa hoặc từ thẻ nhớ USB bằng chương trình tiện ích như Unetbootin (<https://unetbootin.github.io/>) Hình VI-1. Chương trình Unetbootin hỗ trợ việc tải về trực tiếp các phiên bản LINUX mà người dùng có thể cài đặt.



Hình VI-1. Giao diện tạo đĩa cài cho ổ USB flash.

Việc cài đặt Ubuntu tương đối dễ dàng và đơn giản nhờ có giao diện thân thiện và hỗ trợ nhiều ngôn ngữ. Trước tiên, người quản trị lựa chọn ngôn ngữ cho việc cài đặt có thể chọn tiếng Việt hay các ngôn ngữ khác. Để cài đặt máy chủ, bước tiếp theo người quản trị chọn kiểu cài đặt là máy chủ “*Install Ubuntu Server*”. Các bước tiếp theo như sau:

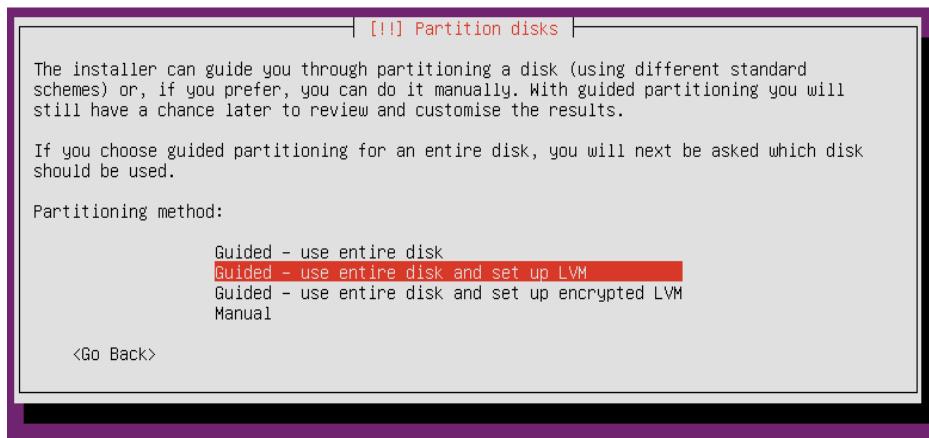
1. *Chọn ngôn ngữ hệ thống.* Khác với bước trước, ngôn ngữ này được sử dụng để hiện thị toàn bộ các lựa chọn và dùng cho các ứng dụng chạy trên máy chủ.
2. *Lựa chọn kiểu bố trí bàn phím.* Thông thường kiểu bàn phím thường dùng ở Việt Nam làm kiểu bàn phím tiêu chuẩn của Mỹ.
3. *Cài đặt các chương trình phát hiện và điều khiển cho phần cứng máy chủ.* Chú ý nếu người quản trị không muốn sử dụng địa Internet tự động thì có thể chọn cài đặt thủ công.
4. *Thiết lập người dùng có quyền cao nhất root.* Người quản trị tạo tên/mật khẩu đăng nhập để quản trị máy chủ.
5. *Lựa chọn mã hóa thư mục người dùng.* Việc này giúp tăng tính bảo mật các thông tin và dữ liệu của người dùng hệ thống.
6. *Thiết lập thời gian cho hệ thống* (Hình VI-2). Đây là thông tin quan trọng nếu thiết lập không chính xác làm cho các chương trình cần đến yêu tố thời gian như mã hóa hay xác thực không hoạt động được.



Hình VI-2. Thiết lập thời gian hệ thống.

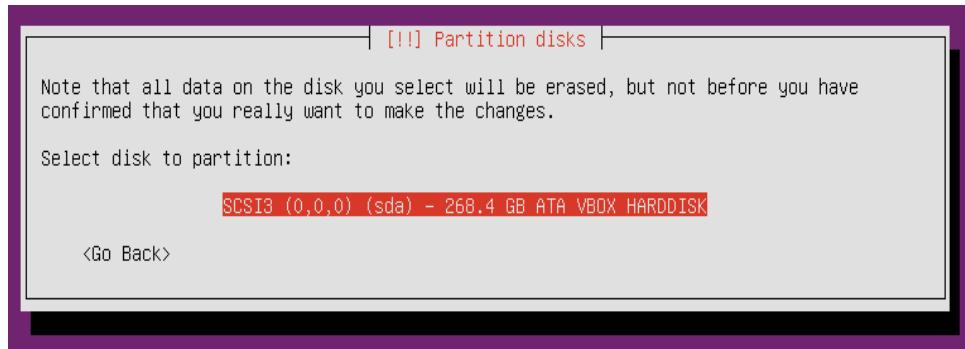
7. *Phân vùng ổ đĩa vật lý*. Đây là bước rất quan trọng và tương đối phức tạp. Về cơ bản LINUX cần 2 vùng ổ cứng riêng biệt để hoạt động ổn định. Thứ nhất là phân vùng cho thư mục gốc, nơi sẽ chứa thư mục và các file chương trình cần cho máy chủ và người dùng. Phân vùng này chiếm phần lớn không gian lưu trữ. Thứ hai là vùng ổ cứng dành cho việc lưu trữ tạm thời (*swap*). Với hệ thống có bộ nhớ nhỏ hơn 16GB thì kích cỡ của vùng này khoảng 8GB là phù hợp. Với hệ thống mà bộ nhớ lớn hơn 64GB thì nên có tối thiểu 32GB cho vùng lưu trữ tạm thời. Với trường hợp khác, kích thước vùng lưu trữ tạm thời tối đa nên gấp đôi dung lượng bộ nhớ của hệ thống.

Chương trình cài đặt trợ giúp người quản trị lựa chọn các thao tác phân vùng có hướng dẫn (*guide*) hoặc thủ công (*manual*). Ngoài ra, chương trình hỗ trợ cài đặt LVM (*Logical Volume Manager*) cho phép ổ đĩa lô-gíc trải trên nhiều ổ vật lý.



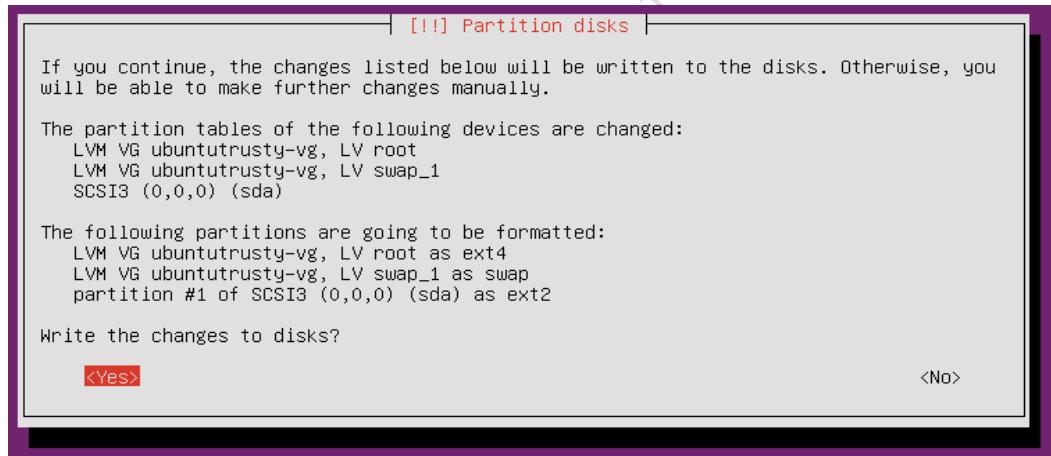
Hình VI-3. Các lựa chọn phân vùng ổ cứng.

Sau khi chọn phân vùng có hướng dẫn, chương trình sẽ yêu cầu người quản trị lựa chọn ổ vật lý và kích thước của các phân vùng để cài đặt như trong hình sau.



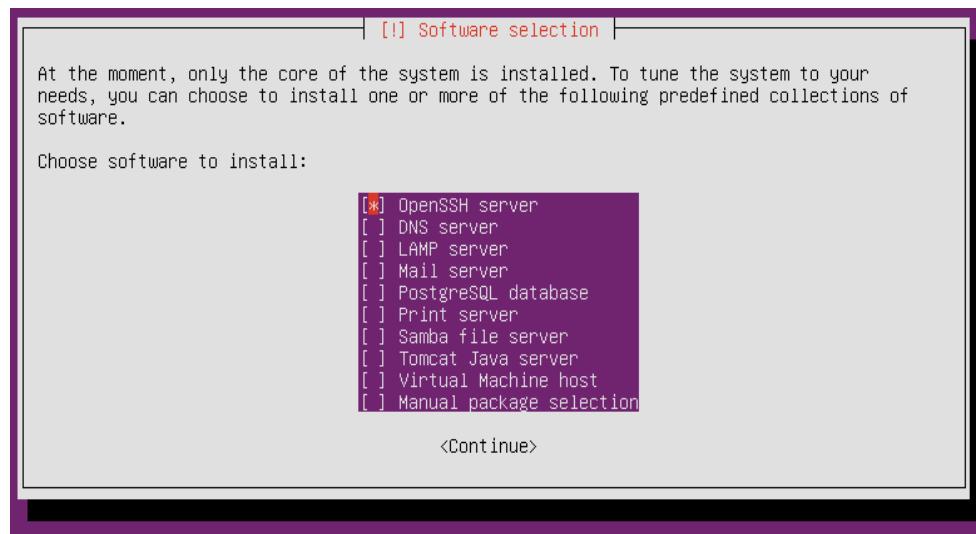
Hình VI-4. Lựa chọn ổ đĩa vật lý để cài đặt.

Kết thúc chương trình sẽ thông báo các lựa chọn của người quản trị để tiếp tục quá trình cài đặt như trong hình dưới đây. Nếu người quản trị muốn thay đổi các thiết lập ổ đĩa thì từ chối việc ghi các thiết lập và làm lại việc phân vùng từ đầu.



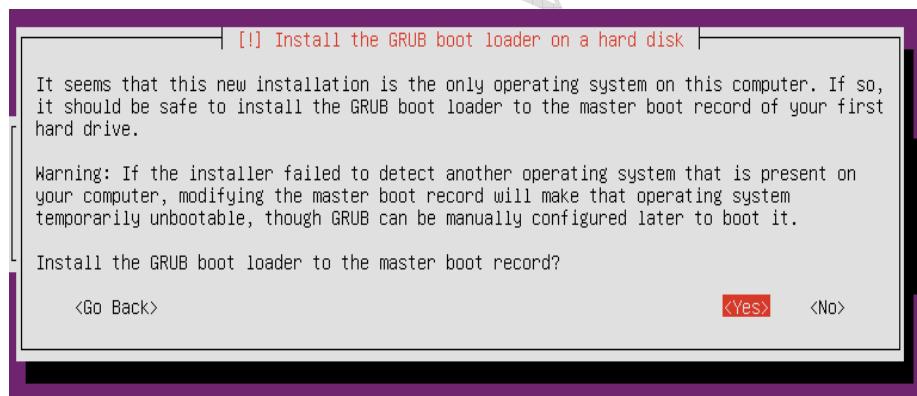
Hình VI-5. Tóm tắt các thông tin về phân vùng ổ đĩa.

8. Ở bước kế tiếp, người quản trị lựa chọn việc *cập nhật và tự động cài đặt các bản cập nhật* cho hệ thống. Thông thường, các bản cập nhật liên quan đến an toàn hệ thống nên được tự động cài đặt.
9. *Lựa chọn cài đặt các phần mềm dịch vụ máy chủ* như trong hình dưới. Các phần mềm này có thể được cài đặt riêng rẽ nếu như người quản trị chưa muốn thực hiện cài đặt các gói phần mềm này.



Hình VI-6. Các gói phần mềm dành cho các dịch vụ máy chủ.

10. *Cài đặt phần mềm quản lý khởi động GRUB.* Đây là phần mềm cho phép quản lý khởi động nhiều hệ điều hành khác nhau trên cùng một máy tính vật lý. Nếu người quản trị chỉ muốn cài duy nhất một hệ điều hành thì có thể bỏ qua cài đặt này.



Hình VI-7. Cài đặt trình quản lý khởi động GRUB.

11. Sau khi cài đặt thành công máy tính sẽ khởi động và màn hình làm việc sẽ hiện ra như hình dưới đây. Người quản trị sử dụng tên/mật khẩu tạo trong quá trình cài đặt để đăng nhập vào hệ thống và thực hiện các cài đặt tiếp theo. Cần chú ý rằng, để sử dụng giao diện đồ họa người quản trị cần phải tiếp tục thực hiện việc cài đặt riêng biệt. Việc dùng giao diện đồ họa sẽ làm tăng gánh nặng cho hệ thống và rủi ro an toàn.

```

Starting /etc/rc.local Compatibility...
Starting Network Manager Wait Online...
[ OK ] Started Modem Manager.
[ OK ] Started /etc/rc.local Compatibility.
Starting Wait for Plymouth Boot Screen to Quit...
[ OK ] Started Wait for Plymouth Boot Screen to Quit.
[ OK ] Started Getty on tty1.
Starting Getty on tty1...
[ OK ] Reached target Login Prompts.
[ OK ] Started Network Manager Wait Online.

Ubuntu 15.04 ubuntu tty1
ubuntu login: _

```

Hình VI-8. Màn hình khởi động Ubuntu của người dùng *ubuntu*

VI.1.2 Cài đặt mạng

Nếu người quản trị muốn tự gán địa chỉ mạng cho máy chủ thì cần sử dụng câu lệnh *ifconfig*. Câu lệnh này cần đặc quyền quản trị để có hiệu lực nhờ vào câu lệnh *sudo*. Câu lệnh sau sẽ gán địa chỉ Internet 192.168.1.9 cho giao tiếp mạng *eth1*:

```
sudo ifconfig eth1 192.168.1.9 netmask 255.255.255.0
```

Người quản trị có thể liệt kê các thông số mạng LAN qua câu lệnh “*ifconfig -a | grep eth*”. Kết quả câu lệnh như trong hình sau

```

phamhduy@ubuntu:~$ ifconfig -a
eth0      Link encap:Ethernet HWaddr 00:0c:29:73:84:80
          inet addr:192.168.200.131 Bcast:192.168.200.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe73:8480/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:6809 errors:0 dropped:0 overruns:0 frame:0
             TX packets:2270 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:7570595 (7.5 MB) TX bytes:430573 (430.5 KB)

eth1      Link encap:Ethernet HWaddr 00:0c:29:73:84:8a
          inet addr:192.168.1.9 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe73:848a/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1456 errors:0 dropped:0 overruns:0 frame:0
             TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:107143 (107.1 KB) TX bytes:8117 (8.1 KB)

```

Hình VI-9. Các tham số cài đặt cho mạng LAN.

Việc cài đặt tham số mạng cũng có thể được thực hiện qua việc sửa đổi file cấu hình mạng “*/etc/network/interfaces*”. Người quản trị cần sử dụng đặc quyền để sửa đổi nội dung của file này. Việc sửa đổi có thể dùng bất cứ trình soạn thảo đi kèm nào như *vi*. Câu lệnh sẽ là “*sudo vi /etc/network/interfaces*”. Nội dung cấu hình như sau

```
iface eth1 inet static
address 192.168.1.9
netmask 255.255.255.0
gateway 192.168.1.1
```

Trong trường hợp giao tiếp mạng sử dụng phương pháp tự động cấp địa chỉ Internet cho giao tiếp mạng LAN *eth0* thì nội dung file cấu hình là

```
auto eth0
iface eth0 inet dhcp
```

VI.1.3 Cài đặt giao diện đồ họa

Việc cài đặt giao diện đồ họa cho máy chủ có một số nhược điểm:

- Nhiều đoạn mã được sử dụng hơn nên dễ dẫn đến nhiều rủi ro về an ninh, quản lý việc cập nhật.
- Hiệu năng chịu ảnh hưởng do chia sẻ tài nguyên cần cho giao diện đồ họa
- Phần giao diện đồ họa chứa một số phần mềm có thể không thích hợp với môi trường máy chủ dễ gây xung đột
- Hỗ trợ kỹ thuật hạn chế từ nhà cung cấp.

Thay vì cài đặt giao diện đồ họa đầy đủ, người quản trị có thể cài đặt dịch vụ quản trị qua Web như Zentyal. Trong trường hợp cần thiết người quản trị có thể cài đặt giao diện hạn chế bằng cách sử dụng *X Windows*. Trước tiên, cài đặt máy chủ dịch vụ *X Windows* bằng câu lệnh *sudo apt-get install xorg*, tiếp theo người quản trị có thể cài chương trình quản lý giao diện nhỏ gọn, chạy nhanh, tiêu tốn ít tài nguyên như *Openbox* hay *Fluxbox* qua câu lệnh *sudo apt-get install fluxbox*.

Khi người sử dụng mong muốn môi trường làm việc đầy đủ, người quản trị có thể cài đặt:

- Giao diện Unity của Ubuntu qua câu lệnh *sudo apt-get install ubuntu-desktop*
- Giao diện Kubuntu (KDE) qua câu lệnh *sudo apt-get install kubuntu-desktop*
- Giao diện GNOME qua câu lệnh *sudo apt-get install gnome-shell*

VI.2 Quản trị các trình điều khiển thiết bị

Phần cứng máy tính ngày càng trở nên phổ biến và dễ sử dụng đặc biệt là các thiết bị được thiết kế theo kiểu cảm-chạy hay sử dụng giao tiếp như USB. Tất cả thiết bị phần cứng cần phần mềm nhân còn gọi là trình điều khiển thiết bị để có thể được sử dụng thích đáng từ hệ điều hành. Phần lớn trình điều khiển thiết bị được tích hợp sẵn vào nhân của Linux. Các chương trình này có thể đã được tích hợp sẵn trong nhân hoặc sẽ được nạp khi phát hiện phần cứng phù hợp.

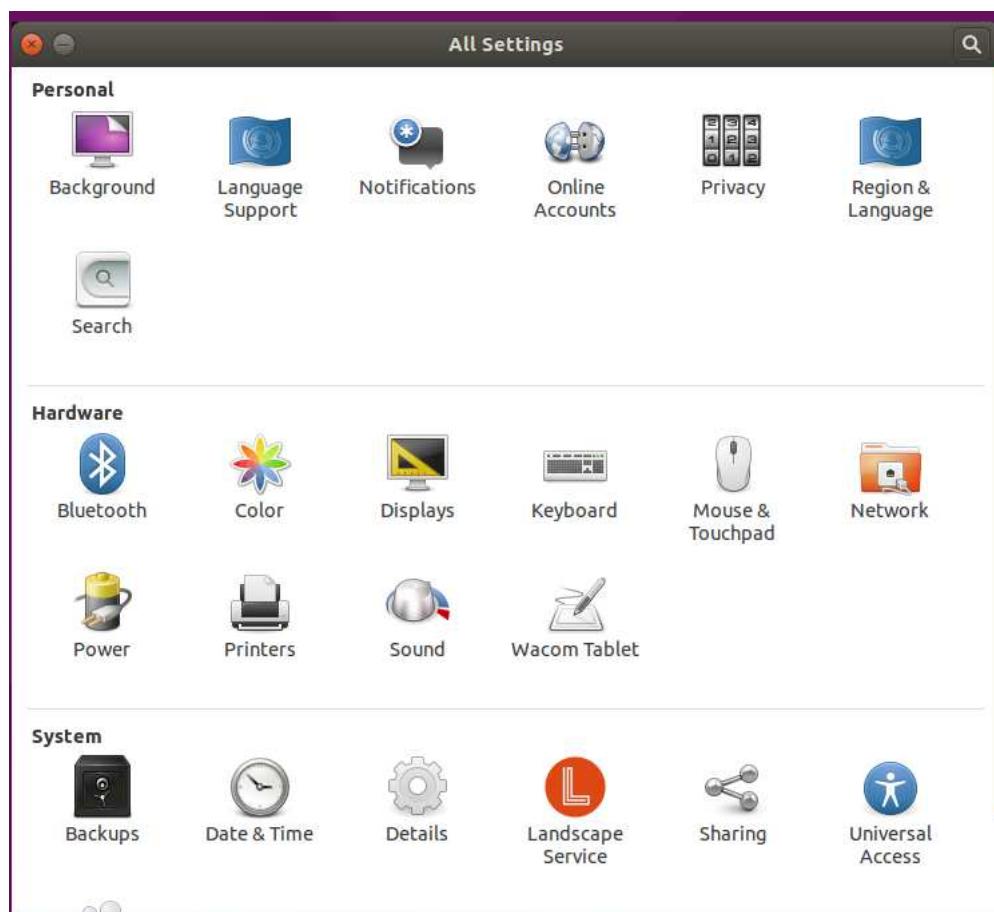
Điều cần chú ý là do đặc tính mở và cộng đồng nên trình điều khiển có thể do cá nhân, cộng đồng hay nhà sản xuất viết/bảo trì. Ngoài ra, còn có trình điều khiển riêng thường do một số nhà sản xuất không chia sẻ chương trình điều khiển nên người dùng phải tự cài đặt.

Khi sử dụng giao diện dòng lệnh, người quản trị có thể sử dụng các câu lệnh quản lý các mô-đun nhân để quản lý các trình điều khiển thiết bị như dưới đây:

- *lsmod*: liệt kê các chương trình điều khiển thiết bị được nạp vào bộ nhớ và thông tin về bộ nhớ và số lần chương trình này được sử dụng.

- *modprobe*: nạp chương trình điều khiển thiết bị vào bộ nhớ
- *rmmod*: loại bỏ chương trình điều khiển thiết bị ra khỏi bộ nhớ. Cần chú ý là không có chương trình nào khác sử dụng chương trình này.

Linux cung cấp công cụ đồ họa cho phép quản trị phần cứng và trình điều khiển. Trong Ubuntu, tiện ích này được cung cấp qua bộ giao diện đồ họa và dễ dàng truy nhập. Qua tiện ích này người quản trị có thể xem xét và quản lý các phần cứng cũng như trình điều khiển thiết bị một cách nhanh chóng và thuận tiện như trong hình dưới đây.



Hình VI-10. Tiện ích quản lý thiết bị trong Ubuntu.

Như trong hình vẽ, các cài đặt về phần cứng và hệ thống được thể hiện dưới các biểu tượng tương ứng giúp cho người dùng có thể lựa chọn các thao tác phù hợp như quản lý các thiết bị mạng, màn hình, hay máy in.

VI.3 Hệ thống lưu trữ

VI.3.1 Giới thiệu

Hệ thống lưu trữ file Linux/Unix được tổ chức thành cây thư mục thống nhất với thư mục gốc “/”. Các file và thư mục được lưu trong thiết bị lưu trữ và được “cài đặt” vào cây thư mục. Nói cách khác, từ góc độ người dùng thông thường sẽ không thể phân biệt được các

thiết bị lưu trữ vật lý được sử dụng trong hệ thống. Điều này khác với người dùng Windows truyền thống ở chỗ người dùng cần nhận biết các thiết bị lưu trữ vật lý như ổ đĩa cứng hay ổ đĩa quang.

Để đơn giản và thuận tiện cho người dùng thông thường cũng như che dấu các chi tiết vật lý của thiết bị lưu trữ, người quản trị phải thực hiện các thao tác phân chia, lựa chọn kiểu hệ thống file, và cài đặt. Nói chung các thao tác này chỉ cần tiến hành một lần tại thời điểm cài đặt và cấu hình hệ thống song nó cũng có thể được thực hiện nhiều lần do nhu cầu sử dụng thay đổi như việc thay đổi kích cỡ của phân vùng lưu trữ dành cho ứng dụng người dùng.

VI.3.2 Đặt tên thiết bị lưu trữ

Các ổ đĩa vật lý theo chuẩn kết nối SCSI* hay SATA† được ký hiệu là *sd* và số thứ tự của các ổ đĩa vật lý được phân biệt thông qua chữ cái với *a* thể hiện ổ đĩa vật lý thứ nhất. Tiếp theo, các phân vùng trong ổ đĩa vật lý được phân biệt nhờ số thứ tự. Như vậy *sda1* dùng để chỉ tới phân vùng đầu tiên của ổ cứng thứ nhất sử dụng kết nối SCSI/SATA. Tương tự như vậy, các ổ đĩa vật lý theo chuẩn kết nối IDE‡ sử dụng ký hiệu *hda1* cho phân vùng đầu tiên của ổ đĩa vật lý IDE đầu tiên.

Việc phân chia ổ đĩa vật lý được thực hiện thông qua các tiện ích dòng lệnh như *fdisk*, *parted* hay tiện ích đồ họa như *gparted*. Một ổ cứng vật lý có thể được chia thành nhiều vùng giúp cho việc sử dụng và quản lý hiệu quả không gian lưu trữ. Về cơ bản, người quản trị có thể phân chia các phân vùng chủ yếu như sau:

- *sda1*, phân vùng đầu tiên, làm phân vùng khởi động được ánh xạ (cài đặt) vào thư mục */boot*, kích cỡ khoảng 100MB.
- *sda2*, phân vùng thứ 2, làm thư mục gốc (*/root*) chứa hệ điều hành với kích cỡ có thể chiếm hầu hết không gian lưu trữ.
- *sda3*, phân vùng thứ 3, làm thư mục chính cho người dùng (*/home*) lưu trữ các file dữ liệu cũng như chương trình với kích cỡ tùy theo khả năng lưu trữ và nhu cầu.
- *sda4*, phân vùng thứ 4, làm vùng nhớ tạm (*swap*) cho bộ nhớ chính của hệ điều hành.

```
# fdisk /dev/sda
Command (m for help): p

Disk /dev/sda: 240 heads, 63 sectors, 2184 cylinders
Units = cylinders of 15120 * 512 bytes

Device Boot Start End Blocks Id System
/dev/sda1      1   14 105808+  83 Linux
/dev/sda2     15   49 264600   82 Linux swap
/dev/sda3     50   70 158760   83 Linux
/dev/sda4     71 2184 15981840     5 Extended
```

Hình VI-11. Sử dụng câu lệnh *fdisk*.

* SCSI - Small Computer System Interface: Giao tiếp hệ thống máy tính nhỏ

† SATA - Serial AT Attachment: Kết nối AT(Advanced Technology) nối tiếp

‡ IDE - Integrated Drive Electronics: Ổ đĩa điện tử tích hợp

Sau khi thực hiện việc phân chia các vùng trong không gian lưu trữ vật lý, người quản trị cần phải tiến hành cài đặt hệ thống file cho phân vùng mới. Hệ thống file chính là cách thức lưu trữ và quản lý các file và thư mục của người dùng (Tham khảo mục V.4). Từ giao diện dòng lệnh, người quản trị có thể sử dụng câu lệnh `mkfs.<kiểu_hệ_thống_file>`. Ví dụ để cài đặt hệ thống file ext3 cho ổ đĩa cứng thứ nhất, phân vùng thứ hai người quản trị dùng câu lệnh `mkfs.ext3 /dev/sda2`.

Để sử dụng được hệ thống file mới cài đặt người quản trị cần thực hiện thao tác “*gắn*” hệ thống file mới này vào trong cấu trúc cây thư mục. Về cơ bản, thao tác này yêu cầu người quản trị lựa chọn vị trí thư mục để liên kết với phân vùng vừa được cài đặt hệ thống file xong. Câu lệnh `mount` giúp thực hiện thao tác này. Để gắn phân vùng thứ hai vào thư mục người dùng có thể sử dụng câu lệnh như sau:

```
mount -t ext3 /dev/sda2 /home
```

VI.3.3 File cấu hình

Để thuận tiện thông tin chi tiết cấu hình về các thiết bị lưu trữ như ổ đĩa cứng được lưu trong file cấu hình “`/etc/fstab`”. Khi khởi động, Linux đọc các thông tin từ file này và cài đặt hệ thống file thống nhất cho người dùng. Nội dung tiêu biểu của file này như sau:

<code>/dev/sda8</code>	<code>/</code>	<code>ext4</code>	<code>defaults,noatime</code>	<code>0 0</code>
<code>/dev/sda5</code>	<code>none</code>	<code>swap</code>	<code>sw</code>	<code>0 0</code>
<code>/dev/sda6</code>	<code>/boot</code>	<code>ext4</code>	<code>noauto,noatime</code>	<code>0 0</code>
<code>/dev/sda7</code>	<code>/home</code>	<code>ext4</code>	<code>defaults,noatime</code>	<code>0 0</code>
<code>/dev/sdb1</code>	<code>/media/usb</code>	<code>auto</code>	<code>user,noauto,gid=users</code>	<code>0 0</code>

Hình VI-12. Nội dung file fstab.

Cột thứ nhất của `fstab` cho biết thiết bị lưu trữ vật lý và phân vùng; Cột thứ hai cho biết vị trí của thư mục hệ thống được liên kết với phân vùng này; Cột thứ ba cho biết kiểu hệ thống file; cột thứ 4 là các tham số liên quan đến việc truy nhập hệ thống file; Cột thứ năm cho biết hệ thống file có sử dụng sao lưu với hay không; Cột thứ sáu cho biết thứ tự kiểm tra hệ thống file khi khởi động.

Với các thông tin trong `fstab` câu lệnh `mount` có thể rút gọn như “`mount /home`” thay vì cung cấp đầy đủ các tham số.

VI.3.4 Quản lý ổ đĩa lô-gíc LVM

Quản lý ổ đĩa lô-gíc LVM (*Logical Volume Manager*), được nhiều phiên bản Linux hỗ trợ, cho phép người quản trị thiết lập nhóm thiết bị lưu trữ hay tạo phân vùng một cách linh hoạt. Với LVM các ổ đĩa và phân vùng có thể chứa nhiều ổ đĩa và phân vùng khác nhau. Nói cách khác, LVM quản lý ổ đĩa và phân vùng lô-gíc ánh xạ tới nhiều ổ đĩa và phân vùng vật lý mà hệ điều hành hay người dùng không biệt được là một hay nhiều thiết bị vật lý.

LVM cung cấp giải pháp cho phép người quản trị dễ dàng mở rộng, nâng cấp hay thay đổi không gian lưu trữ một cách mềm dẻo và linh hoạt. Khi cài đặt Ubuntu, LVM được hỗ trợ sẵn trong quá trình cài đặt. Người quản trị không cần phải tải về bộ công cụ LVM.

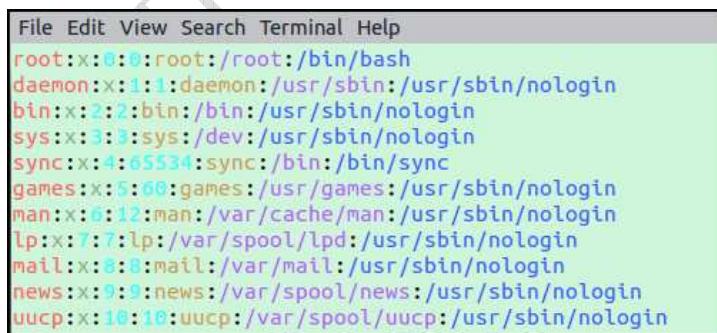
VI.4 Người dùng và quyền truy nhập

Linux/Unix là hệ điều hành hỗ trợ nhiều người dùng. Ngay cả khi hệ thống chỉ có một người sử dụng, nó vẫn được cấu hình như là hệ thống nhiều người dùng. Điều này có một số lợi ích:

- Đảm bảo an ninh và ngăn chặn phần mềm độc hại nhờ việc các ứng dụng chạy bằng tài khoản người dùng thông thường chứ không phải với đặc quyền quản trị hệ thống.
- Trong trường hợp hệ thống cần cho nhiều người dùng, chỉ cần tạo thêm người dùng vào hệ thống.
- Dễ dàng sao lưu các file của người dùng vì chúng được lưu bên trong thư mục riêng của từng người dùng.

VI.4.1 Người dùng và nhóm

Mỗi người dùng được phân biệt thông qua tên hay định danh người dùng. Thực tế Linux/Unix phân biệt định danh người dùng dưới dạng số và tên người dùng. Mỗi người dùng được xác thực nhờ cơ chế kiểm tra mật khẩu. Mặc định, các thông tin người dùng này được lưu trong file `/etc/passwd`. Về cấu trúc, file `passwd` lưu các thông tin về người dùng vào trong 1 dòng có cấu trúc: tên đăng nhập, mật khẩu hay `x` nếu được lưu ở chỗ khác, số định danh, số định danh nhóm, mô tả, thư mục riêng, ngôn ngữ mặc định.



```
File Edit View Search Terminal Help
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
```

Hình VI-13. Nội dung cơ bản của `passwd`.

Cấu trúc nguyên thủy của `passwd` đặt ra vấn đề về bảo mật do thông tin về mật khẩu được lưu ở dạng không mã hóa. Vì thế cần phải sử dụng công cụ khác như `shadow` để hạn chế rủi ro này. Các mật khẩu người dùng khi được mã hóa lưu vào file `/etc/shadow` và các thông tin giúp quản lý tốt hơn mật khẩu người dùng như thời hạn mật khẩu, thời gian thay đổi mật khẩu.

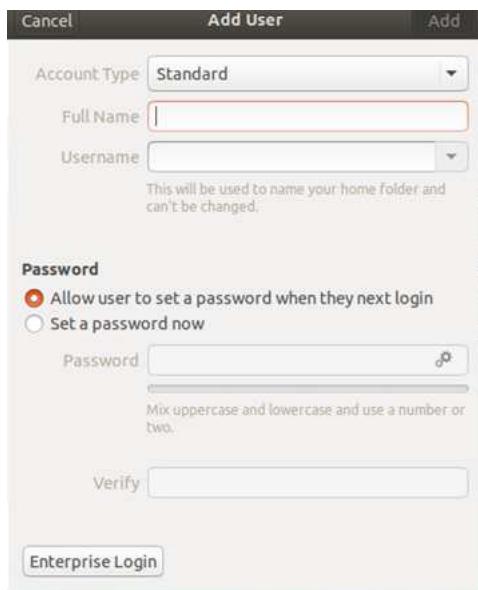
Nhóm người dùng thường được dùng để tập hợp những người dùng khác nhau mà cần truy nhập vào các tài nguyên chia sẻ. Như vậy việc gán quản lý người dùng và tài nguyên được thuận tiện và dễ dàng hơn. Nhóm người dùng được lưu trong file `/etc/group`, mỗi dòng

trong file có cấu trúc như sau: Tên nhóm; Mật khẩu nhóm: tùy chọn cho phép người dùng ngoài nhóm tham gia vào; Số định danh nhóm; Các thành viên.

Người quản trị có thể sử dụng các câu lệnh thêm, xóa, hay sửa thông tin người dùng và nhóm như sau:

- *useradd, userdel, usermod*: nhóm lệnh quản lý người dùng
- *groupadd, groupdel, groupmod*: nhóm lệnh quản lý nhóm
- *passwd*: thay đổi mật khẩu người dùng.

Ví dụ, để thêm người dùng *SVCNTT* vào hệ thống: *useradd SVCNTT*. Ngoài ra, người quản trị có thể sử dụng giao diện đồ họa cho các thao tác quản lý người dùng. Dưới đây là hình ảnh của bộ công cụ đi kèm theo giao diện đồ họa Ubuntu.



Hình VI-14. Giao diện thêm người dùng của Ubuntu.

VI.4.2 Quyền truy nhập

Hệ thống file của Linux/Unix cho phép cài đặt một số quyền truy nhập tới file và thư mục. Các quyền phổ biến được dùng đó là đọc (*r*), ghi (*w*) và thực thi (*x*). Ý nghĩa cụ thể của các quyền này đổi khi lệ thuộc vào đối tượng giám sát cụ thể. Để tăng cường tính an toàn, Linux/Unix bổ sung thêm ba kiểu đặc quyền hay nhóm đặc quyền. Đó là chủ sở hữu file, nhóm sở hữu file, và những người dùng còn lại. Như vậy, có thể chia nhỏ hơn quyền truy nhập tới các file và thư mục chia sẻ.

Với một file, quyền đọc thông báo cho hệ thống biết là file đó có thể đọc được từ người dùng. Quyền ghi có nghĩa là người dùng có thể thay đổi nội dung. Và quyền thực thi cho phép người dùng chạy file đó.

Với thư mục, quyền ghi thông báo cho hệ thống biết nội dung của thư mục có thể được liệt kê (xem); Quyền ghi tới thư mục là nội dung của thư mục đó có thể bị người dùng thay đổi; Quyền thực thi thư mục cho phép người dùng di chuyển vào bên trong thư mục đó.

Người dùng có thể thay đổi quyền thông qua các câu lệnh sau *chown* và *chmod*. Trong đó, *chown* cho phép thay đổi quyền sở hữu file hay thư mục và *chmod* thay đổi quyền truy nhập file hay thư mục. Câu lệnh này sử dụng ký hiệu *u* cho người dùng; *g* –nhóm của người dùng; *o*–người dùng khác; *r* – đọc; *w*–ghi; *x*–thực thi. Ngoài ra người dùng có thể dùng số *0* hay “-” thể hiện việc loại bỏ quyền và số *1* hay “+” cho việc thêm quyền.

Ví dụ, thay đổi quyền ghi vào file *passwd* qua câu lệnh

“*chmod g-w,o-r /etc/passwd*”

biểu diễn tương đương dưới dạng số

“*chmod 644 /etc/passwd*”.

Hay ví dụ khác “*chmod ug+x,o-wx file.sh*”

hay dưới dạng số “*chmod 755 file.sh*” cho phép người dùng trong nhóm được chạy *file.sh*, khác nhóm thì không được ghi và chạy.

Trong một số trường hợp người dùng cần sử dụng đặc quyền để thực thi một số thao tác quản trị, người dùng có thể sử dụng câu lệnh *su* hoặc *sudo* để có được quyền truy nhập mong muốn với điều kiện người dùng cung cấp mật khẩu hợp lệ.

VI.4.3 Danh sách kiểm soát truy nhập

Quyền truy nhập file cơ bản của Linux/Unix chỉ đủ khi hệ thống có số lượng người dùng vừa phải cũng như yêu cầu cơ bản về việc chia sẻ file. Việc sử dụng danh sách kiểm soát truy nhập ACL* giúp việc chia sẻ và giám sát truy nhập đơn giản và thuận tiện hơn. Về cơ bản, danh sách ACL cho biết những người dùng và nhóm nào có quyền gì với thư mục hay file cụ thể. ACL cho phép xác định chi tiết các quyền như chỉ người dùng *a* được phép sửa tối file *b*, còn người dùng *c* thì không có quyền gì, người dùng còn lại chỉ được đọc. Khác với kiểu truy nhập truyền thống, người dùng sở hữu file hay thư mục có khả năng gán các quyền cho người dùng khác mà không cần tới đặc quyền quản trị.

Trong Ubuntu, người quản trị có thể cài đặt gói *acl* để kích hoạt cơ chế giám sát này. Ngoài việc sử dụng câu lệnh như *chacl*, *getfacl*, và *setfacl*, người dùng có thể sử dụng giao diện đồ họa như *Eiciel* để quản lý truy nhập tới file và thư mục.

VI.4.4 Mô-đun xác thực

Nhiều ứng dụng Linux/Unix cần xác thực hay các đặc quyền theo cách này hay cách khác để truy nhập các thiết bị, file hay khởi động các chương trình sử dụng tài khoản người dùng hay nhóm nào đó. Thời kỳ đầu các ứng dụng cần xác thực sử dụng đoạn mã bên trong chương trình. Việc này rất bất tiện khi cần thay đổi hay nâng cao tính an toàn của việc xác thực. Để giải quyết vấn đề này, các kỹ sư của công ty Sun đã phát triển ý tưởng xây dựng mô-đun xác thực có thể tích hợp PAM (*Pluggable Authentication Modules*). Mô-đun này cung cấp cơ chế

* ACL – Access Control List: Danh sách kiểm soát truy nhập.

xác thực linh hoạt và mềm dẻo cho bất kỳ ứng dụng hay dịch vụ nào cần tới việc xác thực. Mô hình này đã được nhiều nhà phát triển Linux/Unix sử dụng và bổ sung.

Các ứng dụng và dịch vụ tương thích với PAM dùng các file cấu hình ở dạng văn bản để xác định và mô tả các yêu cầu xác thực cũng như các thư viện phần mềm sử dụng cho quá trình xác thực này.

PAM đáp ứng các yêu cầu xác thực khác nhau của chương trình giống như việc dùng lại các đoạn mã và thư viện dùng chung. Chẳng hạn như, chương trình đăng nhập kiểu PAM có thể kiểm tra liệu người dùng đăng nhập với đặc quyền quản trị ở đầu cuối bảo mật hay không hay hiện thời người dùng có được phép đăng nhập vào hệ thống hay không. Do PAM là các mô-đun chia sẻ nên cho phép các ứng dụng có thể cá hóa cho phù hợp với đặc điểm sử dụng của mình.

Có bốn kiểu giao tiếp với mô-đun PAM, mỗi giao tiếp tương ứng với một góc độ của quá trình xác thực:

- *auth*: dùng cho giao tiếp xác thực như yêu cầu và kiểm tra tính hợp lệ của mật khẩu.
- *account*: giao tiếp này kiểm tra xem việc truy nhập có hợp lệ hay không ví dụ như kiểm tra tài khoản người dùng có được phép đăng nhập vào thời gian cho trước hay không.
- *password*: cho phép thay đổi mật khẩu người dùng.
- *session*: giúp cấu hình và quản lý phiên làm việc của người dùng

Nhiều thư viện PAM có sẵn trong các kho phần mềm của Linux/Unix. Một số được tích hợp vào bộ công cụ như Kerberos. Để kiểm tra hay tìm kiếm trong kho phần mềm người quản trị sử dụng từ khóa *libpam*.

VI.5 Các dịch vụ của Linux/Unix

Dịch vụ là chương trình hoạt động ở chế độ nền nhằm thực hiện chức năng nhất định cho hệ thống hoặc cho người dùng. Cũng có trường hợp chương trình chỉ thực hiện một vài nhiệm vụ rồi kết thúc. Một số ví dụ về dịch vụ trong hệ thống Linux/Unix như:

- Dịch vụ nhật ký (*log*) cho phép các chương trình trong hệ thống gửi các thông báo tới một vị trí chung mà ở đó các thông báo này được phân tách và xử lý bởi công cụ nhật ký
- Dịch vụ thời gian như cung cấp thông tin về múi giờ.
- Dịch vụ Web cho phép xử lý các truy vấn trang Web.

Các đoạn mã (*script*) xử lý các dịch vụ được gọi là các đoạn mã khởi tạo và nằm trong */etc/init.d*.

VI.5.1 Dịch vụ khởi tạo

Khi hệ thống khởi động, nhân bắt đầu chạy một dịch vụ tên là *init*. Tùy thuộc theo phiên bản Linux, dịch vụ khởi tạo này dùng SysVInit, Upstart hay Systemd. Trong đó, SysVinit dựa

trên phiên bản Unix System V hỗ trợ cách thức khởi động và dừng dịch vụ dựa trên cấp độ hoạt động; Upstart phổ biến với dòng Ubuntu cải thiện việc quản lý phụ thuộc giữa các dịch vụ và nâng cao tốc độ khởi động hệ thống; Systemd là phiên bản chạy trên Fedora và là phiên bản phức tạp nhất đồng thời mềm dẻo hơn cả vì cho phép quản lý nhiều thiết bị và chức năng khác.

Dịch vụ *init* thực hiện một loạt công việc tùy theo mức độ khởi tạo của hệ thống hay còn gọi là cấp độ hoạt động (*runlevel*). Mỗi cấp độ xác định tập các dịch vụ được khởi động (hay dừng) và được phân cấp từ 0 đến 6 như sau:

- 0: Dừng;
- 1: chế độ 1 người dùng;
- 2: chế độ đa người dùng;
- 3: chế độ đa người dùng có kết nối mạng;
- 4: không sử dụng;
- 5: giống mức 3 có giao diện đồ họa;
- 6: khởi động lại.

Khi sử dụng SysVinit, người quản trị cần xây dựng các đoạn mã khởi tạo tương ứng với từng mức hoạt động và xác định dịch vụ nào cần được chạy và dịch vụ nào phải dừng. Các đoạn mã hoặc liên kết này được lưu vào trong thư mục *rc<mức hoạt động>.d*.

Với hệ thống dựa trên Upstart người quản trị có thể sử dụng công cụ như *sysv-rc-conf* hay *chkconfig* để quản lý mức độ hoạt động của các dịch vụ hoặc thông qua tiện ích *initctl*. Người quản trị có thể kiểm tra trạng thái dịch vụ, liệt kê các dịch vụ hoạt động và khởi động/đừng dịch vụ thông qua các câu lệnh:

```
initctl status <tên dịch vụ>
initctl list
initctl start|stop <tên dịch vụ>
```

Ngoài ra, người quản trị cũng có thể sử dụng câu lệnh *service* với cú pháp *service <tên dịch vụ> stop/start/restart/status* để dừng, chạy, khởi động lại, hay trạng thái của dịch vụ quan tâm.

Với hệ thống dựa trên *Systemd*, người quản trị sử dụng tiện ích *systemctl* để quản lý các dịch vụ với cú pháp tương tự như *initctl* để chạy, dừng, hay khởi động lại dịch vụ. Để cho phép hay cấm dịch vụ, người quản trị sử dụng tham số *enable* và *disable*.

VI.5.2 Các dịch vụ cơ bản

Dưới đây là một số dịch vụ cơ bản của hệ thống Linux/Unix

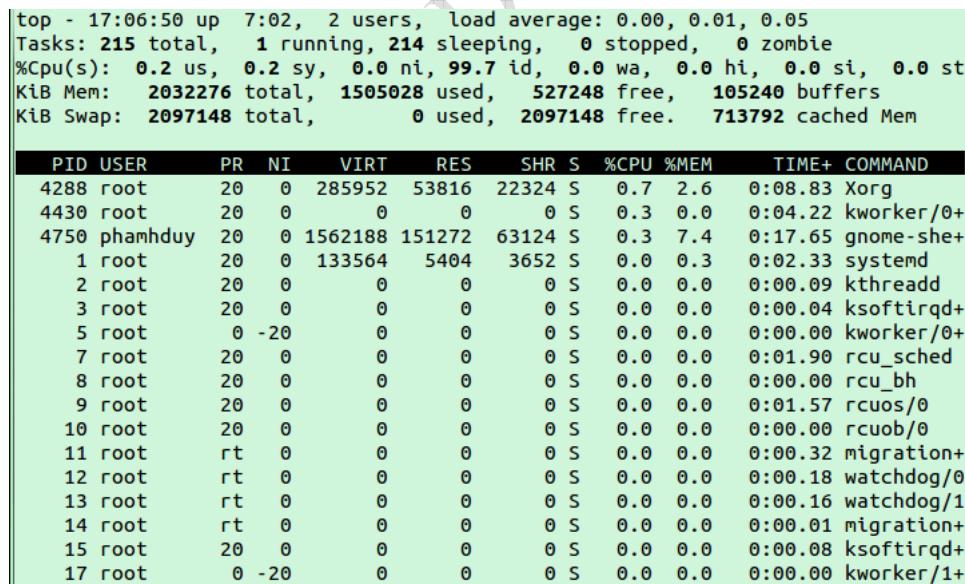
- *bootmisc*: thực hiện một số thao tác khi khởi động: như nạp thông tin từ */etc/sysctl.conf*

- *checkfs*: kiểm tra tính toàn vẹn của hệ thống file
- *inetd*: cung cấp các chức năng liên quan đến mạng như telnet,ftp
- *rsyslog*: lưu lại các sự kiện hệ thống
- *hal*: Chịu trách nhiệm khởi động dịch vụ lớp phần cứng khai thác.
- *clock*: xác lập đồng hồ hệ thống
- *keymaps*: chịu trách nhiệm quản lý các bố trí các phím
- *localmount*: cài đặt toàn bộ hệ thống file cục bộ

VI.5.3 Quản lý chương trình và dịch vụ

Hai câu lệnh hữu ích cho việc quản lý các chương trình và dịch vụ đang chạy là *ps* và *top*. Các câu lệnh này cho phép hiển thị thông tin về các chương trình đang chạy và có thể chấm dứt các chương trình không rõ nguồn gốc chạy ở chế độ nền.

Câu lệnh *top* rất giống với tiện ích quản lý tác vụ trong Windows. Câu lệnh này giám sát và cập nhật thông tin liên tục về các chương trình đang chạy trong hệ thống cũng như các tài nguyên mà chúng sử dụng.



```
top - 17:06:50 up 7:02, 2 users, load average: 0.00, 0.01, 0.05
Tasks: 215 total, 1 running, 214 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.2 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 2032276 total, 1505028 used, 527248 free, 105240 buffers
KiB Swap: 2097148 total, 0 used, 2097148 free. 713792 cached Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
4288 root 20 0 285952 53816 22324 S 0.7 2.6 0:08.83 Xorg
4430 root 20 0 0 0 0 S 0.3 0.0 0:04.22 kworker/0+
4750 phamduy 20 0 1562188 151272 63124 S 0.3 7.4 0:17.65 gnome-she+
1 root 20 0 133564 5404 3652 S 0.0 0.3 0:02.33 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.09 kthreadd
3 root 20 0 0 0 0 S 0.0 0.0 0:00.04 ksoftirqd+
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0+
7 root 20 0 0 0 0 S 0.0 0.0 0:01.90 rcu_sched
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
9 root 20 0 0 0 0 S 0.0 0.0 0:01.57 rcuos/0
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/0
11 root rt 0 0 0 0 S 0.0 0.0 0:00.32 migration+
12 root rt 0 0 0 0 S 0.0 0.0 0:00.18 watchdog/0
13 root rt 0 0 0 0 S 0.0 0.0 0:00.16 watchdog/1
14 root rt 0 0 0 0 S 0.0 0.0 0:00.01 migration+
15 root 20 0 0 0 0 S 0.0 0.0 0:00.08 ksoftirqd+
17 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1+
```

Hình VI-15. Chương trình giám sát *top*.

Hình trên cho biết kết quả giám sát việc sử dụng các tài nguyên cũng như các tham số của các chương trình đang chạy như định danh, tài khoản người dùng chạy chương trình, mức độ ưu tiên, thời gian chạy,...

Để chấm dứt chương trình đang chạy, người quản trị sử dụng lệnh *kill* với tham số là số định danh của chương trình. Tham số này có thể lấy được thông qua câu lệnh *ps* hoặc *top*.

Câu lệnh *ps* cho biết các chương trình đang chạy của người dùng với các thông tin chi tiết như định danh, người dùng, hệ số sử dụng bộ xử lý, bộ nhớ, tên lệnh ... Tuy nhiên, câu lệnh này không thể hiện các tham số trên theo thời gian thực.

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	1.0	0.2	117276	5448	?	Ss	09:04	0:02	/sbin/init
root	2	0.0	0.0	0	0	?	S	09:04	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	09:04	0:00	[ksoftirqd/0]
root	4	0.0	0.0	0	0	?	S	09:04	0:00	[kworker/0:0]
root	5	0.0	0.0	0	0	?	S<	09:04	0:00	[kworker/0:0H]
root	6	0.0	0.0	0	0	?	S	09:04	0:00	[kworker/u256:0]
root	7	0.0	0.0	0	0	?	S	09:04	0:00	[rcu_sched]
root	8	0.0	0.0	0	0	?	S	09:04	0:00	[rcu_bh]
root	9	0.0	0.0	0	0	?	S	09:04	0:00	[rcuos/0]
root	10	0.0	0.0	0	0	?	S	09:04	0:00	[rcuob/0]
root	11	0.0	0.0	0	0	?	S	09:04	0:00	[migration/0]
root	12	0.0	0.0	0	0	?	S	09:04	0:00	[watchdog/0]
root	13	0.0	0.0	0	0	?	S	09:04	0:00	[watchdog/1]
root	14	0.2	0.0	0	0	?	S	09:04	0:00	[migration/1]
root	15	0.0	0.0	0	0	?	S	09:04	0:00	[ksoftirqd/1]
root	16	0.0	0.0	0	0	?	S	09:04	0:00	[kworker/1:0]
root	17	0.0	0.0	0	0	?	S	09:04	0:00	[kworker/1:0H]

Hình VI-16. Câu lệnh *ps -aux*

Để chấm dứt chương trình người dùng đang chạy, người dùng có thể sử dụng câu lệnh *kill* với tham số *-9 định_danh_chương_trình*.

Chương VII. QUẢN TRỊ CÁC MÁY CHỦ DỊCH VỤ CỦA LINUX/UNIX SERVER

Chương này trước hết trình bày cách thức cài đặt dịch vụ quan trọng với mạng Internet là dịch vụ tên miền và tự động đặt cấu hình máy tính. Tiếp theo là các bước cài đặt dịch vụ Web, email, chia sẻ file và truy nhập từ xa. Với mỗi công việc cài đặt, sinh viên cũng được giới thiệu cách kiểm tra việc hoạt động của các dịch vụ sau khi cài đặt.

VII.1 Dịch vụ DNS và DHCP

VII.1.1 Dịch vụ DNS

DNS là dịch vụ tên miền Internet mà tạo ánh xạ từ địa chỉ Internet ra tên miền đầy đủ và ngược lại*. Máy chủ cung cấp dịch vụ DNS có thể chia thành các loại như sau:

- Máy chủ chính (*primary server*): lưu cơ sở dữ liệu về tên/địa chỉ Internet cho một vùng và chịu trách nhiệm trả lời truy vấn cho vùng đó.
- Máy chủ phụ (*secondary server*): đóng vai trò ứng cứu và chia sẻ tài cho máy chủ chính. Máy chủ phụ lấy dữ liệu từ máy chủ chính trong vùng đó và trả lời các truy vấn bên trong một miền.
- Đệm (*caching server*): lưu bản sao các truy vấn/kết quả. Máy chủ này không chứa các file cấu hình cho miền cụ thể nào.

Ubuntu cung cấp dịch vụ DNS qua gói phần mềm BIND (Berkeley Internet Naming Daemon). Phần mềm này có thể tải về và cài đặt qua câu lệnh sau

```
sudo apt-get install bind9
```

Các file cấu hình dịch vụ DNS được đặt trong thư mục */etc/bind*. Trong thư mục này, file cấu hình chính là *named.conf* và *db.root* cung cấp thông tin về máy chủ DNS gốc, và các file dữ liệu cụ thể về địa chỉ Internet/tên miền và ngược lại.

Để cài đặt máy chủ tên miền chính cho miền “*example.com*”, người quản trị cần sửa đổi file cấu hình */etc/bind/etc/bind/named.conf.local* bằng bất kỳ tiện ích soạn thảo nào như *vi*, *nano*, hay *gedit* với nội dung như sau:

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

* Chi tiết về khái niệm dịch vụ DNS có thể tham khảo tại mục III.1

Với thẻ *file* mô tả vị trí của file *db.example.com* chứa các dữ liệu về tên miền và địa chỉ Internet. Bước tiếp theo là tạo dữ liệu cho file *db.example.com* bằng cách xây dựng các bản ghi theo các cấu trúc như sau:

- *Bản ghi SOA*: bản ghi khởi đầu cho các mục khác trong file và mô tả các tham số cấu hình cơ bản như số sê-ri của dữ liệu, tên miền gốc, thời gian làm mới, thời gian đệm ...
- *Bản ghi NS*: thông báo máy chủ lưu các bản ghi cho vùng tên miền theo cấu trúc “*ns IN A địa chỉ IP*”. Ví dụ: *ns IN A 192.168.1.10*
- *Bản ghi A*: cho biết tên và địa chỉ Internet theo cấu trúc “*Tên IN A địa chỉ IP*”. Ví dụ: *www IN A 192.168.1.12*
- *Bản ghi CNAME*: tạo ánh xạ tới bản ghi A, ví dụ: *Web IN CNAME www*
- *Bản ghi PTR*: tạo ánh xạ từ địa chỉ sang tên theo cấu trúc “*Địa chỉ IP IN PTR tên_đầy đủ*”. Ví dụ: *192.168.1.2 IN PTR mail.mydomain.*

Dưới đây là file “*db.example.com*” chứa dữ liệu về địa chỉ sử dụng cho máy chủ tên miền:

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

Điều cần chú ý là số sê-ri trong bản ghi SOA được tăng lên sau mỗi lần thay đổi dữ liệu. Để việc thay đổi có hiệu lực, người quản trị cần khởi động lại dịch vụ DNS thông qua câu lệnh “*sudo service bind9 restart*”.

Để tạo cơ sở dữ liệu cho dịch vụ tra cứu địa chỉ/tên miền hay còn gọi là dịch vụ tra cứu tên miền ngược, như cho dài địa chỉ 192.168.1.*., người quản trị cần sửa đổi file cấu hình “*/etc/bind/named.conf.local*” nội dung sau:

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

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

```

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

```

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

Để kiểm tra các cài đặt dịch vụ DNS có hoạt động như mong muốn, người quản trị có thể sử dụng các câu lệnh kiểm tra sau:

- ❖ *ping*: Kiểm tra máy trạm gắn với tên miền có hoạt động hay không
 - ping my_server
- ❖ *named-checkzone*: kiểm tra dữ liệu tên
 - named-checkzone my_domain /etc/bind/db.mydomain
- ❖ *nslookup*: kiểm tra tên Internet
 - nslookup google.com

VII.1.2 Dịch vụ DHCP

Dịch vụ DHCP* (Dynamic Host Configuration Protocol) là dịch vụ mạng cho phép gán cấu hình mạng tự động cho các máy tính trong mạng. Điều này giúp cho việc triển khai và quản lý mạng được thuận tiện và nhanh chóng so với việc người quản trị phải thiết lập các tham số cho các máy tính một cách thủ công. Các điều chỉnh và sửa đổi chỉ cần thực hiện tại máy chủ cung cấp dịch vụ DHCP. Về cơ bản, thông tin cấu hình gồm có:

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

Dịch vụ DHCP có thể cung cấp một số thông tin khác như tên máy trạm, tên miền, máy chủ thời gian,...

Máy chủ dịch vụ DHCP hỗ trợ các chế độ hoạt động như sau:

- *Cấp phát tĩnh (thủ công)*: Gán thông tin cấu hình mạng không đổi cho máy trạm căn cứ vào địa chỉ vật lý của kết nối mạng mỗi khi có yêu cầu từ máy trạm
- *Cấp phát động*: Gán thông tin cấu hình mạng từ dải địa chỉ định trước trong một khoảng thời gian nhất định còn gọi là thời gian mượn địa chỉ. Khi hết hạn cấu hình này có thể được gán cho máy khác.

* DHCP – Dynamic Host Configuration Protocol: Giao thức cấu hình máy tính động

- **Cấp phát tự động:** Tự động gán cấu hình mạng cố định từ dài địa chỉ định trước cho thiết bị yêu cầu. So với phương pháp cấp phát động, thông tin cấu hình mạng không bị hết hạn.

Cài đặt dịch vụ DHCP

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

```
sudo apt-get install isc-dhcp-server
```

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

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

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

Hình VII-1. Cấu trúc thông tin cấu hình mạng của dịch vụ DHCP

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

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

```

dhcpd.leases x
# The format of this file is documented in the dhcpcd(5) man page.
# This lease file was written by isc-dhcp-4.3.1

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

```

Hình VII-2. Nội dung file nhật ký cấp phát DHCP

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

VII.2 Dịch vụ web

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

- Linh hoạt và dễ cấu hình đối với việc bổ sung các tính năng mới, các địa chỉ Web và hỗ trợ các yêu cầu tăng dần mà không phải biên dịch hay cài đặt lại
- Hỗ trợ việc xác thực để hạn chế người dùng truy nhập tới các trang hay địa chỉ Web cụ thể
- Hỗ trợ các ứng dụng tạo ra các trang Web động như Perl hay PHP (*Personal Home Page* hay *Hypertext Preprocessor*) cho phép các trải nghiệm nội dung trang Web tùy theo từng người dùng.
- Hỗ trợ liên lạc mã hóa giữa trình duyệt và dịch vụ Web để đảm bảo và xác thực an toàn cho các liên lạc này.

Phần dưới đây cung cấp các thông tin cài đặt dịch vụ máy chủ Web Apache. Đây là máy chủ Web sử dụng mã nguồn mở được triển khai nhiều nơi như Amazon, IBM. Máy chủ Web Apache hoạt động được trên nhiều hệ thống, ổn định, an toàn và linh hoạt.

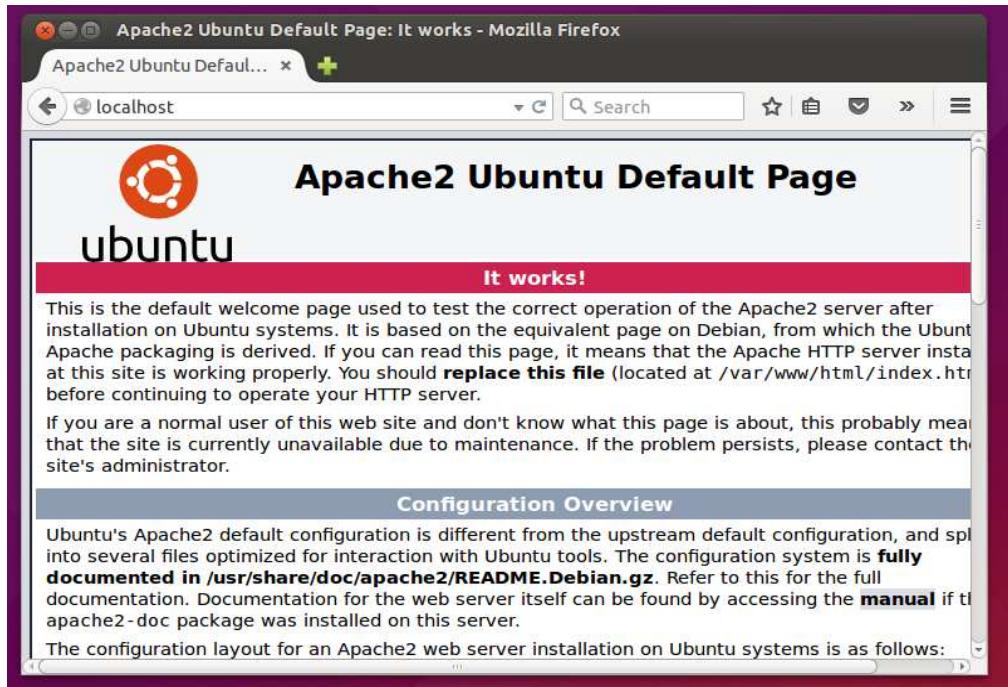
Khi khởi động Apache sử dụng quyền cao nhất (root) để đăng ký hoạt động ở cổng 80 (ngầm định cho web). Sau khi kết thúc quá trình này, máy chủ Apache hoạt động như người dùng bình thường. Việc này giúp giảm thiểu rủi ro khi bị chèn mã độc vào trang Web.

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

- *mod_cgi*: hỗ trợ Common Gateway Interface
- *mod_perl*: tích hợp trình thông dịch Perl

- *mod_aspdotnet*: cung cấp giao tiếp ASP.NET
- *mod_ftp*: hỗ trợ giao thức truyền file

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



Hình VII-3. Máy chủ Apache hoạt động trên địa chỉ cục bộ.

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

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

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

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

Nội dung của file cấu hình chứa các định nghĩa cho các tham số:

- *ServerAdmin*: khai báo địa chỉ quản trị máy chủ web
- *Listen*: địa chỉ cổng chạy trang web trong file cấu hình */etc/apache2/ports.conf*
- *ServerName*: khai báo tên máy chủ web
- *DocumentRoot*: xác định nơi chứa các file nội dung của trang web

Dưới đây là ví dụ nội dung file cấu hình

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Sau khi cài đặt thành công file cấu hình, người quản trị thực hiện các câu lệnh như sau đây để các thay đổi có hiệu lực

```
sudo a2ensite mynewsite
```

```
sudo service apache2 restart
```

Khi muốn loại bỏ địa chỉ trang Web hiện có, người quản trị thực hiện các câu lệnh sau (*mynewsite* là tên gán với địa chỉ trang Web)

```
sudo a2ensite mynewsite
```

```
sudo service apache2 restart
```

Trong trường hợp có lỗi xảy ra, người quản trị cần kiểm tra lại thông tin trong bản ghi nhật ký của dịch vụ Web được mô tả trong file cấu hình. Trong đó:

- *access.log*: cho biết toàn bộ các lần thử truy nhập vào máy chủ, liệt kê địa chỉ của máy khách, thời gian, yêu cầu cụ thể và thông tin về trình duyệt được sử dụng.
- *error.log*: cho biết toàn bộ các lỗi và mức độ cảnh báo mà dịch vụ Web gặp phải khi xử lý các yêu cầu truy nhập, bao gồm các trang không tìm thấy, các thư mục bị từ chối truy nhập.

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

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

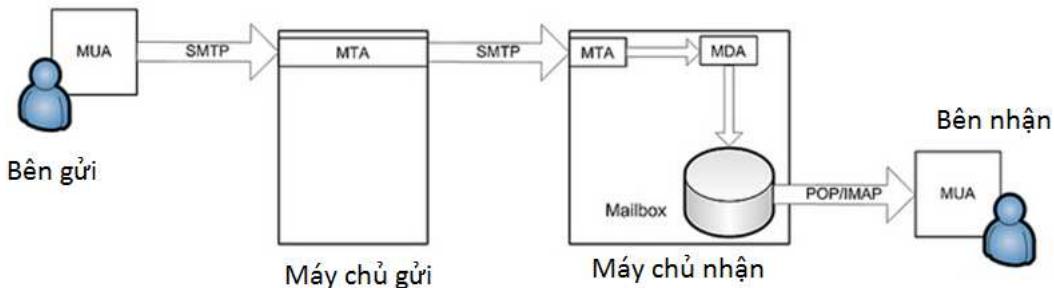
- *sửa lỗi*: các thông tin về thay đổi trạng thái của hệ thống như các file được mở, hoạt động của các máy chủ trong khi khởi động hay chạy và những thứ khác.

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

VII.3 Dịch vụ thư điện tử

VII.3.1 Giới thiệu

Thư điện tử là một trong những dịch vụ quan trọng và có tầm ảnh hưởng sâu rộng đến cách thức tương tác và thói quen làm việc của những người dùng Internet. Thư điện tử hoạt động theo nguyên tắc không đồng bộ. Người gửi có thể chuyển thư tới người nhận từ bất cứ vị trí vật lý nào miễn là có kết nối Internet. Người nhận sẽ đọc được thư khi họ kết nối vào Internet. Quá trình gửi và nhận thư cần có sự tương tác giữa các phần mềm khác nhau như trong hình dưới đây.



Hình VII-4. Quá trình gửi và nhận thư điện tử

Dịch vụ thư người dùng MUA (*Mail User Agent*) giúp người dùng tương tác với máy chủ thư điện tử, truy nhập vào hòm thư Mailbox cho phép người dùng đọc và soạn thư. Dịch vụ này kết nối với máy chủ dịch vụ thông qua các giao thức như POP (*PostOffice Protocol*) hay IMAP (*Internet Mail Access Protocol*). Các phần mềm tiêu biểu chạy trên máy tính gồm có Outlook, Thunderbird, hay Eudora. Ngoài ra, dịch vụ này có thể truy nhập thông qua Web nhờ Squirrelmail, OpenWebmail.

Dịch vụ chuyển thư MTA (*Mail Transport Agent*) xử lý việc nhận từ vị trí này sang vị trí khác trong mạng Internet bằng việc sử dụng giao thức chuyển thư đơn giản SMTP (*Simple Mail Transfer Protocol*). Phần mềm đảm nhiệm chức năng MTA có thể kể tới Microsoft Exchange, Sendmail, postfix, Exim. Thông thường dịch vụ MTA thường được coi như là dịch vụ máy chủ thư điện tử.

Dịch vụ phân phát thư MDA (*Mail Delivery Agent*) phân phát thư tới hòm thư của người dùng khi có thư được chuyển đến. Để đảm bảo an toàn cho việc sử dụng thư điện tử, MDA còn thực hiện các chức năng lọc thư rác hay quét mã độc được đính kèm theo thư. MDA tương tác với người dùng thư điện tử thông qua các giao thức truy nhập hòm thư như POP hay

IMAP. Bộ phần mềm thực hiện chức năng có thể kể đến Courier, Dovecot, Cyrus. Trên thực tế, các tính năng của MDA và MTA có thể được tích hợp vào một hệ thống duy nhất như trường hợp của Microsoft Exchange.

VII.3.2 Các giao thức

Giao thức tiêu chuẩn cho việc truyền thư điện tử qua mạng Internet là SMTP (*Simple Mail Transfer Protocol*) hoạt động trên cổng 25. Người dùng chuyển thư điện tử tới máy chủ bằng giao thức SMTP sau đó máy chủ thư điện tử xử lý việc chuyển tiếp tới người nhận. Các gói phần mềm hỗ trợ Postfix, Exim, Microsoft Exchange. Các câu lệnh truy vấn được thực hiện qua giao thức SMTP gồm có

HELO: Helo mydomain.vn; kết nối tới máy chủ dịch vụ

MAIL FROM: ; địa chỉ người gửi

RCPT TO: ;địa chỉ người nhận

DATA: thông điệp của thư

QUIT:; ngắt kết nối với máy chủ dịch vụ

Máy chủ thư điện tử nhận và lưu thư điện tử cho người dùng. Để lấy thư điện tử từ máy chủ dịch vụ, người dùng cần sử dụng giao thức POP hay IMAP. Giao thức POP hoạt động trên cổng 110 giúp tải các thư điện tử của người dùng từ hàng đợi của máy chủ thư điện tử về. Thông thường POP lấy hết thư từ máy chủ dịch vụ về máy tính của người dùng. Gói phần mềm hỗ trợ giao thức POP gồm có *courier-pop* và *dovecot-pop3d*. Câu lệnh đăng nhập vào máy chủ dịch vụ qua POP gồm có:

USER: tên đăng nhập hòm thư của người dùng

PASS: mật khẩu đăng nhập

IMAP có chức năng tương tự như POP và hoạt động trên cổng 143. Điểm khác biệt là IMAP tạo các bản sao thư trên máy người dùng và đồng bộ lại với máy chủ khi người dùng kết nối vào mạng. Thông thường có các chế độ hoạt động như sau:

- *Chế độ trực tuyến (online)*: người dùng truy nhập trực tiếp tới hòm thư của mình
- *Chế độ không trực tuyến (off-line)*: giống như giao thức POP, người dùng tải email về và ngắt kết nối với máy chủ.
- *Chế độ không nối mạng*: người dùng làm việc trên các bản sao. Các bản sao này được đồng bộ với hòm thư trên máy chủ khi nối mạng.

Gói phần mềm hỗ trợ gồm có *courier-imap*, *uw-imap*, *dovecot-imapd*. Người dùng có thể sử dụng các câu lệnh LOGIN, LIST, hay LOGOUT để làm việc với máy chủ dịch vụ.

VII.3.3 Cài đặt

Postfix là bộ phần mềm máy chủ dịch vụ thư điện tử trong môi trường Ubuntu. Phần mềm này chịu trách nhiệm MTA, nghĩa là gửi thư của người dùng qua các máy chủ khác nhau

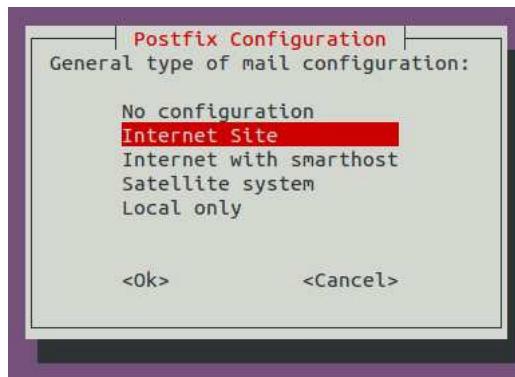
trong mạng Internet. Cài đặt phần mềm này được thực hiện thông qua câu lệnh quản lý các gói phần mềm như sau

```
sudo apt-get install postfix
```

Để sửa đổi các cấu hình cho bộ phần mềm này sử dụng câu lệnh

```
sudo dpkg-reconfigure postfix
```

Các thông tin cần thiết cho việc cài đặt dịch vụ gồm có kiểu dịch vụ, tên máy chủ dịch vụ, tên miền, thư mục chứa thư, thông tin về mạng cục bộ, giao thức Internet. Việc cấu hình được thực hiện qua giao diện đồ họa nên dễ dàng cho người quản trị.



Hình VII-5. Chọn kiểu dịch vụ cài đặt của Postfix.

Mặt khác, người quản trị có thể cấu hình thông qua file cấu hình */etc/postfix/main.cf* với các tham số minh họa như dưới đây:

- Myhostname=my_server.mydomain
- Mydomain= tên miền
- Myorigin=\$mydomain;
- Mail_spool_directory=/var/spool/mail; thư mục chứa thư
- Mynetwork=192.168.0.0/24

Dịch vụ thư điện tử có thể được kích hoạt hay kiểm tra trạng thái qua câu lệnh đặc quyền:

```
sudo service postfix restart/start/stop/status
```

Người quản trị có thể kiểm tra cài đặt qua việc xem xét file nhật ký */var/log/mail.log* hay sử dụng câu lệnh *telnet* để kết nối tới máy chủ dịch vụ và chạy các câu lệnh SMTP.

```
pduy@ux64NoGui:~$ telnet smtp.attt.ptit.edu.vn
Trying 10.0.0.2...
telnet: Unable to connect to remote host: Connection refused
pduy@ux64NoGui:~$ telnet smtp.attt.ptit.edu.vn 25
Trying 10.0.0.2...
Connected to smtp.attt.ptit.edu.vn.
Escape character is '^].
220 ux64NoGui ESMTP Postfix (Ubuntu)
```

Hình VII-6. Telnet tới máy chủ dịch vụ không thành công.

Để người dùng có thể lấy được thư về máy cá nhân, cần cài đặt dịch vụ POP hay IMAP. Trong Ubuntu, các dịch vụ này có thể được cài đặt qua câu lệnh

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

Thông tin đặt cấu hình được lưu trong file `/etc/dovecot/dovecot.conf`. Tham số quan trọng cần cài đặt là vị trí hòm thư người dùng `mail_location = maildir:~/Maildir`.

Để kiểm tra việc hoạt động của POP và IMAP người quản trị dùng `telnet` để kết nối và chạy các câu lệnh truy vấn máy chủ dịch vụ như đăng nhập.

```
pduy@ux64NoGui:~$ telnet pop.attt.ptit.edu.vn 110
Trying 10.0.0.2...
Connected to pop.attt.ptit.edu.vn.
Escape character is '^>'.
+OK Dovecot (Ubuntu) ready.
user pduy
+OK

```

Hình VII-7. Câu lệnh USER qua telnet tới máy chủ dịch vụ.

Để đọc thư trên máy tính của người dùng cá nhân, cần cấu hình phần mềm MUA với các tham số của hệ thống thư điện tử bao gồm tên và giao thức hoạt động của các máy chủ dịch vụ SMTP, POP, và IMAP như được cấu hình.

Account name
courier

Your name
Courier Mail

We'll send your messages using this name.

Incoming email server
pop.attt.ptit.edu.vn

Account type
POP3

User name
courier

Examples: kevinc, kevinc@contoso.com, domain\kevinc

Password

Outgoing (SMTP) email server
smtp.attt.ptit.edu.vn

Outgoing server requires authentication

Use the same user name and password for sending email

Require SSL for incoming email

Require SSL for outgoing email

Hình VII-8. Cấu hình phần mềm thư điện tử Outlook Express

Hình VII-8 giới thiệu cấu hình cho người dùng phần mềm thư điện tử Outlook Express của hệ điều hành Windows 10.

VII.4 Dịch vụ file và in ấn

VII.4.1 Dịch vụ truyền file FTP

Giao thức truyền file FTP (File Transfer Protocol) là giao thức cho phép tải các file giữa các máy tính nối mạng Internet. Giao thức này không hỗ trợ các cơ chế bảo vệ dữ liệu và định danh người dùng trong quá trình truyền. Vì vậy phương pháp này chỉ phù hợp để trao đổi các file dùng chung như các file phần mềm.

FTP hoạt động theo cơ chế chủ/khách và sử dụng hai cổng: cổng 21 dùng để điều khiển (lệnh); cổng 20 dùng cho trao đổi dữ liệu. Phần chạy trên máy chủ được gọi là nhân FTP (*FTP daemon*) làm nhiệm vụ lắng nghe các yêu cầu tải file từ các máy khách. Máy chủ dịch vụ FTP hỗ trợ hai chế độ hoạt động:

- *Nặc danh (Anonymous)*: Người dùng không cần mật khẩu. Sử dụng tài khoản ngầm định anonymous
- *Xác thực (Authenticated)*: Người dùng phải có tài khoản và mật khẩu để truy nhập.

Việc cài đặt trên Ubuntu được thực hiện qua câu lệnh

```
sudo apt-get install vsftpd
```

Ở chế độ ngầm định các thư mục chia sẻ file ngầm định đặt tại /svr/ftp. Các thông tin cấu hình chi tiết cho dịch vụ này được lưu trong file /etc/vsftpd.conf. Các cấu hình cơ bản bao gồm:

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

Để sử dụng dịch vụ FTP, người dùng cần chương trình khách *ftp* hoặc các chương trình sử dụng giao diện đồ họa khác. Để kết nối người dùng dùng câu lệnh *ftp tên_máy_chủ_dịch_vụ*. Ở chế độ dòng lệnh người dùng sử dụng các câu lệnh sau:

- Mở đóng kết nối: *open/close*
- Thoát chương trình: *bye*
- Tải file về: *get, mget*
- Nạp file lên máy chủ: *put, mput*

VII.4.2 Dịch vụ file mạng NFS

Dịch vụ NFS (*Network File System*) là dịch vụ chia sẻ file trong môi trường Linux/Unix. Dịch vụ này cho phép người dùng sử dụng file/thư mục trên máy tính mạng giống như trong ổ đĩa cục bộ. Dịch vụ NFS hoạt động theo mô hình chủ/khách trong đó:

- Máy chủ chia sẻ thư mục /shared
- Máy khách truy nhập vào thư mục chia sẻ trên máy chủ server:/shared qua câu lệnh *mount*

Ưu điểm của dịch vụ NFS là cho phép tiết kiệm không gian lưu trữ trên các máy trạm nhờ vào việc cất giữ các dữ liệu dùng chung lên máy chủ mà truy cập được qua mạng. Người dùng không cần phải có thư mục gốc (home) riêng biệt trên các máy trạm. Câu lệnh dưới đây cài đặt dịch vụ NFS:

```
sudo apt-get install nfs-kernel-server
```

Để khởi động, dừng hay kiểm tra trạng thái dịch vụ người quản trị có thể dùng câu lệnh **sudo service nfs-kernel-server start/restart/stop/status**

Cấu hình thư mục/file chia sẻ được thực hiện thông qua việc thay đổi các dòng trong file */etc/export*. Mỗi dòng mô tả thư mục/file được chia sẻ theo dạng *Thư_mục_chia_sẻ client|ip (quyền)*. Dưới đây là ví dụ chia sẻ thư mục *home* cho tất cả các máy trong mạng.

```
/home * (rw,sync,no_root_squash)
```

Các quyền truy nhập gồm có:

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

Cần khởi động lại dịch vụ NFS mỗi khi thay đổi cấu hình qua câu lệnh **sudo service nfs-kernel-server restart**.

Từ phía người dùng hay máy khách, cần sử dụng câu lệnh *mount* để liên kết thư mục chia sẻ của NFS với thư mục trên máy của người dùng theo dạng

```
sudo mount Máy_chủ:/thư_mục_chia_sẻ /local/thư_mục_chia_sẻ
```

VII.4.3 Quản lý máy in

Dịch vụ CUPS (*Common UNIX Printing System*) cung cấp dịch vụ in ấn và quản lý in cho người dùng sử dụng giao thức chuẩn in ấn Internet (*Internet Printing Protocol*). Dịch vụ CUPS cũng hỗ trợ việc tự động phát hiện các máy in mạng và cung cấp các công cụ quản trị và đặt cấu hình đơn giản qua Web.

CUPS được cài qua gói quản lý phần mềm nhờ câu lệnh **sudo apt-get install cups**. Các thông tin cấu hình CUPS được lưu trong file */etc/cups/cupsd.conf*. Các cấu hình cơ bản gồm có:

- Địa chỉ quản trị: *ServerAdmin địa chỉ_email_quản_trị*
- Cổng hoạt động: *Listen 192.168.1.2:631*
- Cho phép sử dụng dịch vụ: *Allow from 192.168.0.**
- Từ chối dịch vụ: *Deny from all*

Ngoài ra người quản trị có thể cấu hình thông qua giao diện Web tại địa chỉ ngầm định <http://localhost:631/admin>.

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

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

VII.5 Dịch vụ truy nhập từ xa

Telnet là công cụ truyền thống cho phép thực thi các câu lệnh trên máy chủ từ xa qua mạng trong môi trường Unix. Tuy nhiên, dữ liệu của telnet truyền dưới dạng văn bản không được mã hóa nên không đảm bảo an toàn cho người dùng.

OpenSSH là phiên bản miễn phí của dịch vụ truy nhập bảo mật SSH (*Secure Shell*) cung cấp công cụ hữu hiệu cho việc truy nhập máy chủ Linux/Unix qua mạng. SSH dựa trên cơ chế mã hóa khóa công khai để đảm bảo việc xác thực người dùng và trao đổi khóa bí mật giúp chống lại việc xâm phạm dữ liệu trao đổi trên đường truyền Internet.

OpenSSH bao gồm hai phần:

- Ứng dụng hoạt động trên máy chủ chờ yêu cầu kết nối từ người dùng
- Ứng dụng trên máy khách: gửi yêu cầu kết nối tới máy chủ

Trong Ubuntu việc cài đặt ứng dụng trên máy chủ và máy khách được thực hiện qua câu lệnh sau

```
sudo apt-get install openssh-server  
sudo apt-get install openssh-client
```

Thông tin cấu hình được lưu trong file */etc/ssh/sshd_config*. Các tham số cấu hình tiêu biểu như sau:

- Áp dụng xác thực mã khóa công khai: *PubkeyAuthentication yes*
- Hiện thông báo trong file *issue.net* khi đăng nhập: *Banner /etc/issue.net*
- Hoạt động trên địa chỉ: *ListenAddress 10.0.0.2*
- Cho phép người dùng sử dụng SSH: *AllowUsers tên_người_dùng*
- Cấm người dùng sử dụng SSH: *DenyUsers tên_người_dùng*

Bước tiếp theo người dùng cần tạo khóa công khai và bí mật để sử dụng trong dịch vụ SSH qua câu lệnh

```
ssh-keygen -t rsa
```

Khóa sinh ra gồm khóa công khai và bí mật và được lưu trong thư mục của người dùng. Trong đó, khóa công khai tại *~/.ssh/id_rsa.pub* còn khóa bí mật tại *~/.ssh/id_rsa*. Để sử dụng khóa công khai trong quá trình xác thực, người dùng cần chép khóa vào máy chủ qua câu lệnh theo dạng như dưới đây

```
ssh-copy-id tên_người_dùng@máy_chủ_ssh
```

Nếu quyền truy nhập vào file chứa khóa xác thực chưa phù hợp thì phải cập nhật lại theo câu lệnh

chmod 600 .ssh/authorized_keys

Hình dưới đây hiển thị phiên làm việc với máy chủ Ubuntu qua giao tiếp kết nối SSH.

```
Login as: pduy
Ubuntu 15.04
Phien lien lac SSH
pduy@ssh.attt.ptit.edu.vn's password:
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
 
 System information as of Thu Sep 17 09:27:10 ICT 2015

 System load:  0.09          Users logged in:      1
 Usage of /:   11.5% of 38.02GB  IP address for eth0: 10.0.0.1
 Memory usage: 41%           IP address for eth1: 10.0.0.2
 Swap usage:   0%            IP address for eth2: 10.0.0.50
 Processes:    290

 Graph this data and manage this system at:
 https://landscape.canonical.com/
 
Last login: Thu Sep 17 08:56:16 2015 from 10.0.0.2
pduy@ux64NoGui:~$ █
```

Hình VII-9. Màn hình kết nối từ xa sử dụng SSH

Chương VIII. BẢO TRÌ, KHẮC PHỤC LỖI VÀ GIÁM SÁT HOẠT ĐỘNG CỦA LINUX/UNIX

Chương này giúp sinh viên làm quen với các nhiệm vụ đảm bảo hệ thống hoạt động an toàn và ổn định. Mở đầu chương giới thiệu các cách thức giúp cài đặt các bản vá và cập nhật của hệ điều hành. Phần kế tiếp trình bày cách tiếp cận để xử lý sự cố trong quá trình vận hành hệ thống và các công cụ giúp theo dõi các chương trình và người dùng hoạt động trong hệ thống. Cuối cùng là các công cụ hỗ trợ quản trị từ và ngôn ngữ lập trình *shell*.

VIII.1 Cập nhật các bản vá

Trong quá trình hoạt động và vận hành hệ thống, người quản trị liên tục phải tiến hành việc cập nhật các phần mềm ứng dụng cũng như hệ thống. Việc này cần thiết do các phần mềm đều có chu kỳ thay đổi nhất định. Khi này, các phần mềm thường sẽ được bổ sung các tính năng mới và sửa chữa những vấn đề mắc phải xuất hiện trong quá trình sử dụng. Ngoài ra, các hãng và công ty sản xuất phần mềm thường xuyên thực hiện các sửa chữa phần mềm nhằm đối phó với các lỗ hổng hay vấn đề tương thích với các phần mềm khác. Việc này nhằm giảm thiểu các rủi ro về an toàn và bảo mật cho chương trình và đảm bảo các phần mềm hoạt động ổn định.

Ở góc độ kỹ thuật, việc quản lý các thay đổi phần mềm trong Linux/Unix có thể được thực hiện từ:

- *Mã nguồn*: đây là cách thức truyền thống. Người dùng thực hiện việc biên dịch và cài đặt phần mềm theo các hướng dẫn đi kèm trong gói phần mềm cập nhật.
- *Gói quản lý phần mềm RPM (Redhat Package Manager)*: đây là công cụ quản lý phần mềm phổ biến cho các phiên bản Linux dựa trên RedHat
- *Hệ thống quản lý phần mềm DPMS (Debian Package Management System)*: dùng cho các phiên bản Linux dựa trên Debian.

Việc sử dụng mã nguồn cho việc cập nhật đòi hỏi người quản trị có hiểu biết chắc chắn về các thư viện mà bản cập nhật sẽ sử dụng như vị trí lưu trữ và việc chia sẻ với các phần mềm khác. Mặt khác, người quản trị cũng cần nắm vững cách thức cấu hình cho việc biên dịch và cài đặt. Các thông tin này thường được nhúng trong file *make*. Trong khi cài đặt, người quản trị sẽ phải đối phó với tình huống như mã nguồn bị lỗi hay thiếu thư viện làm cho việc biên dịch không thành công.

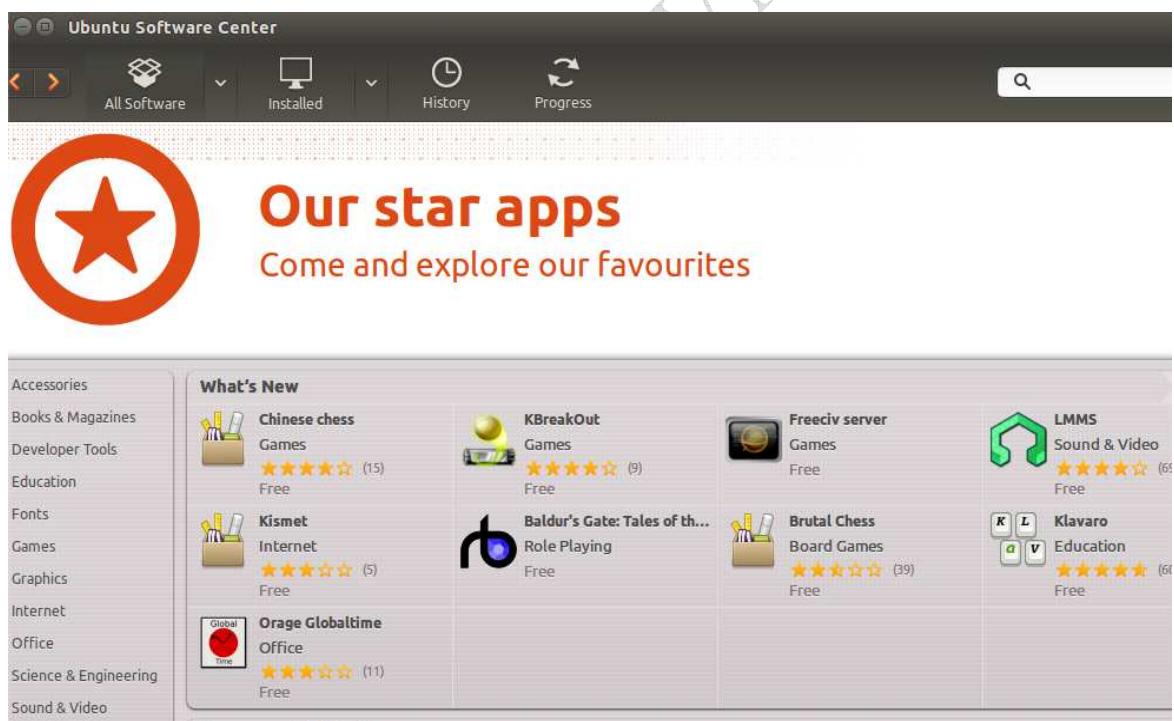
Gói quản lý phần mềm như RPM hay DPMS giảm thiểu gánh nặng cho người quản trị và làm cho quá trình cập nhật được dễ dàng và thuận tiện hơn. DPMS cung cấp câu lệnh *dpkg* cho phép người dùng Linux nắm được các phần mềm đã được cài đặt cũng như thực hiện các thao tác cài đặt phần mềm:

- Liệt kê các gói phần mềm được cài đặt: `dpkg -l`
- Liệt kê các file được cài đặt bởi một gói phần mềm: `dpkg -L phần_mềm`
- Liệt kê gói phần mềm cài đặt file `dpkg -S /etc/hosts.conf`
- Cài đặt gói phần mềm: `sudo dpkg -i phần_mềm.deb`
- Gỡ bỏ gói phần mềm: `sudo dpkg -r phần_mềm`

Mặt khác, người dùng Ubuntu có thể tương tác với các gói phần mềm được quản lý trên nền `dpkg`. Người dùng Ubuntu có thể sử dụng các câu lệnh sau để quản lý việc cập nhật các phần mềm:

- Cài đặt gói phần mềm: `sudo apt-get install phần_mềm`
- Gỡ bỏ phần mềm: `sudo apt-get remove phần_mềm`
- Cập nhật thông tin về kho phần mềm: `sudo apt-get update`
- Nâng cấp gói phần mềm: `sudo apt-get upgrade`

Ngoài giao diện dòng lệnh, người dùng Ubuntu có thể thực hiện việc cập nhật và sửa đổi các phần mềm qua giao diện đồ họa của Trung tâm phần mềm Ubuntu (*Ubuntu Software Center*).



Hình VIII-1. Trung tâm phần mềm Ubuntu.

Để thuận tiện cho người quản trị, các phần mềm có thể được cài đặt cho việc tự động cập nhật hay cảnh báo cho người dùng về các bản sửa chữa hay cập nhật mới như trong hình dưới đây.



Hình VIII-2. Lựa chọn tự động hóa cập nhật.

Qua giao diện, người có thể lựa chọn các phần cập nhật theo mức độ quan trọng của bản cập nhật, thực hiện việc kiểm tra theo các chu kỳ khác nhau như ngày hay tuần cũng như cách thức thông báo về các bản cập nhật.

VIII.2 Sao lưu và khôi phục dự phòng

Thực hiện sao lưu là trách nhiệm tối quan trọng đối với bất kỳ người dùng thông thường và đặc biệt với quản trị hệ thống. Khi tiến hành sao lưu người quản trị cần quan tâm tới một số vấn đề sau:

- *Khối lượng dữ liệu.* Đây luôn là thách thức với người quản trị do nhu cầu và tình hình phát triển của cơ quan/tổ chức mà khối lượng dữ liệu biến động. Ngoài ra tần suất và khối lượng biến động dữ liệu có thể thay đổi tùy theo thời điểm hoạt động. Một khía cạnh khác của dữ liệu cũng là vấn đề khó khăn khi thực hiện sao lưu như dữ liệu cá nhân hay của nhóm, dữ liệu có nén hay không.
- *Phản ứng và phương tiện sao lưu.* Tính chất vật lý của các phương tiện sao lưu ảnh hưởng tối quyết định hay tổ chức thực hiện sao lưu. Các đĩa DVD hay Bluray có chi phí thấp song tuổi thọ ngắn; Ổ cứng hay ổ đĩa theo kiểu RAID có tốc độ cao song chi phí cao hơn; Các ổ đĩa mạng lệ thuộc vào hạ tầng mạng.
- *Năng lực (bandwidth) mạng.* Để đảm bảo băng thông chung của hệ thống khi sao lưu không nên sao lưu hai máy tính trong cùng một phân đoạn mạng.
- *Tốc độ và khả năng khôi phục dữ liệu.* Sao lưu vào ổ cứng cho tốc độ cao hơn so với các phương tiện lưu trữ tháo lắp như đĩa DVD. Tuy nhiên với các thao tác như khôi phục phần mềm hệ thống như hệ điều hành của máy tính thì việc thực hiện

trên đĩa DVD lại thuận tiện hơn. Thêm vào đó, người dùng bình thường cũng sẽ dễ dàng sử dụng đĩa DVD hơn là ổ cứng.

Từ dòng lệnh người quản trị có thể dùng lệnh *dump* và *restore* để thực hiện việc sao lưu/khôi phục toàn bộ hệ thống file Linux. Lệnh *dump* thực hiện sao lưu tăng dần và sử dụng tham số *cấp độ sao lưu* từ 0 đến 9 như sau:

- *Cấp 0*: sao lưu toàn bộ
- *Cấp 1*: sao lưu bổ sung so với cấp 0
- *Cấp 9*: cấp cao nhất

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

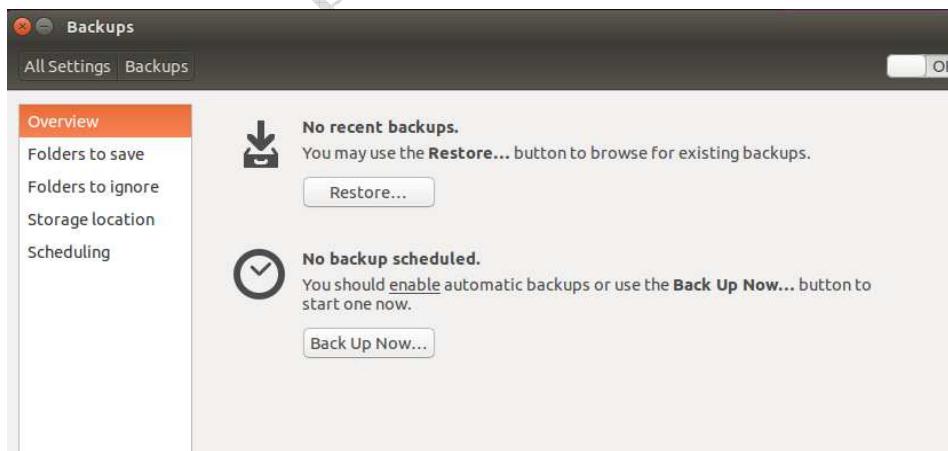
```
dump -0 -f /dev/sdb1 /dev/sda1
```

Lệnh *restore* đọc file tạo ra từ phần mềm *dump* và trích ra các file và thư mục tùy theo tham số được sử dụng. Các tham số tiêu biểu như sau

- *-i*: Chế độ tương tác. Phần mềm cung cấp giao diện cho phép người quản trị lựa chọn thư mục và file để khôi phục
- *-r*: Khôi phục lại hệ thống file
- *-f tên_file*: Đọc từ file sao lưu
- *-v*: Hiển thị kết quả khôi phục

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

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



Hình VIII-3. Giao diện đồ họa cho việc sao lưu và khôi phục.

Qua giao diện, người dùng có thể xác định nội dung cần được sao lưu cũng như thực hiện việc sao lưu tới các ổ đĩa cục bộ cũng như qua mạng. Nội dung sao lưu có thể được bảo vệ qua việc sử dụng mật khẩu. Việc sao lưu có thể được tiến hành tự động theo thời gian người dùng xác định.

Ngoài ra, còn có các bộ phần mềm sao lưu và khôi phục với các tính năng đa dạng và phong phú khác hoạt động trên môi trường Linux. AMANDA (*Advanced Maryland Automatic Network Disk Archiver*) là hệ thống sao lưu cho phép dùng một máy chủ sao lưu để sao lưu nhiều máy qua mạng vào ổ đĩa hay băng từ hay ổ quang.

Dirvish là hệ thống sao lưu ra đĩa cứng viết bằng ngôn ngữ Perl sử dụng tiện ích sao lưu của Linux. Hệ thống này thuận tiện cho việc tự động hóa sao lưu và dễ dàng khôi phục lại và thích hợp cho việc sao lưu file và thư mục.

The screenshot shows the BackupPC Server Status interface. On the left, there's a sidebar with links like 'Hosts', 'Status', 'Admin Options', etc. The main area has three sections: 'General Server Information' (listing server PID, status generation time, configuration load time, and PC queueing details), 'Currently Running Jobs' (a table header with columns Host, Type, User, Start Time, Command, PID, Xfer PID), and 'Failures that need attention' (a table header with columns Host, Type, User, Last Try, Details, Error Time, Last error (other than no ping)).

Hình VIII-4. Giao diện màn hình làm việc chính BackupPC.

BackupPC hỗ trợ sao lưu cho Linux ra ổ cứng trên máy chủ sử dụng giao diện Web. BackupPC cho phép sao lưu file và thư mục. Để tăng khả năng sao lưu, BackupPB sử dụng giải pháp nén đĩa để tăng khả năng sao lưu.

VIII.3 Khắc phục các sự cố

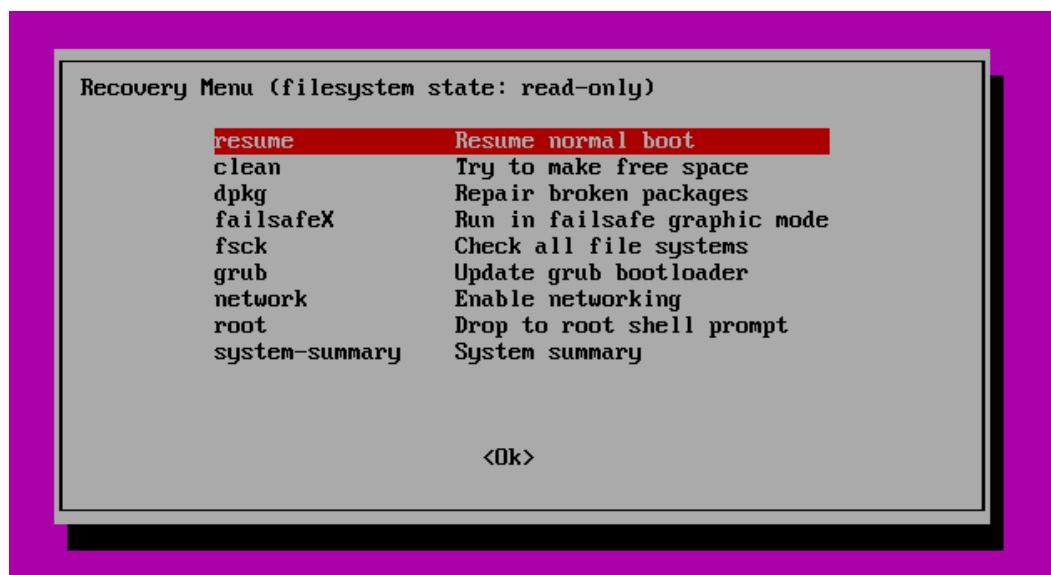
Trong quá trình cài đặt và vận hành hệ thống Linux/Unix, người quản trị có thể gặp phải nhiều vấn đề khiến cho việc triển khai phần mềm không được thuận lợi. Để hạn chế tình trạng này và giúp cho việc khắc phục, người quản trị cần có kế hoạch triển khai đầy đủ và rõ ràng. Tuy nhiên, khi xảy ra tình trạng lỗi cần ghi nhận tình trạng lỗi một cách đầy đủ nhất bằng cách đơn giản như dùng trình soạn thảo văn bản hay chép màn hình để ghi lại các thông báo lỗi hay các cảnh báo của hệ thống và các phần mềm.

Ngoài ra, người quản trị có thể tìm kiếm thông tin về tình trạng hoạt động trong các file nhật ký. Các file này thường được lưu trữ trong thư mục `/var/log`. Với mỗi ứng dụng cụ thể, người quản trị đều có thể yêu cầu chương trình ghi lại tình trạng hoạt động với các mức độ khác nhau. Người quản trị có thể sửa đổi cấu hình này để kiểm tra nguyên nhân khi chương trình hoạt động không ổn định.

Bên cạnh đó, quá trình sử dụng của người dùng cũng thường được lưu lại trong các file như *.bash_history* và *.xsession*. Các file này cung cấp thông tin cụ thể về phiên làm việc của người dùng.

Sau khi có thông tin về tình trạng lỗi, người quản trị có thể tìm kiếm giải pháp xử lý thông qua các trang mạng của nhà sản xuất như *help.ubuntu.com* hay các trang cộng đồng. Các trang này thường được cập nhật và cung cấp các biện pháp xử lý một cách liên tục. Sau khi lựa chọn giải pháp, người quản trị cần lên chi tiết các bước thực hiện nhằm tránh tình trạng gây hư hỏng thêm và không thẩm tra được việc sửa chữa và khắc phục lỗi.

Đĩa cài Ubuntu cung cấp công cụ cho phép kiểm tra. Công cụ này cho phép người quản trị truy nhập tạm thời vào hệ thống file và thực hiện một số thao tác kiểm tra và sửa lỗi cơ bản như lỗi lô-gíc của hệ thống file, cập nhật lại gói phần mềm bị lỗi, khởi động hệ thống ở chế độ tối thiểu... như trong hình dưới đây.



Hình VIII-5. Các chức năng khắc phục lỗi cơ bản.

VIII.4 Giám sát hoạt động và kiểm toán

Với dịch vụ máy chủ, điều quan trọng với người quản trị là duy trì tình trạng hoạt động ổn định. Tuy nhiên, trong quá trình vận hành các dịch vụ máy chủ sẽ có thể bị trục trặc và tạm dừng. Khi việc này sẽ hay sắp xảy ra, người quản trị cần phải được cảnh báo hay dự đoán trước để có biện pháp xử lý. Các công cụ giám sát và kiểm toán không chỉ giúp người quản trị được thông báo kịp thời về tình trạng chung của hệ thống mà còn có thông tin chính xác để khắc phục hay giúp cho các dịch vụ và hệ thống hoạt động được đảm bảo hơn.

VIII.4.1 Giám sát

Các file nhật ký cung cấp thông tin về tình trạng hoạt động chung của các dịch vụ và hệ thống máy chủ và được lưu trong thư mục "*var/log/*" như

- *syslog*: nhật ký về hoạt động chung của hệ thống

- *mail*: nhật ký về hệ thống thư điện tử

Dưới đây là ví dụ về thông tin lưu trong file nhật ký hệ thống.

```
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] KERNEL supported cpus:
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] Intel_GenuineIntel
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] AMD_AuthenticAMD
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] Centaur_CentaurHauls
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] Disabled fast string operations
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] e820: BIOS-provided physical RAM map:
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x0000000000000000-0x00000000000e7fff] usable
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x00000000000e800-0x00000000009ffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x0000000000dc000-0x0000000000fffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x0000000000100000-0x000000007fedffff] usable
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x00000000007fe0000-0x000000007fefefff] ACPI data
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x00000000007fef0000-0x000000007feffffff] ACPI NVS
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x00000000007ff0000-0x000000007fffffff] usable
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x0000000000f00000-0x00000000f7fffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x000000000fec0000-0x00000000fec0ffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x000000000fee0000-0x00000000fee0ffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] BIOS-e820: [mem 0x000000000ffe0000-0x00000000ffe0ffff] reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] NX (Execute Disable) protection: active
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] SMBIOS 2.7 present.
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS
6.00 07/02/2015
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] Hypervisor detected: VMware
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Oct 14 10:01:53 ux64NoGui kernel: [ 0.00000] e820: remove [mem 0x000a0000-0x000fffff] usable
```

Hình VIII-6. Nhật ký hệ thống

Bên cạnh đó Linux/Unix cung cấp một số công cụ cho phép theo dõi tình trạng sử dụng các tài nguyên hệ thống của các chương trình và dịch vụ qua các câu lệnh:

- *ps*: liệt kê các chương trình đang hoạt động và số lượng tài nguyên hệ thống chúng sử dụng
- *df*: cho biết dung lượng lưu trữ đã được sử dụng trong hệ thống
- *netstat*: cho biết thông tin về các cổng và các giao thức mạng đang hoạt động của hệ thống

Active Internet connections (servers and established)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:47788	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:110	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:143	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:40179	0.0.0.0:*	LISTEN
tcp	0	0	192.168.1.13:53	0.0.0.0:*	LISTEN

Active UNIX domain sockets (servers and established)						
Proto	RefCount	Flags	Type	State	I-Node	Path
unix	2	[ACC]	STREAM	LISTENING	22527	/var/run/dovecot/indexer
unix	2	[ACC]	STREAM	LISTENING	24577	/var/run/dovecot/login/imap
unix	2	[ACC]	STREAM	LISTENING	24579	/var/run/dovecot/imap-urlauth-worker
unix	2	[ACC]	STREAM	LISTENING	26117	/run/user/1000/keyring/gpg
unix	2	[ACC]	STREAM	LISTENING	24581	/var/run/dovecot/token-login/imap-urlauth
unix	2	[ACC]	STREAM	LISTENING	27190	@/tmp/.ICE-unix/2487
unix	2	[ACC]	STREAM	LISTENING	24583	/var/run/dovecot/imap-urlauth
unix	2	[ACC]	STREAM	LISTENING	26125	/run/user/1000/keyring/pkcs11
unix	2	[ACC]	STREAM	LISTENING	24589	/var/run/dovecot/doveadm-server

Hình VIII-7. Kết quả của câu lệnh *netstat*

Ngoài ra, *sysstat* là công cụ giám sát hiệu năng tốt cho môi trường Linux. Công cụ này cho phép ghi lại các thông kê tình trạng hệ thống tiêu biểu như :

- Tài của bộ xử lý
- Thao tác vào/ra và tốc độ truyền theo từng chương trình, ổ đĩa, kết nối mạng ...
- Sử dụng bộ nhớ và bộ nhớ hoán đổi
- Bộ nhớ ảo, lỗi trang

- Sử dụng mạng

Bộ công cụ *sysstat* cung cấp các tiện ích để thực hiện các thao tác giám sát cụ thể như

- *iostat*: lập báo cáo thống kê về bộ xử lý, các thiết bị vào ra và hệ thống file mạng
- *mpstat*: lập báo cáo chung hay riêng rẽ về các bộ xử lý
- *pidstat*: lập báo cáo về các công việc được thực thi của Linux.
- *sar*: thu thập, lập báo cáo và ghi lại các thông tin về hoạt động của hệ thống
- *sa2*: lập báo cáo hàng ngày về hoạt động của hệ thống
- *sadf*: hiển thị dữ liệu thu thập bởi *sar* theo các định dạng khác nhau

Để cài đặt công cụ này, người quản trị cần sử dụng câu lệnh *sudo apt-get install sysstat* và *sudo dpkg-reconfigure sysstat* để cấu hình. Để lấy thông tin về các thao tác vào/ra, người quản trị có thể sử dụng câu lệnh *sar -b*. Kết quả của câu lệnh cho biết tốc độ trao đổi dữ liệu tính theo giao dịch (đọc hay ghi) và tốc độ tính theo đơn vị dữ liệu trên giây như trong hình dưới đây.

	07:44:20 PM	tps	rtps	wtps	bread/s	bwrtn/s
	07:45:01 PM	8.03	0.00	8.03	0.00	106.61
	07:55:01 PM	8.78	0.14	8.64	3.35	127.59
	08:05:01 PM	7.16	0.00	7.16	0.00	61.14
	08:15:01 PM	8.17	0.14	8.03	5.82	139.02
	08:25:01 PM	9.50	0.06	9.44	4.09	212.62
	08:35:01 PM	8.27	0.00	8.27	0.01	74.66
	08:45:01 PM	8.04	0.00	8.04	0.00	71.51
	08:55:01 PM	7.64	0.00	7.64	0.00	66.46
	09:01:18 PM	7.11	0.00	7.11	0.36	63.73
	09:05:01 PM	7.61	0.00	7.61	0.00	72.11
Average:		8.11	0.04	8.06	1.67	102.52

Hình VIII-8. Thông kê vào/ra đĩa

VIII.4.2 Kiểm toán

Việc kiểm toán hệ thống cho phép người quản trị thực hiện các nhiệm vụ tiêu biểu như sau:

- Theo dõi truy nhập file và thay đổi
- Giám sát các lời gọi và chức năng hệ thống
- Phát hiện các bát thường như các tiến trình bị hỏng/ngưng.
- Các câu lệnh thực hiện bởi người dùng

Mục tiêu cơ bản của việc kiểm toán là đảm bảo hệ thống được vận hành một cách an toàn, giảm thiểu các rủi ro, và ứng phó một cách hữu hiệu khi có trực trặc xảy ra. Bộ công cụ *auditd* cho phép người quản trị thực hiện các thao tác kiểm toán trong môi trường Linux và được cài đặt thông qua câu lệnh *sudo apt-get install auditd*.

Bộ công cụ này cung cấp các tiện ích như sau

- *auditd*: dịch vụ ghi nhận các sự kiện (file log)
- *auditctl*: công cụ cấu hình auditd
- *aureport*: công cụ báo cáo từ file log

- *ausearch*: xem các sự kiện
- *ausyscall*: cho biết ID lời gọi hệ thống và tên
- *audit.rules*: các luật kiểm toán
- *autrace*: kiểm tra vết của chương trình
- *auditd.conf*: file cấu hình

Việc giám sát các thao tác được thực hiện thông qua việc xây dựng các luật từ người quản trị và đưa vào trong hệ thống *auditd* qua file cấu hình hoặc tiện ích *auditctl*. Dưới đây là một số tình huống cụ thể.

Giám sát các thay đổi trong việc truy nhập file và thư mục.

Câu lệnh thiết lập các luật việc giám sát các thay đổi ở file *passwd* là *sudo auditctl -w /etc/passwd -p rwxa* trong đó các tham số có ý nghĩa như sau

- -w đường_dẫn: thêm vào danh sách theo dõi file được mô tả trong đường dẫn
- -p: các kiểu truy nhập cần được giám sát gồm có r: đọc, w: ghi, x: thực thi, a: thuộc tính

Để giám sát thư mục, người quản trị sử dụng câu lệnh *sudo auditctl -w /var/www/html*. Tại bất kỳ thời điểm nào, người quản trị có thể theo dõi các giám sát đã được thiết lập thông qua câu lệnh sử dụng đặc quyền như trong hình dưới đây.

```
pduy@ux64NoGui:~$ sudo auditctl -l
-w /etc/passwd -p rwxa
-w /var/www/html/ -p rwxa
```

Hình VIII-9. Danh sách các luật đã thiết lập

Khi muốn xem các truy nhập đã được thực hiện tới các đối tượng chịu giám sát, người quản trị sử dụng tiện ích *ausearch*. Với luật giám sát lên file *passwd*, người quản trị xem các truy nhập qua câu lệnh *sudo ausearch -f /etc/passwd*. Kết quả như trong hình dưới đây.

```
dev=fc:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 namet
type=CWD msg=audit(1444794266.794:544): cwd="/home/p
type=SYSCALL msg=audit(1444794266.794:544): arch=c000
exit=3 a0=7f7f1ea63f94 a1=80000 a2=1b6 a3=0 items=1 p
967295 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1
y=pts18 ses=4294967295 comm="sudo" exe="/usr/bin/sudo
-----
time->Wed Oct 14 10:44:26 2015
type=PROCTITLE msg=audit(1444794266.794:545): proctit
68002D66002F6574632F706173737764
type=PATH msg=audit(1444794266.794:545): item=0 name=
dev=fc:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 namet
type=CWD msg=audit(1444794266.794:545): cwd="/home/p
type=SYSCALL msg=audit(1444794266.794:545): arch=c000
exit=5 a0=7f7f1ea63f94 a1=80000 a2=1b6 a3=0 items=1 p
967295 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1
y=pts18 ses=4294967295 comm="sudo" exe="/usr/bin/sudo
-----
```

Hình VIII-10. Thông tin truy nhập vào file chịu giám sát.

Các thông tin cơ bản về truy nhập bao gồm:

- *time*: thời điểm ghi nhận
- *name*: tên đối tượng theo dõi
- *cwd*: thư mục hiện thời
- *syscall*: lời gọi hệ thống
- *auid*: định danh người dùng
- *comm*: câu lệnh

Giám sát các tiến trình.

Người quản trị thực hiện giám sát các chương trình (lệnh) của Linux qua câu lệnh *sudo autrace -r /bin/ls*. Câu lệnh này theo dõi việc thực hiện câu lệnh *ls*. Tùy theo nhu cầu quản trị, người quản trị có thể đặt các giám sát với các chương trình và lệnh khác nhau của hệ thống. Cũng giống như giám sát các file, người quản trị dùng *ausearch* để xem các thông tin cụ thể về việc sử dụng các chương trình này.

Báo cáo giám sát.

Tiện ích *aureport* thực hiện việc sinh ra các báo cáo từ các file nhật ký của dịch vụ giám sát *auditd* thông qua việc sử dụng các câu lệnh như sau:

- *sudo aureport*: báo cáo tóm tắt
- *sudo aureport -au*: báo cáo về việc xác thực
- *sudo aureport -m*: báo cáo về các thay đổi tài khoản
- *sudo aureport -u*: báo cáo về người dùng
- *sudo aureport -n*: báo cáo về các bất thường

Hình dưới đây thể hiện báo cáo về việc kiểm tra xác thực với người dùng. Trong một số tình huống, người dùng đã xác thực không thành công.

```
pduy@ux64NoGui:~$ sudo aureport -au

Authentication Report
=====
# date time acct host term exe success event
=====
1. 10/07/2015 14:31:34 pduy ? /dev/pts/3 /usr/bin/sudo no 329
2. 10/07/2015 14:31:35 pduy ? /dev/pts/3 /usr/bin/sudo no 330
3. 10/07/2015 14:37:28 pduy ? /dev/pts/3 /usr/bin/sudo yes 333
4. 10/14/2015 08:32:51 pduy ? :0 /usr/sbin/lightdm yes 77
5. 10/14/2015 08:33:53 pduy ? /dev/pts/7 /usr/bin/sudo yes 90
6. 10/14/2015 09:59:06 pduy ? /dev/pts/7 /usr/bin/sudo yes 144
7. 10/14/2015 10:05:43 pduy ? :0 /usr/sbin/lightdm yes 92
8. 10/14/2015 10:06:49 pduy ? /dev/pts/6 /usr/bin/sudo yes 105
9. 10/14/2015 10:28:45 pduy ? /dev/pts/2 /usr/bin/sudo no 365
10. 10/14/2015 10:28:50 pduy ? /dev/pts/2 /usr/bin/sudo yes 367
11. 10/14/2015 10:30:55 pduy ? /dev/pts/18 /usr/bin/sudo yes 418
12. 10/14/2015 10:55:20 pduy ? /dev/pts/2 /usr/bin/sudo yes 670
```

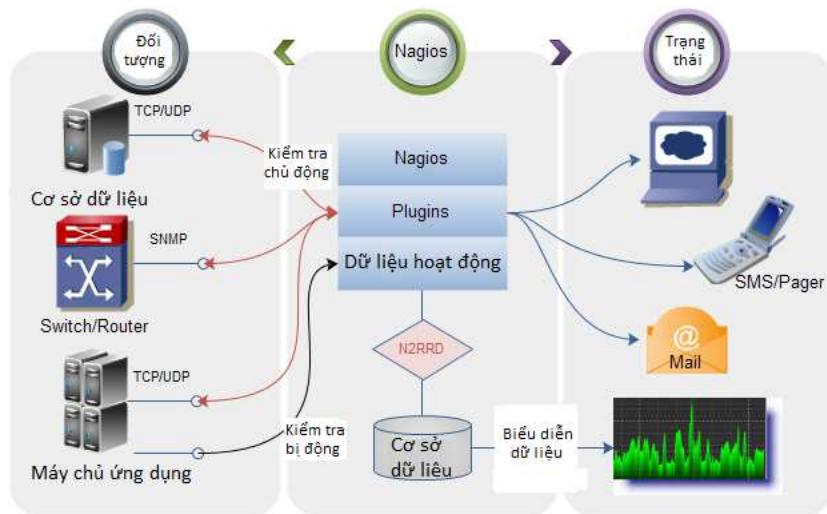
Hình VIII-11. Thông tin về việc xác thực người dùng.

Bên cạnh *auditd*, NAGIOS là bộ phần mềm mã nguồn mở, được thiết kế để chạy trên nền Linux, cho phép giám sát hạ tầng hệ thống và mạng. Quan trọng hơn, NAGIOS cung cấp dịch

vụ giám sát và cảnh báo tình trạng hoạt động của các máy chủ, bộ chuyển mạch, các ứng dụng và dịch vụ.

Về cơ bản, NAGIOS cho phép:

- Giám sát các dịch vụ mạng SMTP, POP3, SSH, HTTP, SNMP
- Giám sát các tài nguyên trên máy trạm (CPU, ổ cứng)
- Giám sát bằng cách chạy các đoạn mã từ xa thông qua bộ thực thi từ xa Nagios Remote Plugin Executor
- Hỗ trợ người dùng lập trình các dịch vụ kiểm tra theo yêu cầu riêng bằng C++, PHP, Perl,..



Hình VIII-12. Các bộ phận NAGIOS

Các bộ phận cấu thành NAGIOS gồm có:

- NRPE (*Nagios Remote Plugin Executor*): cho phép giám sát các hệ thống ở xa bằng các đoạn mã cài trên hệ thống ở xa. NRPE cho phép chạy các đoạn mã thêm vào của Nagios trên hệ thống ở xa để giám sát các tài nguyên của hệ thống như CPU, ổ đĩa, người dùng.
- NRD (Nagios Remote Data Processor): cung cấp cách thức xử lý và truyền dữ liệu mềm dẻo. NRD sử dụng giao thức tiêu chuẩn *http* và *xml* để truyền và đóng gói dữ liệu.
- NSClient+++: chủ yếu dùng giám sát các máy chạy Windows
- N2RRD (*Nagios to Round Robin Database*): lưu dữ liệu từ các phần mềm theo dõi Nagios vào cơ sở dữ liệu.

Cài đặt NAGIOS gồm các gói dịch vụ *nagios*, *nagios-nrpe-plugin* và *nagios-nrpe-server*. Trên máy chủ dùng để giám sát toàn bộ hệ thống cần *ngaios* và *nagios-nrpe-plugin*. Trên máy chủ dịch vụ cần giám sát cần *nagios-nrpe-server*.

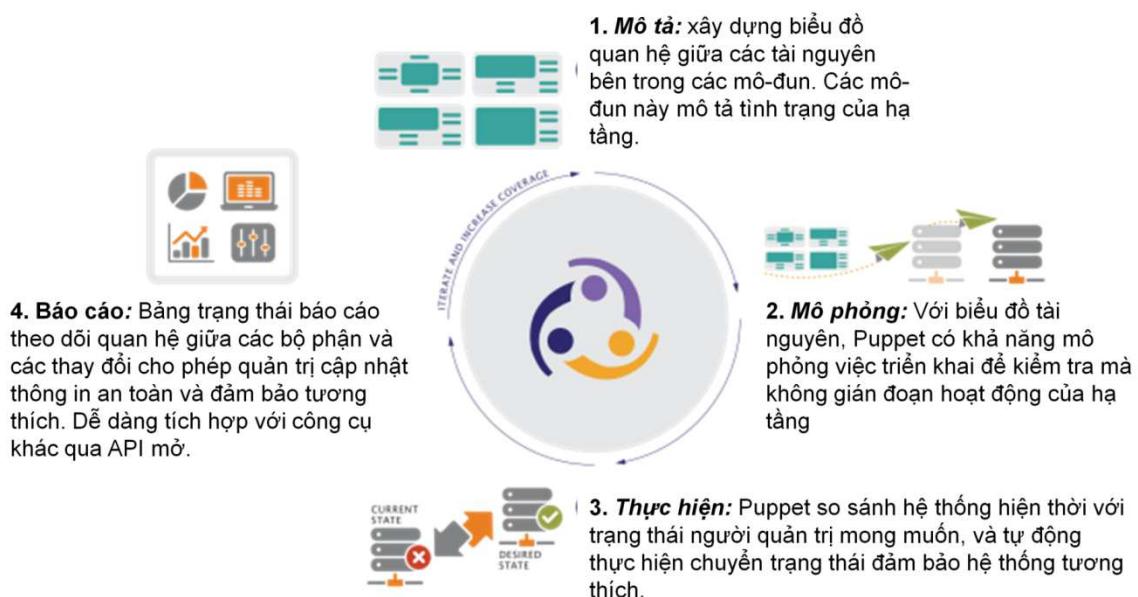
Việc sử dụng NAGIOS giúp cho việc giám sát và kiểm toán được thuận tiện hơn nhờ có giao diện qua Web và người dùng quản trị có thể lựa chọn các cách thức biểu diễn dữ liệu giám sát mềm dẻo.

VIII.5 Giới thiệu các công cụ quản trị từ xa

Trong nhiều trường hợp người quản trị cần thực hiện các công việc quản trị với các máy trạm hay các máy chủ dịch vụ từ xa do sự cách biệt vật lý với vị trí của người quản trị. Các công cụ quản trị từ xa phổ biến trong môi trường Linux có thể kể đến: OpenSSH, Puppet và Zentyal.

OpenSSH là gói phần mềm được cung cấp miễn phí dựa trên bộ giao thức Secure Shell (SSH) cho phép điều khiển và truyền file một cách an toàn giữa các máy tính. OpenSSH giúp làm thuận tiện việc điều khiển máy tính từ xa được an toàn và bảo mật nhờ sử dụng cơ chế mã hóa công khai và giữ bí mật khóa phiên làm việc.

Puppet là bộ phần mềm hoạt động trên nhiều hệ thống (Windows và Linux) hỗ trợ việc quản trị cấu hình hệ thống do Puppet Labs cung cấp. Puppet sử dụng ngôn ngữ mô tả riêng để quản lý cấu hình hệ thống. Các thông tin về cấu hình của các thiết bị được lưu trữ kiểm tra trong quá trình hoạt động giúp thuận tiện cho việc triển khai và quản trị. Để triển khai việc quản trị, người quản trị cần thực hiện 4 bước cẩn thận như trong hình dưới đây.



Hình VIII-13. Các bước thực hiện quản trị Puppet.

Sử dụng Puppet cho phép người quản trị xác định trạng thái mong muốn của hệ thống, mô phỏng việc thay đổi trạng thái (cấu hình) trước khi thực sự triển khai các thay đổi này, thực hiện việc thay đổi một cách tự động và sau đó báo cáo sự khác biệt giữa hai trạng thái (cấu hình). Trạng thái mong muốn được xác định trên máy chủ Puppet và các tác vụ phần mềm Puppet được cài đặt trên các máy trạm hay máy chủ được giám sát sẽ tải về và thực hiện việc thay đổi trạng thái. Để cài đặt máy chủ Puppet cần cài qua câu lệnh `sudo apt-get install`

puppetmaster còn phần mềm tác tử chạy trên máy được giám sát được cài đặt qua câu lệnh *sudo apt-get install puppet*.

Zentyal là bộ phần mềm máy chủ cung cấp nhiều chức năng như quản trị hạ tầng, máy chủ văn phòng, máy chủ thông tin v.v. Bộ phần mềm này cung cấp giao diện đồ họa qua web giúp việc quản trị được dễ dàng và thuận tiện. *Zentyal* cung cấp các mô-đun chức năng như sau:

- *zentyal-core & zentyal-common*: cung cấp các chức năng giao tiếp thiết yếu và thư viện dùng chung cho bộ phần mềm bao gồm mô-đun lưu trữ log và sự kiện.
- *zentyal-network*: quản lý cấu hình mạng từ các giao tiếp mạng đến các máy chủ cổng (gateway).
- *zentyal-objects & zentyal-services*: cung cấp lớp trừu tượng hóa địa chỉ mạng và tên cổng. Nói cách khác, mô-đun này cho phép diễn giải các tài nguyên mạng thân thiện với người dùng: cổng 80 -> dịch vụ web.
- *zentyal-dns & zentyal-dhcp*: cấu hình DNS và DHCP.
- *zentyal-users*: cho phép quản lý người dùng và nhóm.
- *zentyal-printers*: cho phép quản lý máy in và người dùng máy in.
- *Zentyal-antivirus*: tích hợp phần mềm chống mã độc.

Để cài đặt người quản trị sử dụng câu lệnh *sudo apt-get install <tên-mô-đun-Zentyal>*.

VIII.6 Lập trình Shell

Các đoạn mã Shell cho phép nhanh chóng triển khai hay thử nghiệm một ứng dụng trong môi trường dòng lệnh của Linux/Unix sử dụng số lượng hạn chế các cấu trúc và câu lệnh của hệ thống. Mặt khác, chương trình shell cho phép tự động hóa nhiều nhiệm vụ trong việc quản trị hệ thống. Phần dưới đây giới thiệu các khái niệm cơ bản để viết các chương trình Shell.

Để viết đoạn mã Shell, người dùng có thể sử dụng bất cứ trình soạn thảo nào như vi, nano, gedit... Để chạy người dùng cần chú ý thay đổi thuộc tính của file chứa đoạn mã sang dạng thực thi được qua câu lệnh *chmod*. Sau đó, đoạn mã có thể chạy qua câu lệnh *sh tên_file*.

Shell cho phép chạy nhiều câu lệnh một cách tuần tự. Thay vì nhập lệnh vào từng dòng, các câu lệnh có thể được ghi vào trong một dòng và phân cách bằng dấu chấm phẩy như dưới sau: *~\$ mkdir Documents; cd Documents*.

VIII.6.1 Thực hiện có điều kiện.

Các câu lệnh chạy trong Linux/Unix thường có giá trị trả về cho biết kết quả thực hiện câu lệnh. Khi câu lệnh thực hiện thành công mã trả về là 0 và được lưu trong một biến đặc biệt là *\$. Đoạn mã sau biểu diễn cách dùng của biến này.*

```

~$ ls
Documents tasks.txt bookmarks.html
~$ echo $?
0
~$ ls -z
ls: invalid option -- 'z'
Try 'ls --help' for more information
Using A Shell
197
~$ echo $?
2

```

Giá trị trả về của câu lệnh có thể dùng làm điều kiện để thực thi câu lệnh kế tiếp thông qua ký hiệu `&&`. Ví dụ `mkdir Documents && cd Documents`. Ngoài ra, có thể sử dụng ký hiệu `||`, trong trường hợp nếu câu lệnh trước lỗi thì sẽ thực hiện câu lệnh sau như trong ví dụ: `mount /media/USB || sudo mount /media/USB`. Nếu như lệnh `mount` không thành công thì sẽ thử lại với câu lệnh `sudo`.

VIII.6.2 Các thao tác vào ra.

Trong quá trình thực hiện câu lệnh hệ thống, kết quả thực hiện của câu lệnh có thể dùng làm dữ liệu đầu vào cho câu lệnh khác nhờ ký tự `|`. Đoạn mã sau tìm kiếm từ khóa “*complete emerge*” từ file nhật ký `emerge.log` và chọn lấy 5 dòng cuối cùng.

```

~$ grep 'completed emerge' /var/log/emerge.log | tail -5
1283033552: :: completed emerge (1 of 1) app-admin/cvechecker-0.5 to /
1283033552: :: completed emerge (1 of 3) dev-perl/HTML-Tagset-3.20 to /
1283033552: :: completed emerge (2 of 3) dev-perl/MP3-Info-1.23 to /
1283033552: :: completed emerge (3 of 3) app-pda/gnupod-0.99.8 to/
1283033552: :: completed emerge (1 of 1) app-admin/cvechecker-0.5 to /

```

Ký hiệu `|` cho phép tạo thành các *ống* kết nối dữ liệu giữa các câu lệnh và có thể xâu chuỗi nhiều hơn 2 ứng dụng. Một khái niệm `>` cho phép thay đổi luồng dữ liệu. Ví dụ như muốn lưu toàn bộ tên file và thư mục hiện thời vào file `content.txt`, có thể sử dụng câu lệnh `ls > content.txt`.

Trong trường hợp muốn ghi tiếp vào file đã có, sử dụng ký hiệu `>>` như trong câu lệnh `ls >> content.txt`.

VIII.6.3 Câu lệnh điều kiện

If...then...if. Cấu trúc điều kiện này cho phép thực thi các câu lệnh tùy thuộc vào điều kiện đặt ra có được thỏa mãn hay không. Đoạn mã dưới đây minh họa cách thức sử dụng

```

#Ví dụ
chon=1
if [ "$chon" = "1" ]
then
    echo "Chọn 1"
elif [ "$chon" = "2" ]
then
    echo "Chọn 2"
elif [ "$chon" = "3" ]
then
    echo "Chọn 3"
else
    echo "Chọn tất cả còn lại?"
    echo "Chọn lại"
fi

```

Ký hiệu # báo hiệu phần ghi chú của đoạn mã, \$chon mô tả đoạn mã sử dụng biến chon, ký hiệu “[...]" mô tả điều kiện kiểm tra. Các phép toán kiểm tra điều kiện bao gồm: bằng “=”, lớn hơn “-gt”, nhỏ hơn “-lt”, không bằng “-ne”, thuộc “-in” ... Khi cần kết hợp nhiều điều kiện có thể sử dụng ký hiệu lô-gíc và “&&” hay hoặc “||”.

For ... do ... done. Cấu trúc lặp cho phép thực hiện các câu lệnh chừng nào biểu thức điều kiện sau từ khóa for còn hiệu lực. Dưới đây là ví dụ về việc sử dụng cấu trúc này.

```
fruitlist="Apple Pear Tomato Peach Grape"
for fruit in $fruitlist
do
    if [ "$fruit" = "Tomato" ] || [ "$fruit" = "Peach" ]
    then
        echo "I like ${fruit}es"
    else
        echo "I like ${fruit}s"
    fi
done
```

while...do...done. Cấu trúc lặp này sẽ thực hiện các câu lệnh trong phần do...done chừng nào mà điều kiện sau từ khóa while còn có hiệu lực. Sau đây là một ví dụ.

```
count=$3
while [ $count -gt 0 ]
do
    echo $count giay!
    count=$((expr $count -1))
    sleep 1
echo "Het gio"
```

VIII.6.4 Ví dụ

Dưới đây là ví dụ về đoạn mã shell sử dụng cho việc sao lưu hệ thống

```
#!/bin/sh
# Necessário
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Vị trí sao lưu
dest="/mnt/backup"

# Tên file lưu trữ
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Hiển thị thông báo
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Sử dụng công trình tar để sao lưu
tar czf $dest/$archive_file $backup_files

# Thông báo kết thúc
echo
echo "Backup finished"
```

```
date  
# Kiểm tra các file tệp và vị trí $dest.  
ls -lh $dest
```

Trong đoạn mã trên, ý nghĩa của các biến như sau:

- *\$backup_file*: liệt kê các thư mục muốn sao lưu. Chi tiết có thể thay đổi phù hợp với yêu cầu sao lưu.
- *\$day*: cho biết ngay trong tuần và dùng để sinh các file lưu trữ theo ngày trong tuần.
- *\$hostname*: tên của máy tính trong mạng, giúp phân biệt bản sao lưu của các máy khác nhau.
- *\$archive_file*: tên file lưu trữ dạng đầy đủ.
- *\$dest*: vị trí của file lưu trữ. Trong trường hợp này, thư mục này cần được tạo trước và gắn với một thư mục cụb bộ.

Tài liệu tham khảo

- [1] Ashley J.S Mills, Unix Shell Scripting Tutorial, The University Of Birmingham, 2005
- [2] Ellen Siever, Stephen Figgins, Robert Love, Arnold Robbins, Linux in a Nutshell, O'Reilly Media, 2009.
- [3] Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, UNIX and Linux System Administration Handbook, Prentice Hall, 2010.
- [4] Kyle Rankin, Benjamin Mako Hill, The Official Ubuntu Server Book Second Edition, Prentice Hall, 2010
- [5] Microsoft Technet Library, <https://technet.microsoft.com>
- [6] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [7] Tom Carpenter, Microsoft Windows Operating System Essentials, Sybex, 2012.
- [8] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.
- [9] Wikipedia, https://en.wikipedia.org/wiki/History_of_Unc
- [10] William Panek, Tylor Wentworth, Mastering Microsoft Windows 7 Administration, Sybex, 2009.
- [11] William Panek, MCSA Windows Server 2012 Complete Study Guide, Sybex, 2012
- [12] William von Hagen, Ubuntu Linux Bible, Wiley Publishing, Inc., 2007